THÈSE DE DOCTORAT DE
SORBONNE UNIVERSITÉ

Spécialité

Informatique

École doctorale Informatique, Télécommunications et Électronique (Paris)

Présentée par

Clémence Bouvier

Pour obtenir le grade de

DOCTEUR de SORBONNE UNIVERSITÉ

Cryptanalysis and design of symmetric primitives defined over large finite fields

soutenue publiquement le 27 novembre 2023

devant le jury composé de :

Anne CANTEAUT	Inria Paris, France	Directrice de thèse
Léo PERRIN	Inria Paris, France	Co-directeur de thèse
Henri GILBERT	ANSSI, France	Rapporteur
Sondre RØNJOM	University of Bergen, Norway	Rapporteur
Pierre-Alain FOUQUE	Université de Rennes, France	Président du jury
Gregor LEANDER	Ruhr University Bochum, Germany	Examinateur
Willi MEIER	FHNW, Windisch, Switzerland	Examinateur
Damien VERGNAUD	Sorbonne Université, France	Examinateur

À Toi, à Moi, à Eux,
À tous ceux qui le veulent…

Remerciements

Il est difficile de trouver les mots justes pour exprimer ce que je ressens en rédigeant ces remerciements, en repensant à tout le chemin qui m'a menée jusqu'ici et surtout à toutes les personnes qui m'ont accompagnée dans cette aventure. Une thèse ne se résume pas seulement à un manuscrit de quelques centaines de pages : soutenir ses travaux est l'accomplissement de mois de recherche, de remises en question, de découragements, d'idées bien souvent infructueuses et de déconvenues souvent ponctuées de larmes. Finalement, une thèse, c'est un peu comme un marathon. Au-delà de cette distance mythique de 42.195km, franchir la ligne d'arrivée est l'accomplissement de semaines de préparation, de privations, d'entraînements longs et intenses, parfois dans le froid, sous la pluie. Ces deux aventures, si souvent associées à une réussite personnelle et un engagement individuel, ne sont pourtant rien sans les conseils et le soutien de ses pairs. J'aimerais ainsi remercier toutes les personnes ayant contribué, par un simple regard, un geste, quelques mots ou bien plus, à l'aboutissement de ces trois riches années de thèse.

Débuter une thèse en ces temps de confinement n'était assurément pas le scénario que j'aurais imaginé. Le contexte sanitaire a apporté son lot de complications, mais j'ai eu la chance de croiser le chemin de personnes formidables, et je suis particulièrement reconnaissante envers toutes celles qui se sont heurtées, de près ou de loin, à l'hypersensible qui réside en moi. Certains trouveront un excès de lyrisme dans mes propos, mais ceux qui me connaissent savent mon attachement aux beaux et longs discours. Mon aisance à l'écrit a toujours surpassé celle à l'oral[1] et c'est pourquoi je saisis l'occasion de ces "quelques lignes" pour exprimer plus chaleureusement mes remerciements. La liste des personnes à qui je suis redevable est longue, j'aspire à ne négliger personne et être la plus juste possible.

Mes premières pensées se dirigent naturellement vers Anne et Léo qui m'ont prise sous leurs ailes dès mon stage de master pour me suivre jusqu'en thèse. Tout d'abord, un grand merci pour m'avoir offert l'opportunité de travailler sur ce sujet. À mes débuts, un peu réticente à l'idée de venir "à la capitale" me lancer en crypto symétrique, j'ai finalement découvert un sujet passionnant que j'ai vu évoluer et gagner en popularité, favorisant ainsi d'enrichissantes collaborations.

Léo, merci de m'avoir présentée à la communauté, intégrée dans des projets et emmenée en vadrouille. En particulier, merci de m'avoir permis de participer à la conception d'Auld, devenu Anemoi. Certes, le papier n'a pas toujours fait l'unanimité, mais Anemoi est, et restera, une de mes plus grandes fiertés. Ce projet a également représenté ma première réelle collaboration avec des scientifiques d'horizons divers donc, je te remercie pour cet enrichissement à la fois personnel et professionnel. Merci pour ta disponibilité, pour les discussions scientifiques, pour ton partage. Enfin, merci de m'avoir écoutée encore et encore, tant pour mes présentations en conférences et séminaires, que la préparation du concours MT180. Tu es, sans aucun doute, la personne à qui j'aurais le plus cassé la tête.

Anne, je mesure ma chance d'avoir pu commencer à tes côtés et profiter de tes connaissances, ta rigueur scientifique et tes précieux conseils. Un grand merci pour ton enthousiasme, ton engagement malgré tes nombreuses occupations et ton efficacité pour gérer les soucis

[1] Toutes ces belles déclarations pourraient en effet se traduire, oralement, par un timide "merci".

administratifs ou débloquer les problèmes par tes idées judicieuses. Ton stylo bleu m'aura parfois valu quelques sueurs froides mais il m'a tellement apporté. Et même quand elle n'est pas là, Anne veille sur nous, comme en témoigne Anemoi, qui se prononce officiellement : *"Anemoï"* mais peut également se lire plus affectueusement : *"Anne et moi"*.

Enfin, je vous remercie pour votre relecture attentive de ce manuscrit.

I would like to thank Henri Gilbert, Sondre Rønjom, Pierre-Alain Fouque, Gregor Leander, Willi Meier and Damien Vergnaud for accepting to be part of my thesis jury. I would particularly like to thank Henri and Sondre for accepting the difficult task of reviewing this long (maybe too long) manuscript.

Merci également à Yann et Damien d'en avoir assuré le suivi.

Merci aux membres de l'équipe COSMIQ, et ses "squatteurs" réguliers, que j'ai eu le plaisir de côtoyer pendant ces trois années : Agathe, André (le jeune), André (le sage), Anthony, Antonio, Anne, Augustin, Aurélie, Aurélien, Axel, Charles, Christina, Clara, Daniel, Dounia, Jean-Pierre, Johanna, Jules, Gaëtan, Léo, María, Matthieu, Maxime, Nicolas, (le petit) Nicolas, Pascale, Paul, Pierre, Rachelle, Rémi, Ritam, Rocco, Simona, Valentin, Virgile, Yann, ... et tous ceux que j'aurais pu oublier.

J'aimerais également remercier Christelle, pour son dynamisme et sa réactivité face à mes nombreuses sollicitations pour les contrariétés administratives.

J'en profite d'ailleurs pour présenter officiellement mes plus plates excuses auprès du grand chef, Jean-Pierre, pour lui avoir ruiné sa réputation de maître incontesté des tournois de babyfoot[2].

Un grand merci au *Bureau des Renseignements*[3], pour les commérages en tout genre, pour les discussions sérieuses et existentielles, puis d'autres un peu moins. Fortes de notre "charisme" légendaire, nous n'avons pas toujours "osé" mais nos moments de doutes partagés, et nos encouragements mutuels ont définitivement celés une belle amitié. Merci d'avoir rendu ces trois années agréables, faisant oublier l'enfer du confinement et les difficultés de la thèse.

Merci à ma jumelle, Clara, enquêtrice de renom, voisine de palier, mais surtout grande complice pour les ragots de la pause café. Souvent confondues, il faut admettre que nous n'aidions pas beaucoup à dissiper les confusions : originaires de province, sportives, inséparables en conférences, jusqu'à souvent arborer les mêmes tenues fétiches. Merci pour tous ces beaux moments partagés et pour les nombreuses bêtises racontées.

Merci Aurélie, ma partenaire de vulgarisation. À ces petites pauses qui se terminaient souvent en sessions confidences et chuchotements à l'abri des oreilles indiscrètes. Merci également pour ton expertise de traductrice, mais surtout de nous avoir partagé tes exploits artistiques et culinaires menant parfois à des dégustations surprenantes.

Augustin, merci pour ta gentillesse, me laissant l'opportunité de présenter le papier à FSE alors que tu aurais très légitimement pu le faire, ou acceptant *aveuglement* de me remplacer pour mes TDs en plein mois de février.

Merci Daniel pour l'accueil chaleureux lors de mon arrivée au C201.

Simona, thanks for the printing advice, for the running sessions that helped me to practise my English, and simply thanks for your kindness and your generosity.

Merci Nicolas, compagnon de galères administratives.

[2] Qui plus est une élimination suite à une défaite contre Charles, quelle honte...

[3] Il m'a semblé plus approprié de taire le nom officiel.

Rachelle, merci pour les réflexions et discussions que nous avons partagées lors des conférences et de tes visites au bureau.

Jules, j'ai toujours trouvé que les rôles avaient été inversés : tu es mon petit frère académique mais pourtant le plus mature de nous deux et enclin à prendre du recul sur les situations compliquées et stressantes ou sur les problèmes mathématiques. Merci pour tes mots justes, encourageants et toujours à la hauteur de la situation. Tu maîtrises l'art du brainstorming comme personne, un grand merci également pour tes brillantes idées qui ont indéniablement inspiré mes présentations. Je ne peux que regretter que tu n'aies pas, toi aussi, fait partie de la team *AOP*.

Et puis, il y a toujours un individu pour divertir le groupe, coupable idéal quels que soient les soucis rencontrés, nul doute qu'il aura été démasqué bien avant que son identité ne soit révélée. Du rock improvisé rue Daumesnil, aux histoires croustillantes des cantines entre *frère et sœur*, merci Charles pour avoir apporté un peu de gaieté. Merci également pour ta témérité, osant franchir la porte du bureau alors que beaucoup l'avaient fui. Finalement, malgré cette sombre histoire d'"incohérence", malgré nos façons de penser plus que diamétralement opposées, tu auras su éclairer mon esprit parfois si naïf.

Enfin, merci à tous les deux de m'avoir offert un petit coin de bureau au calme pour rédiger plus sereinement, et d'avoir permis ce "safe space" dont j'avais besoin.

Je souhaite également exprimer ma plus grande reconnaissance envers mes dépanneurs informatiques, que je ne saurais énumérer sans en oublier. Merci pour leur dévouement, leur fidélité et leur assistance précieuse tout au long de cette thèse.

Merci à mes divers partenaires de course à pied, du 2e étage au 4e, notamment Fabian et Thomas qui m'ont accompagnée sur quelques séances de fractionné pendant la prépa marathon. Merci aux membres de l'ALJCC (Association Légendaire des Jeunes Coureurs de Cosmiq) et de "Paris sportifs" pour nos belles victoires respectives bien que restées si tristement non récompensées.

Au début marquée par divers confinements successifs, ma thèse s'est finalement révélée synonyme de découvertes, de rencontres, d'invitations et de premières expériences dans divers pays : Allemagne, Autriche, Croatie, États-Unis, Grèce, Israël, Japon et Norvège. Ces expériences furent bien évidemment ponctuées de multiples péripéties. Entre un taxi illégal et une valise perdue à l'aéroport je n'aurais pas échappé au fameux bizutage du premier voyage en conférence.

Je souhaite ainsi adresser un petit clin d'œil chaleureux à tous mes compères impliqués dans ces aventures plus incroyables les unes que les autres. En particulier, merci aux gardes du corps venus à ma rescousse après les mésaventures de taxi.

Thanks Anu, roommate for Crypto, and Barbara my "bedmate" in Passau during the Cross-"Fire" workshop.

Merci aux surfeurs de Hendaye, aux chanteurs de Kobé, de Bergen et de Najac.

Thanks to the Tel Aviv billionaire for the crazy party, and to the prince met in LA for the fascinating stories.

Je tiens aussi à exprimer ma sincère reconnaissance envers toutes les personnes qui m'ont accompagnée tout au long de l'aventure MT180 : Claudine et Alexandra, les 17 autres finalistes de Sorbonne Université, les nombreux cobayes (collègues, famille et amis) ainsi que Lucile et le Service Communication et Médiation d'Inria Paris pour leur précieux soutien. Un merci tout particulier à mes fidèles supporters lors de la finale, qui m'ont offert des encouragements inestimables me permettant de remporter le Prix des internautes.

J'aimerais également remercier Clémentine pour avoir été une des premières à me solliciter pour la médiation scientifique, me transmettant avec enthousiasme sa passion.

I would also like to thank my co-authors with whom I had the pleasure of working. Thanks Anne, Augustin, Danny, Fukang, Gaëtan, Léo, Lorenzo, Pierre, Pyrros, Robin, Vesselin, Willi. I am deeply grateful for your contributions and our scientific discussions, as this manuscript would not exist without you. Special thanks to the Anemoi team, for the interesting discussions which gave me a lot of scientific input, and also for the unfailing support despite the rejections. But we finally make it, thank you all.

Robin, dès le master, tu as été d'un précieux soutien. Tu es une des rares personnes en qui j'ai une totale confiance et je suis donc extrêmement fière d'avoir pu continuer à tes côtés, même si tu me faisais souvent travailler à des heures tardives. Tes questions, toujours pertinentes, m'ont parfois poussée dans mes retranchements, mais elles m'ont également fait sentir intelligente et utile, au-delà de mes compétences artistiques. Enfin, merci, du fond du cœur, d'avoir si généreusement proposé de relire cette interminable thèse et pour ton incroyable réactivité face à mes nombreuses sollicitations de dernières minutes.

I extend my heartfelt thanks to Reinhard for the fascinating discussions we have shared, spanning from professional to personal or more philosophical topics. In particular, I would like to express again my gratitude for your kindness and warm welcome during my stay in Graz. I am deeply grateful to you for proposing the visit, and to Christian for making it possible.

I also wish to express my deep appreciation to Gregor for the invitation in Bochum, and for allowing me to join a German team as a post-doc although I am not a beer drinker.

Gohar, thank you for inviting me in Rostock and for the interesting scientific discussion that might have inspired some of the figures in this thesis.

Thanks Carlos for the invitation in a sunny[4] Bergen for the first meeting of COSINUS team.

Merci aux équipes de Rennes, Angers et Paris 8 pour leurs invitations respectives.

J'aimerais également remercier Sihem pour m'avoir offert l'opportunité de chairer, pour la première fois de ma vie, une session à Fq.

À l'écriture de ces remerciements, j'aimerais aussi remonter le temps et exprimer ma gratitude envers les personnes m'ayant guidée lors de moments importants.

Mon année de M2 aura probablement été l'une des plus compliquées de mon cursus universitaire. Un peu découragée, j'ai eu la chance d'avoir un premier aperçu de la recherche dans une ambiance sereine, encourageante et dans la plus grande bienveillance. Je souhaiterais donc sincèrement remercier Delphine Boucher sans qui je n'aurais certainement jamais osé envoyer un mail pour un stage à COSMIQ.

Je voudrais également exprimer ma plus profonde reconnaissance envers une des premières personnes à avoir cru en moi. Cette thèse n'aurait peut-être même jamais vu le jour si nos chemins ne s'étaient pas croisés. Merci de m'avoir écoutée. Merci de m'avoir conseillée. Merci d'avoir mis des mots sur ce qu'on ne m'avait jamais dit. Enfin, merci de ne pas m'avoir laissée tomber malgré mon "sacré caractère". Nous pouvons être forts, persévérants, tenaces, mais parfois, nous avons aussi besoin d'autres personnes pour nous tenir la main, nous faire prendre conscience de certaines choses ou tout simplement pour nous dire que tout ira bien. Ces quelques mots ne suffiront donc jamais à remercier son investissement, son implication mais surtout son légendaire soutien "contre vents et marées". Je finirai simplement par : Merci Etienne Mann.

[4] Cela fera certainement grommeler Jean-Pierre, mais ne lui en déplaise, il ne pleut pas tout le temps à Bergen !

Je ne peux mettre de point final à ces remerciements sans une pensée pour mes proches pour leur soutien ayant grandement contribué à la réussite de cette thèse.

Fanny, merci pour ta grande gentillesse et tes mots réconfortants, ta philosophie de vie si positive m'impressionnera toujours et je ne remercierais jamais assez Blablacar de m'avoir permis te croiser ta route.

Merci Ninon, ma fidèle partenaire de course à pied. À nos footings, plus séances de commérages qu'entraînements intensifs, mais qui font les petits plaisirs des retours en Mayenne.

Merci également à toutes les deux d'avoir accepté de relire ma prose.

Jojo, merci pour ces belles années passées à tes côtés, pour ton soutien, très cher à mes yeux, tant sur le plan sportif que professionnel. Un grand merci pour ta bienveillance, prenant soin de concocter des séances en adéquation avec mon emploi du temps chargé, me permettant de trouver le parfait équilibre entre vie sportive et vie professionnelle.

Enfin, je tiens à remercier chaleureusement ma famille. Malgré une certaine incompréhension de mes travaux, je peux toujours compter sur leur soutien dans chacun de mes projets, augmentant les vues des enregistrements YouTube de présentations, ou bien se mobilisant en nombre pour me donner leur vote lors de MT180.

Et puisqu'il semblerait que la volonté de faire une thèse se transmette dans la fratrie : Le Boss, à ton tour !

Abstract

Abstract (english)

In recent years, new symmetric cryptographic primitives have been proposed for advanced protocols, like multi-party computation, in combination with a fully homomorphic encryption or in various systems of zero-knowledge proofs. Such protocols are parts of a context marked by the development of cloud and blockchain technologies, and must therefore respond to the growing security concerns of users.

These protocols have put forward the need to minimize the number of multiplications performed by the primitive in large finite fields. Classical symmetric algorithms are then inappropriate in this context and the new cryptographic protocols must be combined with symmetric primitives (encryption or hash function) with particular properties.

While the number of designs defined over large fields, called “arithmetization-oriented”, is increasing significantly, few cryptanalysis works have been proposed. The first aim of this manuscript is then to contribute to fill this gap, and hence to better understand the specificities of these new objects. We also propose a new vision to design such primitives, covering both aspects of cryptology, the cryptography and the cryptanalysis.

Keywords: symmetric cryptography · cryptanalysis · arithmetization-oriented primitives · Anemoi · algebraic degree · MiMC

Résumé (français)

Ces dernières années, de nouvelles primitives de cryptographie symétrique ont été proposées pour être utilisées dans des protocoles avancés comme le calcul multi-partite, en combinaison avec un chiffrement homomorphe ou encore dans divers systèmes de preuve à apport nul de connaissance. De tels protocoles s’inscrivent dans un contexte marqué par le développement du Cloud et des technologies de type Blockchain et doivent ainsi répondre à une préoccupation croissante des utilisateurs en matière de sécurité.

Ces protocoles ont mis en avant le besoin de minimiser le nombre de multiplications effectuées par la primitive dans des corps finis de grande taille. Les algorithmes symétriques classiques sont alors inappropriés dans ce contexte et les nouveaux protocoles cryptographiques doivent être combinés avec des primitives symétriques (chiffrement ou fonction de hachage) ayant des propriétés particulières.

Alors que le nombre de conceptions définies sur de grands corps dites “orientées arithmétisation” augmente de façon considérable, très peu de travaux d’analyse de sécurité ont été proposés jusqu’ici. L’objectif de ce manuscrit est donc en premier lieu de contribuer à combler ce manque pour mieux comprendre les spécificités de ces nouveaux outils. Nous proposons également une nouvelle vision pour concevoir de telles primitives, couvrant ainsi les deux sous-domaines de la cryptologie que sont la cryptographie et la cryptanalyse.

Mots clés : cryptographie symétrique · cryptanalyse · primitives orientées arithmétisation · Anemoi · degré algébrique · MiMC

Contents

Introduction

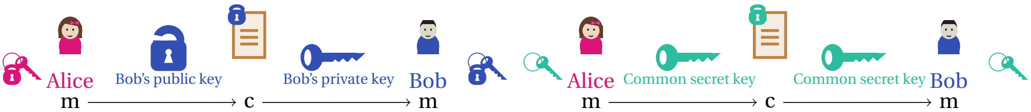
Cryptology is the science of communicating and storing data in a secure and usually secret form. It is a long-standing discipline aimed at ensuring the security of communications. While the first encryption methods were hand-crafted in ancient times, protection techniques have improved with advances first in mechanics, and then in computer science.

Basic cryptographic principles

Due to language misuse, the term *cryptography* is more commonly used, but this only refers to a subfield of cryptology, namely the design of encryption methods to transform plaintext into ciphertext. Cryptology also includes *cryptanalysis*, which covers all the techniques used to recover plaintext from its ciphertext. These two aspects of cryptology will be discussed in this thesis.

Historically, cryptography allows two protagonists, traditionally called Alice and Bob, to communicate in a secure way by ensuring the *confidentiality* (to make the information inaccessible to anyone except the two protagonists), the *authentication* (to guarantee that the person you are communicating with is who they claim to be) and the *integrity* (to ensure that no one has tampered with the information) of the messages exchanged in the presence of an adversary.

We then distinguish *asymmetric cryptography* (Figure 1a) and *symmetric cryptography* (Figure 1b). In the case of asymmetric encryption, also known as public-key encryption, Alice and Bob have their own pair of public key and private key. Let us suppose that Alice wants to send a message to Bob, she will encrypt her message using Bob's public key. Then Bob will decrypt the message using his associated private key. The idea behind this approach is that anyone knowing Bob's public key can send him an encrypted message that only Bob is able to decrypt. In the case of symmetric encryption, also known as secret-key encryption, Alice and Bob share a common secret key. This key allows them to both encrypt and decrypt their messages.



(a) *Asymmetric encryption.*

(b) *Symmetric encryption.*

Figure 1: *Key exchanges.*

The disadvantage of symmetric cryptography is the need to exchange the secret key securely. However, symmetric encryption algorithms are in fact faster than asymmetric ones. As a consequence, in most applications, we use a hybrid encryption, combining the two types of cryptography. More precisely, we use asymmetric cryptography to exchange a secret key, which then sets a symmetric cipher. In this thesis, we will focus on symmetric cryptography.

There are other important differences between asymmetric cryptography and symmetric cryptography, although the frontier is sometimes unclear. The security of asymmetric constructions tends to rely on the difficulty of mathematical problems such as integer factorisation or discrete logarithm solving, for which we do not know polynomial-time algorithms. For symmetric constructions, we generally rely on the absence of practical attacks as a security argument. Therefore, it is necessary to separate the notion of perfect security from computational security. Vernam's encryption [Ver26] is the only cipher offering *perfect secrecy*, meaning that it is theoretically impossible to break while other algorithms rely on the infeasibility of certain attacks because of their high cost.

Zero-Knowledge Proofs

In recent years, new symmetric cryptographic primitives have been proposed for some cryptographic protocols, such as Multi-Party Computation (MPC), or in combination with homomorphic encryption or in various Zero-Knowledge Proof (ZKP) systems. These protocols are part of a context marked by the development of cloud and blockchain technologies, and must therefore respond to the growing security concerns of users.

Blockchain is a digital technology that theoretically allows data to be transferred in a decentralised, secure and transparent manner. This technology is mainly used in cryptocurrencies such as Bitcoin or Ethereum. But beyond the financial sector, blockchain also aims at decentralising social functions such as some legal contracts that have been replaced by "smart contracts", although such applications are open to discussion. In order to ensure the security of these blockchains, new integrity proof systems have appeared and will be detailed in Chapter 1.

Zero-Knowledge Proofs (ZKPs) were first introduced in 1985 by Goldwasser, Micali, and Rackoff [GMR85]. In cryptography, such a proof allows one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any additional information beyond the truth of the statement itself. In other words, the prover can prove that he knows a secret without revealing the secret itself. For example, let us assume that Alice wants to prove to Bob that she knows the password of a secure system, without revealing it. This is possible with ZKP. Such situation applies for authentication, for example, when a user wants to access a bank account. In this case, the system checks that the user knows the password, without recovering its content.

As a concrete example, we can use a sudoku puzzle. Let us suppose that Alice wants to prove to Bob that she has solved a sudoku but she does not want to reveal the solution. After completing her grid on a sheet of paper, Alice cuts it out so that she has papers, one paper for each square. She then turns all the papers over, except the starting numbers, to show Bob that she has the correct grid. She then asks Bob to choose a row and gives him the papers in that row, carefully shuffling them so as not to give Bob any information about the placement of the papers. All Bob has to do is check that all the numbers from 1 to 9 appear. Once this is done, Alice puts the papers in the right order and can ask Bob to repeat the operation for each row... each column... each square... Bob can see that the grid is correct, but Alice has not told him the exact position of each number. The different steps of the process are depicted in Figure 2.

Another example of a zero-knowledge proof is the "Ali Baba cave" problem, where a prover wants to convince a verifier that he knows the secret password to a door without actually revealing the password. This problem is often used to present ZK proofs since its probabilistic approach brings it closer to reality. In this story, Alice randomly chooses a path: either A or B. We illustrate the different steps in Figure 3. Let us suppose she chooses A. Then, Bob enters in the cave and asks Alice to go out of the cave taking a specific path: either A or B. Let us suppose he chooses B. As Alice knows the password, she can go out taking the path asked by Bob. From Bob's point of view there are two situations: if Alice entered through B and went out from B, then this means that it could happen that she didn't know the password, if Alice entered through A and went out

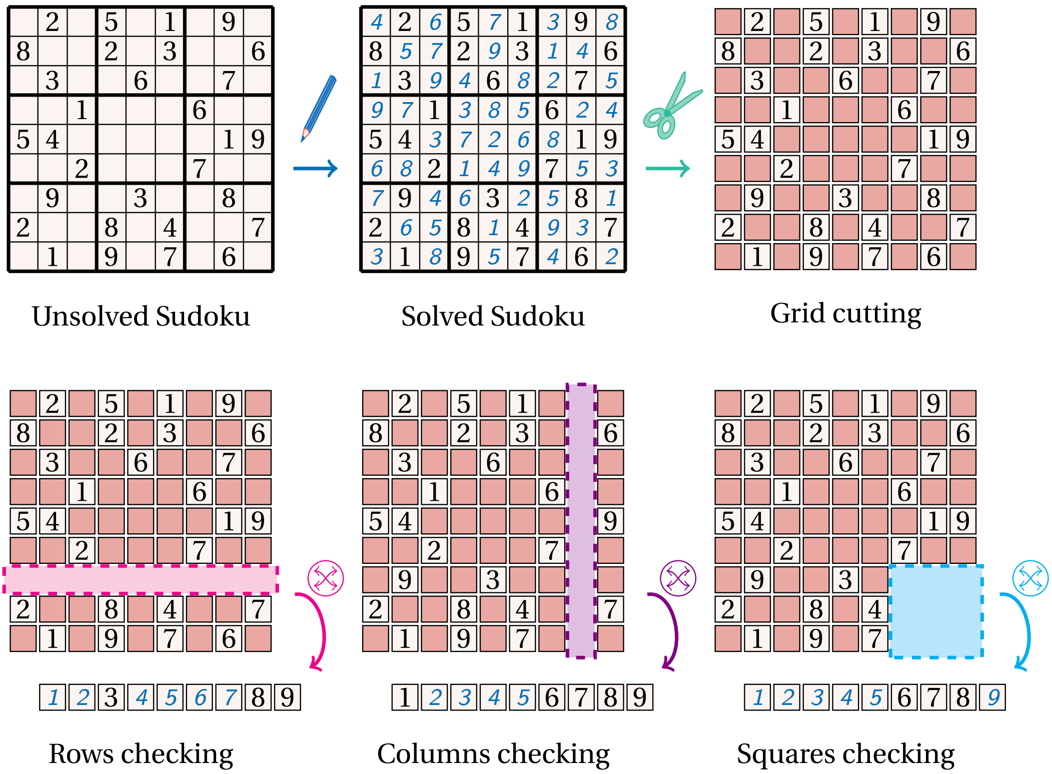


Figure 2: *ZKP with a Sudoku.*

from B, then this proves that she knows the password. To ensure that she did not take the desired exit by chance, they might repeat this game several times.

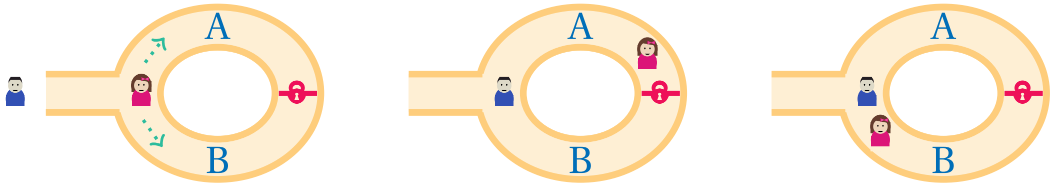
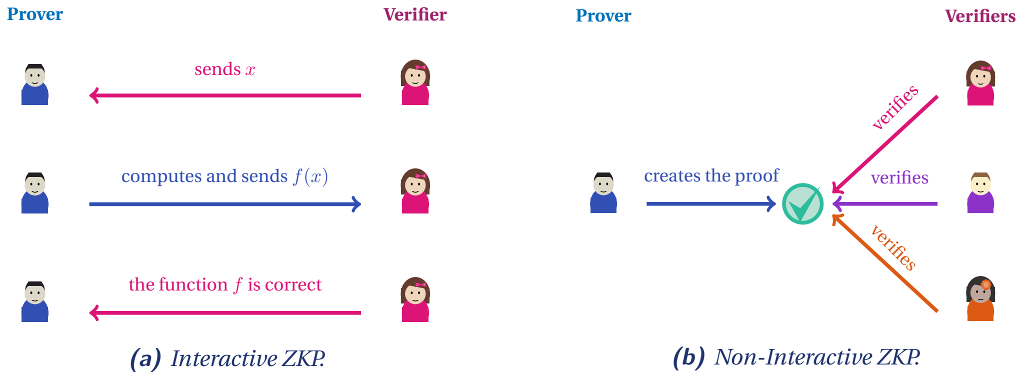


Figure 3: *Ali-Baba cave.*

Those two Zero-Knowledge Proofs are said to be "interactive" since the two parties communicate in rounds, with information going both ways throughout the protocol. Interactive Zero-Knowledge Proofs (IZKP) are opposed to the Non-Interactive Zero-Knowledge Proofs (NIZKP). The main advantage of NIZKP is that they are suitable for use in situations where no interaction between the prover and verifier is possible, such as for online transactions where there may be no real-time communication between the two parties. This is particularly useful in decentralised systems such as blockchains, where transactions are verified by a network of nodes, with no central authority overseeing the verification process. Interactive Zero-Knowledge Proofs and Non-Interactive Zero-Knowledge Proofs are presented in Figure 4.



(a) *Interactive ZKP.*

(b) *Non-Interactive ZKP.*

Figure 4: *Zero-Knowledge Protocols.*

ZKPs work by using complex mathematical algorithms and protocols to create a proof that is verifiable by the verifier. The proof is constructed in such a way that the verifier can be convinced of the truth of the statement without learning any additional information about the secret knowledge. ZKPs are used in many different applications, including authentication protocols, digital signatures, electronic voting and cryptocurrency transactions. They are particularly useful in situations where privacy and security are paramount, such as in electronic voting. The idea is to ensure that the result of the vote, i.e. the number of papers counted for each party, is correct, while keeping each individual's vote secret. ZKPs provide a powerful tool for proving knowledge and verifying the authenticity of information without revealing any sensitive information.

A need for new primitives

Such protocols are usually described as *arithmetic circuits*, showing the different stages of computation. An arithmetic circuit is a graph with a set of vertices called *gates* and a set of edges called *wires*. The gates are connected so as to carry out an arithmetic action, such as an addition, a subtraction, a multiplication, or a division. For instance, in Figure 5 we present an arithmetic circuit for the equation $(a + b) \times c = d$. This circuit has two gates: an addition gate and a multiplicative gate at two different levels.

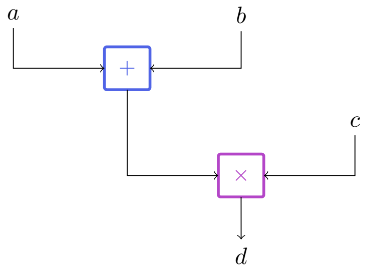


Figure 5: *Arithmetic circuit for* $(a + b) \times c = d$.

The complexity of these proof systems is then determined by various parameters, such as the depth and width of the circuit (i.e. the number of gates at each level of the circuit), but also the multiplicative complexity, which corresponds to the number of multiplication gates. The majority of proof systems are not affected by the number of addition gates on the verifier side, as this operation is considered less costly. However they may have a cost on the prover side.

As a consequence, these protocols have put forward the need to minimize the number of multiplications performed by the primitive in large finite fields, an alphabet containing more than a quintillion elements. Classical symmetric algorithms are inappropriate in this context and new cryptographic protocols must then be combined with symmetric primitives (encryption or hash function) having particular properties. The primitives adapted to these applications, called "Arithmetization-Oriented" (following the terminology introduced by Ashur *et al.* [Aly+19]) are therefore of a completely new type.

Beyond the alphabet used, the properties sought are also different. While usually from a given x we want to be able to compute efficiently $f(x)$ (Figure 6), in this new context, the verification must be efficient: we want to be able to verify that y is the image of x by the function f (Figure 7). The most natural idea is to apply the function f and check that $y = f(x)$ (Figure 7a). But this change of perspective also offers new possibilities of computation since we can consider the inverse of certain operations and thus verify that $x = f^{-1}(y)$ (Figure 7b), or use intermediate checking (Figure 7c). As a consequence, while an inversion in a finite field might be very expensive, it is not in a circuit.

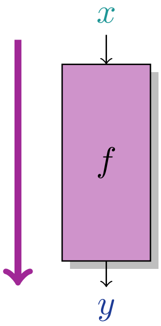
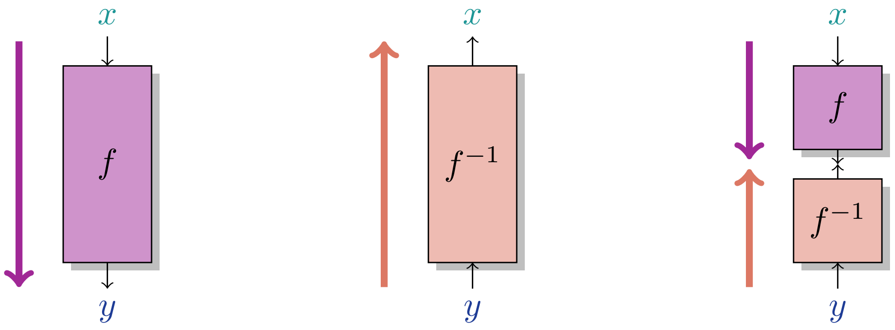


Figure 6: *Evaluation*



(a) *Check if $y = f(x)$.*

(b) *Check if $x = f^{-1}(y)$.*

(c) *Intermediate checking.*

Figure 7: *Verification*

Contributions

In this manuscript, we contribute to a better understanding of these new primitives from several perspectives. In particular, we offer other directions for designing these primitives, searching for more mathematical notions like CCZ equivalence. More importantly, while primitives continue to appear attempting at breaking speed records, we contribute to cryptanalysis by suggesting both practical and theoretical attacks. Indeed, although many Arithmetization-Oriented primitives have been proposed, very few security analyses have been carried out. The aim of this manuscript is therefore first and foremost to help fill this gap in order to better understand the specific features of these new tools. Getting a deeper insight into the cryptanalysis techniques that can threaten such primitives requires revisiting known techniques as well as studying new ones.

We first give, in Chapter 1, some context, mathematical background and a brief state of the art of the new primitives. Chapters 2 and 3 are then dedicated to the design of `Anemoi`, a new family of hash functions offering very good performance for Zero-Knowledge Proofs systems. From a theoretical point of view, `Anemoi` significantly improves the understanding of the design principles involved in the constructions of these new primitives. Indeed, its main component, the `Flystel`, is exploiting a previously unknown link between CCZ-equivalence and Arithmetization-Orientation.

Then, in Chapter 4, we study the resistance of some primitives to algebraic attacks. Such security analysis was first motivated by some cryptanalysis challenges proposed by the Ethereum fundation in November 2021. Finally, in Chapters 5 and 6 we study the algebraic degree of iterated power functions, with a focus on the MiMC block cipher. Our careful analysis of the MiMC block cipher is one of the first to provide such a detailed understanding of the evolution of the algebraic degree of such primitives. Our method is mainly based on a better understanding of the univariate polynomial representation of such a cipher, showing that, for some instances, polynomials are very sparse. Following this work, in Chapter 7 we aim at answering various open problems that would be raised by such a study of the algebraic degree. Although some questions are still open, at the time of writing, they are worthwhile suggestions for future work in these different directions.

In Figure 8 we summarize the plan of this thesis and the interconnection of the different chapters.

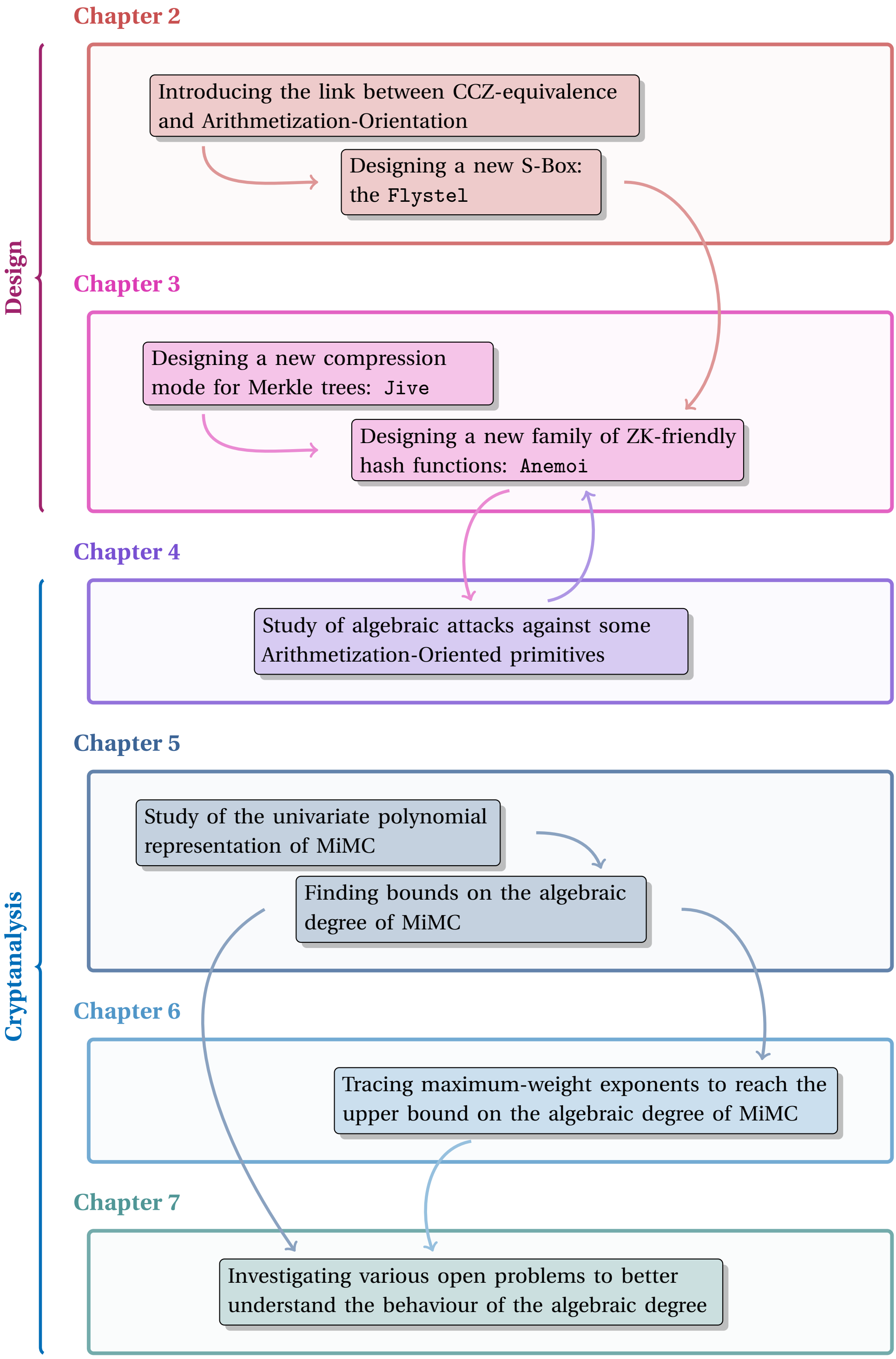

Chapter 2
Introducing the link between CCZ-equivalence and Arithmetization-Orientation
Designing a new S-Box: the Flystel
Design
Chapter 3
Designing a new compression mode for Merkle trees: Jive
Designing a new family of ZK-friendly hash functions: Anemoi
Chapter 4
Study of algebraic attacks against some Arithmetization-Oriented primitives
Cryptanalysis
Chapter 5
Study of the univariate polynomial representation of MiMC
Finding bounds on the algebraic degree of MiMC
Chapter 6
Tracing maximum-weight exponents to reach the upper bound on the algebraic degree of MiMC
Chapter 7
Investigating various open problems to better understand the behaviour of the algebraic degree

Figure 8: *Overview of this thesis.*

Publications

Journals

[Bar+22] Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, and Léo Perrin. “Algebraic attacks against some arithmetization-oriented primitives”. In: *IACR Trans. Symm. Cryptol.* (2022), pp. 73–101 (cit. on pp. 83, 307).

[BCP23] Clémence Bouvier, Anne Canteaut, and Léo Perrin. “On the algebraic degree of iterated power functions”. In: *Designs, Codes and Cryptography* (2023), pp. 997–1033 (cit. on pp. 107, 108, 310).

Conferences with proceedings

[Bou+23] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. “New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode”. In: *CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. LNCS. Springer, 2023, pp. 507–539 (cit. on pp. 17, 31, 54, 65, 67, 79, 101, 306).

[Liu+23b] Fukang Liu, Lorenzo Grassi, Clémence Bouvier, Willi Meier, and Takanori Isobe. “Coefficient Grouping for Complex Affine Layers”. In: *CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. LNCS. Springer, 2023, pp. 540–572 (cit. on pp. 217, 218, 220, 222, 224, 227, 310).

Conferences

[Bou22a] Clémence Bouvier. *New Approach for Arithmetization-Oriented Symmetric Primitives.* CrossFyre Workshop. Passau, Germany. https://crossfyre22.github.io/docs/Bouvier.pdf. Oct. 2022.

[Bou22b] Clémence Bouvier. *On the Algebraic Degree of Iterated Power Functions.* WCC - Workshop on Coding and Cryptography. Virtual (Rostock, Germany). https://www.wcc2022.uni-rostock.de/storages/uni-rostock/Tagungen/WCC2022/Papers/WCC_2022_paper_47.pdf. Mar. 2022.

[BW22] Clémence Bouvier and Danny Willems. *Anemoi and Jive : New Arithmetization-Oriented tools for Plonk-based applications.* ZKProof5 - Zero-Knowledge Proofs. Tel Aviv, Israel. https://youtu.be/3EdbLiClFPI. Nov. 2022.

[Bou23] Clémence Bouvier. *Iterated Power Functions: from Univariate Polynomial Representation to Multivariate Degree.* Fq15 - International Conference on Finite Fields and Their Applications. Aubervilliers, France. https://org.uib.no/selmer/fq15/abstracts.pdf. June 2023 (cit. on p. 107).

Acronyms and notation

Acronyms

AIR	Algebraic Intermediate Representation
ANF	Algebraic Normal Form
AO	Arithmetization-Oriented
APN	Almost Perfect Non-linear
CICO	Constrained Input Constrained Output
DDT	Difference Distribution Table
FHE	Fully Homomorphic Encryption
LAT	Linear Approximation Table
MPC	Multi-Party Computation
PHT	Pseudo-Hadamard Transform
R1CS	Rank-1 Constraint System
SNARK	Succinct Non-interactive ARgument of Knowledge
SPN	Substitution Permutation Network
STARK	Succinct Transparent ARgument of Knowledge
ZK	Zero-Knowledge

Notation

$\mathbb{F}_2^n$	Vectorial space with dimension n
$\mathbb{F}_q$	Finite fields with q elements, where q is any power of a prime number
$a \oplus b$	addition of a and b in a field of even characteristic
$a \boxplus b$	addition of a and b in a field of odd characteristic
$[\![a, b]\!]$	The integers in the interval $[a, b]$
wt	Hamming weight
$\deg^a$	Algebraic degree
$\deg^u$	Univariate degree
$\langle a, b\rangle$	Scalar product between a and b
Γ_F	Graph of the function F

CHAPTER 1
A new type of primitives

The number of the so-called Arithmetization-Oriented primitives, and more generally the number of symmetric primitives defined over large finite fields, has grown quite rapidly in the past few years. In this chapter, we aim at better understanding the specific features of these primitives both in terms of design and cryptanalysis. In particular, one of the key issues is to identify how these primitives differ from the classical ones, or in other words, why classical primitives are inappropriate in these new contexts. More generally, we will define the main concepts that will be studied throughout this thesis.

In Section 1.1, we will first review some important mathematical concepts that will be used throughout this manuscript. Then, in Section 1.2, we will recall some classical design principles usually used in symmetric cryptography (i.e. not influenced by the advanced protocols). In Section 1.3 we will present some cryptanalysis techniques commonly used for classical primitives and that have also been suggested to evaluate the security of those emerging primitives. Moving to the new context, we will describe, in Section 1.4, new systems of constraints introduced by advanced protocols. More specifically, we will present constraints systems for Zero-Knowledge Proofs. This will allow us to understand the principles that have governed the design of new primitives, defined over large finite fields. We will give a brief overview of some primitives that have been proposed in Section 1.5, with a particular focus on Arithmetization-Oriented primitives.

Contents

1.1 Mathematical background

In this section we review some of the fundamental concepts needed to understand the main contributions in this manuscript. In particular we recall some important definitions and properties of finite fields. Throughout this manuscript, we will mainly work over finite fields of size q denoted $\mathbb{F}_q$, where q is often a prime number p or a power of 2. It is sometimes useful to identify the 2^n elements of the finite field $\mathbb{F}_{2^n}$, with the elements of the vectorial space $\mathbb{F}_2^n$.

First, let us focus on some properties of Boolean functions.

Definition 1.1. A Boolean function with n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2 = \{0, 1\}$.

The coordinates of a vectorial function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are the m Boolean functions F_i for $1 \leqslant i \leqslant m$ such that, for all x, $F(x) = (F_1(x), \ldots, F_n(x))$. The algebraic degree of F is then defined from the algebraic degrees of its coordinates as follows.

Definition 1.2 (ANF and Algebraic Degree)**.** Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Its *Algebraic Normal Form (ANF)* is the representation of f as a multivariate polynomial with variables in $\mathbb{F}_2[x_0, \ldots, x_{n-1}]/(x_0^2 + x_0, \ldots, x_{n-1}^2 + x_{n-1}]$, so that

$$f(x_0, ..., x_{n-1}) = \sum_{u \in \mathbb{F}_2^n} a_u x^u ,$$

where $a_u \in \mathbb{F}_2$ for all u, and $x^u = \prod_{i=0}^{n-1} x_i^{u_i}$. The *algebraic degree* of f is

$$\deg^a f = \max \left\{ \mathrm{wt}(u) : u \in \mathbb{F}_2^n, a_u \neq 0 \right\} ,$$

where $\mathrm{wt}(u)$ is the Hamming weight of u. If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, then its algebraic degree, $\deg^a F$, is the maximal algebraic degree of the coordinates of F.

The algebraic degree should not be confused with the *univariate degree*, which is defined for any function $F : \mathbb{F}_q \to \mathbb{F}_q$.

Definition 1.3 (Univariate Representation and Degree)**.** Let q be a prime power and let F be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$. Then the *univariate polynomial representation* of F is

$$F(x) = \sum_{i=0}^{q-1} \alpha_i x^i ,$$

where $\alpha_i \in \mathbb{F}_q$ for all integers i. Its *univariate degree* $\deg^u F$ is the largest integer i for which $\alpha_i \neq 0$.

If $q = 2^n$, then a function $F : \mathbb{F}_q \to \mathbb{F}_q$ can be seen both as a function defined over the finite field, and as a function defined over the vector space $\mathbb{F}_2^n$ using a simple isomorphism between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$. For such a function, the algebraic and univariate degrees are different quantities that are related as follows [Cha13, Page 254]:

$$\deg^a F = \max\{\mathrm{wt}(i) : i \in \mathbb{N}, \alpha_i \neq 0\} ,$$

where $\{\alpha_i, i \geqslant 0\}$ is the set of all coefficients in the univariate representation of F.

Example 1.1. Let F be the function from $\mathbb{F}_2^3$ to $\mathbb{F}_2^3$ defined by $F(x) = x^3$. F is given in its univariate form, so the algebraic degree of F is $\deg^a(F) = \mathrm{wt}(3) = 2$.

Let us notice that the Algebraic Normal Form of F is the following:

$$\begin{aligned}(f_0, f_1, f_2) &= (x_0 + x_1x_2 + x_1 + x_2, x_0x_1 + x_0x_2 + x_1, x_0x_1 + x_2)\\ &= \Big(x^{(1,0,0)} + x^{(0,1,1)} + x^{(0,1,0)} + x^{(0,0,1)},\\ &\quad x^{(1,1,0)} + x^{(1,0,1)} + x^{(0,1,0)},\\ &\quad x^{(1,1,0)} + x^{(0,0,1)}\Big)\ ,\end{aligned}$$

implying that we can also check that the algebraic degree of F is 2 by looking at the algebraic degree of f_0, f_1 and f_2. Each of these Boolean functions has algebraic degree 2.

The Walsh transform is also a good tool to study Boolean functions as we will see in Section 1.3.1.2 concerning linear cryptanalysis.

Definition 1.4. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a Boolean function with n variables. Then the Walsh transform of F is the function $\mathcal{W}_F : \mathbb{F}_2^n \to \mathbb{Z}$ such that

$$\mathcal{W}_F(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a\cdot x + F(x)}\ .$$

Note that a similar definition can be obtained for fields of larger characteristic, involving complex numbers.

Definition 1.5. Let $F : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a function with $q > 2$. Then the Walsh transform of F is the function $\mathcal{W}_F : \mathbb{F}_q^m \to \mathbb{R}$ such that

$$\mathcal{W}_F(a) = \sum_{x \in \mathbb{F}_q^m} \exp\left(\frac{2\pi i(\langle a, x\rangle - F(x))}{q}\right)\ ,$$

where $\langle a, x\rangle$ denotes the scalar product between a and x.

1.2 Classical symmetric primitives

1.2.1 Stream and block ciphers

Symmetric ciphers are divided into two categories: stream ciphers and block ciphers. In this thesis, we will focus on the latter.

1.2.1.1 Stream ciphers

The Vernam cipher [Ver26], also known as the *one-time pad*, is the starting point for stream ciphers. The Vernam cipher leads to perfect secrecy by using the XOR operation to combine bits of the plaintext with bits of the key. This key must be as long as the message, random and used only once, making the Vernam encryption cumbersome. However, such requirements can be released for real life since we are relying on computational security.

Then, stream ciphers solve this problem by combining plaintext digits with a keystream, produced by a pseudo-random generator. In a stream cipher, each digit of the plaintext is encrypted one by one with the corresponding digit of the keystream to produce one digit of the ciphertext stream. More precisely, an initialisation procedure determines the initial state of the generator from the secret key K and a public initialisation vector IV. Then, for each bit or each digit s_i of the keystream, the internal state is updated by the function ϕ_i and a filtering function f is applied as described in Figure 1.1.

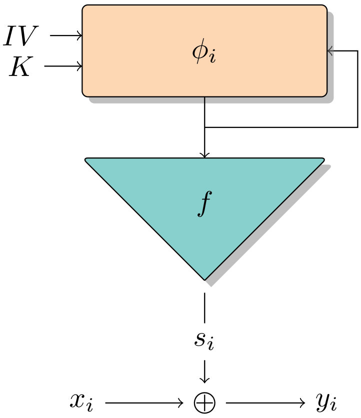
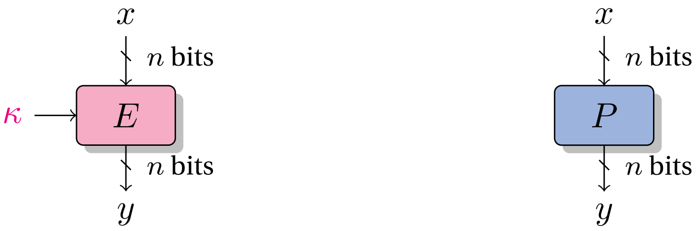


Figure 1.1: General representation of a stream cipher.

1.2.1.2 Block ciphers

While the size of the plaintext can be arbitrary for a stream cipher, it is fixed for a block cipher. A block cipher E_κ is a family of permutations, taking a key κ of k bits as parameter. E_κ takes as input an n-bit block x and returns an encrypted message y of the same size as the input message. In Figure 1.2 we compare the construction of a block cipher with a random permutation.



(a) *Block cipher* **(b)** *Random permutation*

Figure 1.2: Comparison between a block cipher and a random permutation.

For implementation reasons, a block cipher is usually built by iterating a round function as described in Figure 1.3. This process is repeated r times, where r is chosen such that it offers a good security margin, and efficiency when evaluating the function. Sub-keys might optionally be derived from a key schedule algorithm applied to the master key. Then E_κ can be written as the composition of the round functions:

$$y = E_\kappa(x) = F_{\kappa_r} \circ \dots F_{\kappa_1}(x) \,.$$

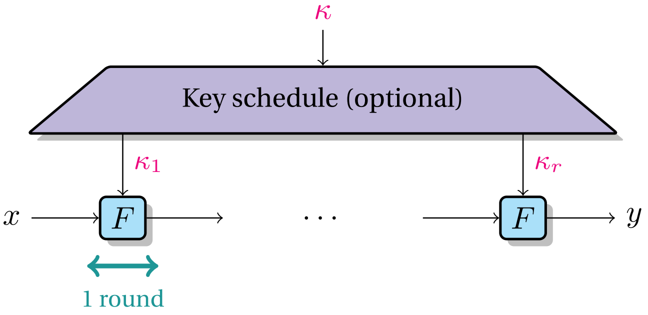


Figure 1.3: *Iterated construction.*

To study the security of block ciphers, we need to check that the number of rounds and the sizes of the blocks and of the key have been well-chosen by the designers. More precisely, a block cipher is said to be secure if E_κ, with a randomly chosen key, is indistinguishable from a random permutation.

Definition 1.6. A *distinguisher* is any property that should not be expected from an ideal object.

Here the ideal object would be a permutation picked uniformly at random from the set of all permutations of $\mathbb{F}_2^n$. The existence of a distinguisher is an undesirable property for a cryptographic primitive. Indeed, block ciphers can be seen as a family of 2^k permutations of n bits, and the choice of a key κ then corresponds to the choice of a permutation in that family. However, for a random permutation, there is no link between the input and the output, and the ciphertext therefore reveals no information about the plaintext.

Each round in the iterated construction must bring some confusion and diffusion as introduced by Shannon [Sha49]. The confusion is used to make the cryptanalysis harder, so that changing the input has unpredictable effect on the output, while the diffusion is used to spread this hardness, so that changing a few entries in the input changes many entries in the output. Different constructions can be used as round functions, but in this thesis we will mainly deal with Feistel networks and Substitution Permutation Networks (SPN).

In a Feistel network, the input x of size n bits is divided into two parts, each of size $n/2$ bits: the left part x_L and the right part x_R. Then the round function of a Feistel network works as follows:

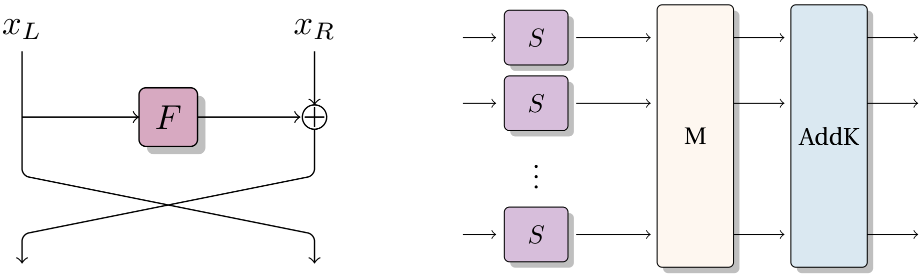
$$(x_L, x_R) = (F(x_L) \oplus x_R, x_L)\,.$$

We describe the round function of such a construction in Figure 1.4a.

One of the best known Feistel cipher is the *Data Encryption Standard* (DES) [Nat77], which uses 56-bit keys. However, it is no longer used because of its small key space, allowing a systematic attack in a reasonable amount of time.

An SPN is composed of three components: an S-box layer S, a diffusion layer M and a sub-key addition K. One round of SPN construction is represented in Figure 1.4b.

The most widely used block cipher is the *Advanced Encryption Standard* (AES) [DR02], which allows 128-bit blocks to be encrypted with keys of size 128, 192 or 256 bits. It is the best-known symmetric encryption, considered to be the most secure in the community.



(a) A Feistel round function.

(b) An SPN round function.

Figure 1.4: *Feistel and SPN round functions.*

1.2.2 Hash functions

Since no key is involved in hash functions, they should neither belong to symmetric cryptographic primitives, nor to asymmetric cryptographic primitives. However, hash functions share some design and cryptanalysis principles with symmetric cryptography so they are often classified as such primitives.

As described in Figure 1.5, a hash function H maps an input x of arbitrary length to an output y of fixed length n. This output y is often called the digest.

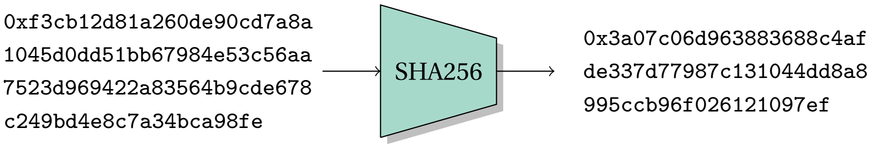


Figure 1.5: *Example of SHA256 hash.*

A hash function must satisfy some properties, like collision-resistance and first-preimage and second-preimage resistance. A collision happens if we find a pair of distinct messages $x_1 \neq x_2$ such that $H(x_1) = H(x_2)$. While collisions obviously exist, we say that a hash function is collision-resistant if it is difficult to find such a collision in practice. Then, the preimage resistance corresponds to the difficulty to find a message $x \in \mathbb{F}_2^n$ such that $H(x) = y$ for a given challenge $y \in \mathbb{F}_2^n$. Similarly, the second-preimage resistance works as follows: given $x_1 \in \mathbb{F}_2^*$, it must be infeasible to find $x_2 \neq x_1$ such that $H(x_1) = H(x_2)$.

There exist different constructions for hash functions. The first one was proposed, independently, by Merkle [Mer90] and Damgård [Dam90]. The structure relies on a compression function iterated as many times as there are message blocks. The Merkle-Damgård construction is depicted in Figure 1.6.

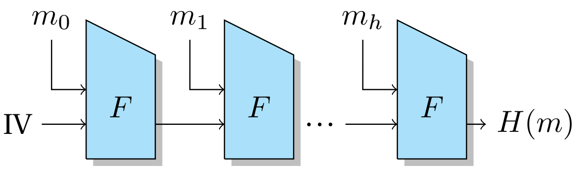


Figure 1.6: *Merkle-Damgård construction.*

We can cite SHA-1 [Nat95] or SHA-2 [Nat22] family to name a few. The advantage of such a construction is that studying the security of the entire hash function is reduced to studying the security of the compression function.

Another construction, that we will use in this thesis, is the sponge construction. This mode was introduced in 2007 by Guido Bertoni *et al.* in [Ber+07]. The sponge construction is parameterized by two integers: the rate r and the capacity c, so that $r + c$ is equal to the width of the permutation. For a well-chosen permutation, the capacity must give the security level of the hash function. A sponge is decomposed into two phases: *absorption* and *squeezing*. During absorption, the first r bits of the state are xored to a block of the padded message, so that each time a block of message is added, the permutation is applied to the full state. Then, squeezing consists in extracting blocks of messages, by applying the permutation each time a block of message is produced. We describe this construction in Figure 3.1. More details will be given in Section 3.1.1.

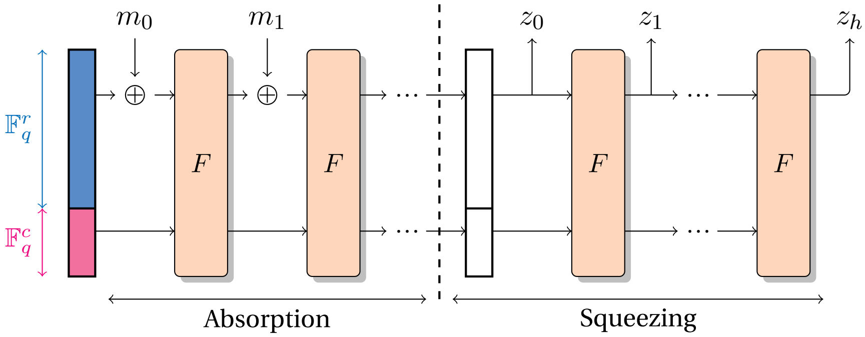


Figure 1.7: *Hash function in sponge mode.*

1.3 Overview of some cryptanalysis techniques

1.3.1 Statistical Attacks

In this section, we first introduce differential and linear attacks. Such attacks are called statistical attacks since they exploit a statistical bias in the cipher, compared to the behaviour of a random permutation. For differential cryptanalysis, this behaviour corresponds to a statistical bias in the distribution of differences observed at the output of the cipher when the input difference between two plaintexts is fixed. In the case of linear cryptanalysis, it corresponds to a biased linear relation between the plaintext, the ciphertext and the key.

1.3.1.1 Differential Cryptanalysis

Differential attacks exploit the differences between two or more plaintext inputs and their corresponding ciphertext outputs. They have been introduced in 1990 by Biham, and Shamir [BS91]. Widely used to evaluate the security of block and stream ciphers, differential cryptanalysis is then particularly efficient in the analysis of symmetric primitives. By analyzing the differences between the two plaintexts and between the corresponding ciphertexts, an attacker can identify patterns in the encryption process that reveal information about the key used to encrypt the data. More precisely, to evaluate the resistance of a cipher to differential attacks, it is important to know the

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	13	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	0	2	0	2	0	0	2	1	2	0	0
2	0	0	1	0	2	2	4	0	2	2	0	0	0
3	0	2	0	1	0	0	2	2	0	4	0	0	2
4	0	0	2	0	2	0	0	0	0	2	4	2	1
5	0	2	2	0	0	4	1	0	0	0	0	2	2
6	0	0	4	2	0	1	2	2	0	0	2	0	0
7	0	0	0	2	0	0	2	2	1	0	2	4	0
8	0	2	2	0	0	0	0	1	4	0	0	2	2
9	0	1	2	4	2	0	0	0	0	2	0	2	0
10	0	2	0	0	4	0	2	2	0	0	1	0	2
11	0	0	0	0	2	2	0	4	2	2	0	1	0
12	0	0	0	2	1	2	0	0	2	0	2	0	4

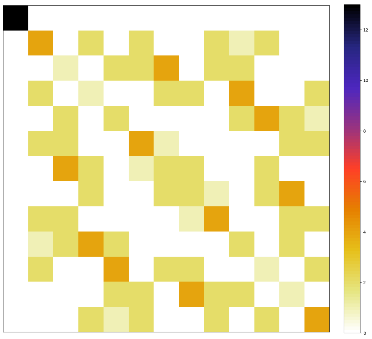


Figure 1.8: Representations of the DDT for $F(x) = x^5$ in $\mathbb{F}_{13}$.

highest probability that a pair of input-output differences $(\Delta_{\text{in}}, \Delta_{\text{out}})$ appear. This property is summarized in a Difference Distribution Table.

Definition 1.7 (DDT and Differential Uniformity)**.** Let $F : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a function, and $\Delta_{\text{in}}, \Delta_{\text{out}}$ be elements of $\mathbb{F}_q^m$. The *Difference Distribution Table* (DDT) collects the number of solutions of the equation

$$F(x + \Delta_{\text{in}}) - F(x) = \Delta_{\text{out}}$$

for each given pair of difference $(\Delta_{\text{in}}, \Delta_{\text{out}})$.

$$\text{DDT}_F[\Delta_{\text{in}}, \Delta_{\text{out}}] = \#\{x \in \mathbb{F}_q^m, F(x + \Delta_{\text{in}}) - F(x) = \Delta_{\text{out}}\} .$$

The maximum value in the DDT, δ_F, is called the *differential uniformity*

$$\delta_F = \max_{\Delta_{\text{in}} \neq 0, \Delta_{\text{out}}} \#\{F(x + \Delta_{\text{in}}) - F(x) = \Delta_{\text{out}}\} .$$

As a consequence, the lower the differential uniformity is, the more resistant the cipher is against differential attacks.

In order to better understand some patterns in the DDT of a function, we can represent it with figures, where the intensity of the color reveals the number of solutions to the equation. In Figure 1.8 we give an example of the representations of the DDT for $F(x) = x^5$ in $\mathbb{F}_{13}$.

As already mentioned, functions with low differential uniformity have good cryptographic properties. In particular, if the differential uniformity is equal to 2, which is the smallest value that can be achieved in characteristic 2, we say that the function is Almost Perfect Non-linear (APN).

Differential cryptanalysis therefore studies the propagation of differences through an iterated construction. However, in practice, it is very difficult to calculate the probability of a differential over several rounds of the encryption scheme. Instead, it is more appropriate to look at *differential trails*, i.e. to specify the evolution of the difference, round after round. In order to be able to calculate a theoretical probability, we usually assume that the average probability of a differential trail is equal to the product of the probabilities of the differentials over each round. This hypothesis is motivated by the fact that the additions of the round keys tend to make the rounds independent. But it does not hold in all cases [BR22].

1.3.1.2 Linear Cryptanalysis

Linear attacks [TG92; Mat94] exploit *biased* linear relations between plaintext inputs and their corresponding ciphertext outputs. This property is summarized in a Linear Approximation Table.

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	13.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1	0.0	0.3	4.0	7.8	1.1	3.0	1.1	1.1	3.0	5.6	4.0	4.0	3.0
2	0.0	4.0	5.6	1.1	3.0	7.8	0.3	3.0	4.0	3.0	1.1	1.1	4.0
3	0.0	7.8	1.1	5.6	3.0	4.0	3.0	3.0	4.0	0.3	1.1	1.1	4.0
4	0.0	1.1	3.0	3.0	7.8	1.1	4.0	4.0	1.1	4.0	0.3	3.0	5.6
5	0.0	2.9	7.8	4.0	1.1	0.3	5.6	1.1	3.0	1.1	4.0	4.0	3.0
6	0.0	1.1	0.3	3.0	4.0	5.6	7.8	4.0	1.1	4.0	3.0	3.0	1.1
7	0.0	1.1	3.0	3.0	4.0	1.1	4.0	7.8	5.6	4.0	3.0	0.3	1.1
8	0.0	2.9	4.0	4.0	1.1	3.0	1.1	5.6	0.3	1.1	4.0	7.8	3.0
9	0.0	5.6	3.0	0.3	4.0	1.1	4.0	4.0	1.1	7.8	3.0	3.0	1.1
10	0.0	4.0	1.1	1.1	0.3	4.0	3.0	3.0	4.0	3.0	5.6	1.1	7.8
11	0.0	4.0	1.1	1.1	3.0	4.0	3.0	0.3	7.8	3.0	1.1	5.6	4.0
12	0.0	3.0	4.0	4.0	5.6	3.0	1.1	1.1	3.0	1.1	7.8	4.0	0.3

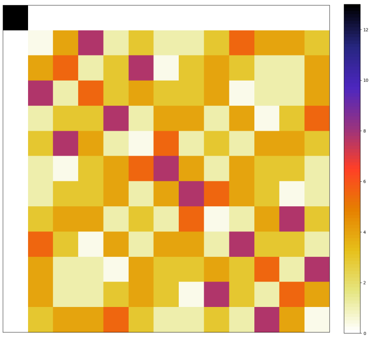


Figure 1.9: Representations of the module of the coefficients in the LAT for $F(x) = x^5$ in $\mathbb{F}_{13}$.

Definition 1.8 (LAT and Linearity). Let $F : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m$ be a function, and a, b be elements of $\mathbb{F}_q$. The *Linear Approximation Table* (LAT) is a table defined by

$$\mathrm{LAT}_F[a,b] = \begin{cases} \displaystyle\sum_{x \in \mathbb{F}_2^m} (-1)^{a \cdot x + b \cdot F(x)} & \text{if } q = 2\,, \\ \displaystyle\sum_{x \in \mathbb{F}_q^m} \exp\left(\frac{2\pi i(\langle a, x\rangle - \langle b, F(x)\rangle)}{q}\right) & \text{if } q > 2\,. \end{cases}$$

The vectors a and b are called input and output masks, respectively, and the coefficients in the LAT are also known as *Walsh coefficients* as defined in Section 1.1. The module of the highest coefficient, $\mathcal{L}_F$, is called the *linearity*

$$\mathcal{L}_F = \max_{a,b \neq 0} |\mathrm{LAT}_F[a,b]| \ .$$

As for differential attacks, we have that the lower the linearity is, the more resistant the cipher is against linear attacks.

For given input mask a and output mask b, if the value in the LAT is 0, then the associated approximation shows no correlation. More generally, the LAT gives scaled versions of bias and correlation for every pair of input and output masks. In particular, a relevant quantity to evaluate the resistance of a cipher to linear attacks is the *bias*, that is the quantity by which the probability that a linear expression holds deviates from $1/2$. Indeed, if the relation is seen as a random variable, the probability that it is equal to 0 is significantly different from $1/2$.

Moreover, as for the DDT, we can sometimes better understand some patterns in the LAT of a function by representing this table in a figure, where the intensity of the color reveals how high the absolute value of the coefficients are. In Figure 1.9, we give an example of the representations of the module of the coefficients in the LAT for $F(x) = x^5$ in $\mathbb{F}_{13}$.

Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, then the DDT and LAT are linked as follows:

$$\begin{aligned} \mathrm{LAT}_F[a,b]^2 &= \sum_{\Delta_{\mathrm{in}} \in \mathbb{F}_2^n} \sum_{\Delta_{\mathrm{out}} \in \mathbb{F}_2^m} (-1)^{\Delta_{\mathrm{in}} \cdot a + \Delta_{\mathrm{out}} \cdot b}\, \mathrm{DDT}_F[\Delta_{\mathrm{in}}, \Delta_{\mathrm{out}}] \\ \mathrm{DDT}_F[\Delta_{\mathrm{in}}, \Delta_{\mathrm{out}}] &= 2^{-(n+m)} \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^m} (-1)^{\Delta_{\mathrm{in}} \cdot a + \Delta_{\mathrm{out}} \cdot b}\, \mathrm{LAT}_F[a,b]^2 \,. \end{aligned}$$

1.3.2 Higher-Order Differential Cryptanalysis

The complexity of so-called *higher-order differential attacks* [Knu95] decreases with the algebraic degree (defined in Section 1.1), implying that it is important to understand how this quantity increases as a given round function is iterated.

Indeed, a distinguisher can be exhibited using the following proposition.

Proposition 1.1 ([Lai94]). *For any function* $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *and any affine subspace* $\mathcal{V} \subset \mathbb{F}_2^n$*, such that* $\dim \mathcal{V} \geqslant \deg^a(F) + 1$*, we have:*

$$\bigoplus_{x \in \mathcal{V}} F(x) = 0.$$

Such a sum corresponds to the value of a differential of order $\dim \mathcal{V}$. Since a permutation randomly selected among all permutations of $\mathbb{F}_2^n$ has algebraic degree $(n-1)$ with a high probability (see e.g. [Wel69; Das02; KP02]), an iterated cipher needs to have enough rounds to reach the maximal algebraic degree in order to be indistinguishable from a random permutation. We refer to such a distinguisher as *zero-sum distinguisher.*

In Chapter 5 and 6 we will investigate the security of the block cipher MiMC [Alb+16] against such attacks.

1.3.3 Invariant attacks

Invariant attacks take advantage of an undesirable structural property of the encryption scheme, due to the preservation of a partition $(A, \mathbb{F}_q^m \backslash A)$ of $\mathbb{F}_q^m$ after applying the encryption function.

Definition 1.9. Let $F : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a permutation, and A a subset of $\mathbb{F}_q^m$. A is an *invariant for* F if the partition $(A, \mathbb{F}_q^m \backslash A)$ is preserved by F.

It follows from the definition that the empty set $\varnothing$ and the entire set $\mathbb{F}_q^m$ are trivial invariants. The particular case where A is an affine subspace $\mathbb{F}_q^m$ corresponds to invariant subspace attacks. Such attacks have been introduced by Leander *et al.* in 2011 [Lea+11]. Non-linear invariant attacks have then been introduced by Todo *et al.* in 2019 [TLS19].

Example 1.2. As a simple example, let us consider, a function $F : \mathbb{F}_q^2 \to \mathbb{F}_q^2$, so that $F(x, y) = (x^{q-2}y, y)$. Then, we easily notice that we have $F(0, y) = (0, y)$. It follows that the subspace $\{(0, y), y \in \mathbb{F}_q\}$ is an invariant for F.

Therefore, given a block cipher E_k, keys for which A is an invariant for E_k are weak keys with respect to invariant attacks. If a weak key is used for a block cipher, then, by exploiting the existence of an invariant, an attacker is able to distinguish the block cipher from a random permutation.

1.3.4 Algebraic Cryptanalysis

Algebraic attacks [CP02] consist in exploiting an algebraic relationship between the plaintext, the ciphertext and the key. Algebraic attacks are particularly effective against ciphers that have a low algebraic degree, which means that the encryption process can be described using algebraic equations of low degree. Indeed, in order to recover the key more quickly than an exhaustive search, the aim is to find sufficiently simple relations to build a polynomial system of equations in the key. This system must be reasonably easy to solve, meaning that it is of low degree, or of small size, or very structured.

One of the main questions concerning systems of polynomial equations is the search for solutions to this system. The complexity of this search highly depends on the form of the polynomial system as we will see in Chapter 4.

As previously explained, Arithmetization-Oriented primitives are designed such that they can be represented by low degree polynomials. This obviously raises the question of their resistance to algebraic attacks. Such attacks are actually considered to be the weakest points of these primitives, and are generally those that govern the number of rounds performed by these primitives. In Chapter 4 we will investigate the security of some Arithmetization-Orientation primitives against algebraic attacks, with a focus on the resolution of the CICO (Constrained Input Constrained Output) problem that we will introduce later.

1.4 Advanced protocols

In this thesis we will mainly discuss Arithmetization-Oriented primitives, i.e. primitives that have been designed for Zero-Knowledge Proofs systems. There are many different constraint systems for such proofs. As these systems are not the main focus of this thesis, we have chosen to briefly introduce some of them only, which will be used in particular to evaluate the performance of `Anemoi` in Chapter 3.

1.4.1 A new context

Recently, new integrity proofs have appeared such as zk-SNARK protocols, like Groth16 [Gro16], developed in the Zcash cryptocurrency or the zk-STARK StarkWare deployed in the Ethereum blockchain. SNARKs (Succinct Non-interactive ARgument of Knowledge) [Ben+13] and STARKs (Succinct Transparent ARgument of Knowledge) [Ben+18] are cryptographic primitives allowing the verification of the integrity of computations. In a client-server model, when a client with low computational power delegates a task to a server with high computational power, they allow the client to efficiently verify whether the server has executed the requested task. These proofs can be verified quickly. In the SNARK acronym, "Non-interactive" means that an interactive protocol is compiled to obtain a non-interactive protocol (NI). If this non-interactive protocol is succinct, then it is a SNARK, but it is worth mentioning that STARKs can also be compiled to be non-interactive. In the STARK acronym, "Transparent" means that the system does not require initial trust configuration. Furthermore, it is also interesting to note that while STARKs are assumed to be post-quantum, traditional SNARKs are based on couplings or elliptic curves.

SNARKs and STARKs can be equipped with a zero-knowledge property, being then referred to as zk-SNARKs and zk-STARKs. Since Zero-Knowledge Proofs allow "a prover" to prove to another individual that a statement is true, without disclosing any information other than the validity of the statement, the goal is to reveal as little data as possible between the two parties. In particular, ZKPs use arithmetic circuits.Arithmetization consists in reducing computational problems to algebraic problems involving "low degree" polynomials over a finite field.

More precisely, these protocols have put forward the need to optimize the multiplicative complexity of their circuits, and notably the algebraic description of encryption schemes or hash functions. This implies that the proposed constructions use non-linear functions, but whose algebraic representations remain very simple on a large finite field, such as a sparse polynomial of $\mathbb{F}_q[X]$. Such design principles correspond to the opposite of what is usually proposed in symmetric cryptography. Indeed, while classical symmetric primitives (such as AES) use operations on small fields $\mathbb{F}_{2^n}$ where n is of the order of 4 or 8, these new primitives use operations on a large finite field $\mathbb{F}_q$ where q is either a large prime integer or a power of 2, greater than 2^{128}. Large finite fields are usually given by the scalar field of elliptic curves, while FRI-based (Fast Reed—Solomon Interactive Oracle Proofs of Proximity) protocols use fields of size 64 or 32 bits. Some examples of prime integers used for such applications are given in Table 1.1.

Origin	$\log_2 p$	p
Mersenne field	31	$2^{31} - 1 =$ `0x7fffffff`
Goldilocks field	64	$2^{64} - 2^{32} + 1 =$ `0xffffffff00000001`
Scalar field of BLS12-377	253	`0x12ab655e9a2ca55660b44d1e5c37b00159aa76fed00000010a11800000000001`
Scalar field of BN-254	254	`0x30644e72e131a029b85045b68181585d2833e84879b9709143e1f593f0000001`
Scalar field of BLS12-381	255	`0x73eda753299d7d483339d80809a1d80553bda402fffe5bfeffffffff00000001`

Table 1.1: Examples of prime integers p used in ZKP.

1.4.2 Some examples of constraints systems

As already mentioned, arithmetic circuits are common models to study the complexity of computing polynomials. In this section we will see that gates do not play the same role in the different constraints systems.

1.4.2.1 Rank-1 Constraint System

R1CS [Ben+13] stands for Rank-1 Constraint System. Bulletproof [Bün+18] or Groth16 [Gro16], for example, rely on this system of constraints. The specificity of R1CS is that the verification corresponds to the evaluation of an arithmetic circuit such that affine gates are free. Then, computing R1CS constraints actually means that we need to determine the number of multiplications needed. The R1CS cost is indeed proportional to the total number of multiplications.

Example 1.3. First, let us consider the following equation and investigate the number of R1CS constraints:

$$y = (ax + b)^3(cx + d) + ex \, ,$$

where a, b, c, d and e are constants. Let us first decompose this equation into additions, multiplications and scalar multiplications so that enforcing this equation could be done with the following operations:

$$\begin{array}{llllllll}
t_0 & = a \cdot x & & t_3 & = t_2 \times t_1 & \textit{(+1)} & t_6 & = t_3 \times t_5 \quad \textit{(+1)} \\
t_1 & = t_0 + b & & t_4 & = c \cdot x & & t_7 & = e \cdot x \\
t_2 & = t_1 \times t_1 & \textit{(+1)} & t_5 & = t_4 + d & & t_8 & = t_6 + t_7
\end{array}$$

Counting the number of multiplication, we deduce that we have 3 constraints.

Example 1.4. Let us now consider the following equation

$$y = x^7 \, .$$

Then, let us compute the number of R1CS constraints.

$$\begin{array}{llllll}
t_0 & = x \times x & \textit{(+1)} & t_2 & = t_1 \times t_1 & \textit{(+1)} \\
t_1 & = t_0 \times x & \textit{(+1)} & t_3 & = t_2 \times x & \textit{(+1)}
\end{array}$$

There are 4 multiplications, implying that we have 4 constraints.

It is interesting to see with those two examples that a function that might look more sophisticated actually allows a more efficient implementation within an R1CS system because of its lower number of multiplications. The aim to design an R1CS-friendly primitive is then to decrease the number of such multiplications.

1.4.2.2 PlonK

PlonK[1] [GWC19] is an acronym meaning Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. Compared to R1CS, the PlonK proof system is more flexible, opening the door to more possibilities for defining the same relationship with constraints. In particular, this implies that additions have a cost. As a consequence, the total number of operations, both linear and non-linear, must be limited to ensure good performances.

Let us briefly describe how the proof system works. Given a certain program P, we first need to convert it into an arithmetic circuit, and then into a constraint system. There exist two types of constraints on the circuit wires: gate constraints and copy constraints. In the following, we will mainly focus on the gate constraints. PlonK's core system consists of gates with *fan-in 2, fan-out 1* meaning that each gate has two inputs and one output. A system of gates constraints can be described with equations of the following form:

$$(\mathcal{Q}_{L_i})a_i + (\mathcal{Q}_{R_i})b_i + (\mathcal{Q}_{O_i})c_i + (\mathcal{Q}_{M_i})a_ib_i + (\mathcal{Q}_{C_i}) = 0\,,$$

where a_i, b_i and c_i are respectively the left, the right and the output wire of each gate i. Then L, R, O, M and C respectively mean Left, Right, Output, Multiply, Constant and indicate the type of the gate: multiplication, addition or constant gate. In Table 1.2 we present the respective value of $\mathcal{Q}_{L_i}, \mathcal{Q}_{R_i}, \mathcal{Q}_{O_i}, \mathcal{Q}_{M_i}$ and $\mathcal{Q}_{C_i}$ for each type of gate.

	$\mathcal{Q}_{L_i}$	$\mathcal{Q}_{R_i}$	$\mathcal{Q}_{O_i}$	$\mathcal{Q}_{M_i}$	$\mathcal{Q}_{C_i}$
Multiplication gate	0	0	-1	1	0
Addition gate	1	1	-1	0	0
Constant gate	1	0	0	0	$-x$

Table 1.2: *PlonK gates constraints.*

Such a set of equations is then normalized into the following equation:

$$\mathcal{Q}_L a + \mathcal{Q}_R b + \mathcal{Q}_O c + \mathcal{Q}_M ab + \mathcal{Q}_C = 0\,,$$

where the vectors $\mathcal{Q}_L, \mathcal{Q}_R, \mathcal{Q}_O, \mathcal{Q}_M$ and $\mathcal{Q}_C$ are called the *selectors* and encode the circuit structure, and the vectors a, b and c are the *witness assignments.*

Each vector is then converted into a list of points in order to obtain a polynomial using interpolation. The aim is to obtain a single polynomial $f(x)$ compressing all constraints as follows:

$$f(x) = \mathcal{Q}_L(x)a(x) + \mathcal{Q}_R(x)b(x) + \mathcal{Q}_O(x)c(x) + \mathcal{Q}_M(x)a(x)b(x) + \mathcal{Q}_C(x)\,,$$

such that $f(x) = 0$ for all $x \in \{0, 1, \ldots, n-1\}$, where n is the number of gates. We will describe those last steps in more details in the following example. Having such a polynomial f is then what allows a polynomial commitment scheme. This scheme consists in proving that a certain polynomial evaluates to a certain value at a certain point, without revealing the polynomial.

[1] In order to respect the choice of the authors we will use the original font.

Example 1.5. Let us consider the following example: $x^3 + 5x^2 + 3 = 31$. To prove that we know the solution of this equation, we first need to convert it into the circuit described in Figure 1.10.

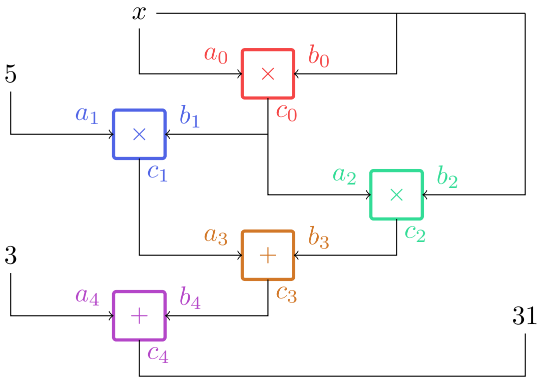


Figure 1.10: *Circuit for* $x^3 + 5x^2 + 3 = 31$.

Such a circuit can then be translated into the following system of gates constraints:

$$\begin{cases} a_0 \times b_0 &= c_0 \\ a_1 \times b_1 &= c_1 \\ a_2 \times b_2 &= c_2 \\ a_3 + b_3 &= c_3 \\ 3 + b_4 &= 31\,. \end{cases} \quad \Leftrightarrow \quad \begin{cases} a_0 \times b_0 - c_0 &= 0 \\ a_1 \times b_1 - c_1 &= 0 \\ a_2 \times b_2 - c_2 &= 0 \\ a_3 + b_3 - c_3 &= 0 \\ b_4 - 28 &= 0\,. \end{cases}$$

Note that in the example we are only focusing on gate constraints, while there are also copy constraints to take into account as $a_3 = c_1$ for example. Then, in each row of Table 1.3 we collect the coefficients $(*)$ of the equations:

$$\forall\, i \in \{0, \ldots 4\} \quad (*) \cdot a_i + (*) \cdot b_i + (*) \cdot c_i + (*) \cdot a_i b_i + (*) = 0\,.$$

i	$\mathcal{Q}_{L_i}$	$\mathcal{Q}_{R_i}$	$\mathcal{Q}_{O_i}$	$\mathcal{Q}_{M_i}$	$\mathcal{Q}_{C_i}$
0	0	0	-1	1	0
1	0	0	-1	1	0
2	0	0	-1	1	0
3	1	1	-1	0	0
4	0	1	0	0	-28

Table 1.3: *Gate constraints for* $x^3 + 5x^2 + 3 = 31$.

Then the vectors $\mathcal{Q}_L, \mathcal{Q}_R, \mathcal{Q}_O, \mathcal{Q}_M$ and $\mathcal{Q}_C$ are converted into a list of points as shown in Table 1.4. Using Lagrange interpolation we then get:

$$\mathcal{Q}_L(x) = -\frac{1}{6}x^4 + \frac{7}{6}x^3 - \frac{7}{3}x^2 + \frac{4}{3}x\,,$$

$$\begin{aligned}
\mathcal{Q}_R(x) &= -\frac{1}{8}x^4 + \frac{11}{12}x^3 - \frac{15}{8}x^2 + \frac{13}{12}x\,,\\
\mathcal{Q}_O(x) &= \frac{1}{24}x^4 - \frac{1}{4}x^3 + \frac{11}{24}x^2 - \frac{1}{4}x - 1\,,\\
\mathcal{Q}_M(x) &= \frac{1}{8}x^4 - \frac{11}{12}x^3 + \frac{15}{8}x^2 - \frac{13}{12}x + 1\,,\\
\mathcal{Q}_C(x) &= -\frac{7}{6}x^4 + 7x^3 - \frac{77}{6}x^2 + 7x\,.
\end{aligned}$$

	Vector	List of points
$\mathcal{Q}_L$	$(0,0,0,1,0)$	$\{(0,0),(1,0),(2,0),(3,1),(4,0)\}$
$\mathcal{Q}_R$	$(0,0,0,1,1)$	$\{(0,0),(1,0),(2,0),(3,1),(4,1)\}$
$\mathcal{Q}_O$	$(-1,-1,-1,-1,0)$	$\{(0,-1),(1,-1),(2,-1),(3,-1),(4,0)\}$
$\mathcal{Q}_M$	$(1,1,1,0,0)$	$\{(0,1),(1,1),(2,1),(3,0),(4,0)\}$
$\mathcal{Q}_C$	$(0,0,0,0,-28)$	$\{(0,0),(1,0),(2,0),(3,0),(4,-28)\}$

Table 1.4: *From vectors to lists of points.*

We let f be such that

$$f(x) = \mathcal{Q}_L(x)a(x) + \mathcal{Q}_R(x)b(x) + \mathcal{Q}_O(x)c(x) + \mathcal{Q}_M(x)a(x)b(x) + \mathcal{Q}_C(x)\,.$$

We can indeed check that $f(0)$ evaluates to 0:

$$\begin{aligned}
f(0) &= \mathcal{Q}_L(0)a_0 + \mathcal{Q}_R(0)b_0 + \mathcal{Q}_O(0)c_0 + \mathcal{Q}_M(0)a_0b_0 + \mathcal{Q}_C(0)\\
&= (0)a_0 + (0)b_0 + (-1)c_0 + (1)a_0b_0 + (0)\,.
\end{aligned}$$

The same holds for $x \in \{1,2,3,4\}$.

The idea is then to write f as follows

$$f(x) = Z(x)\cdot g(x), \qquad \text{where } Z(x) = x(x-1)(x-2)(x-3)(x-4)\,,$$

so that Z is the vanishing polynomial of the domain defined by $x \in \{0,1,2,3,4\}$. We finally define h as

$$h(x) = f(x) - Z(x)\cdot g(x)\,,$$

so that h is the zero polynomial. As a consequence, the proof consists in evaluating h at a random point and see if the result is 0. According to the Schwartz-Zippel lemma [Sch80; Zip79], this would suggest that the polynomial is 0 everywhere with a high probability.

To complete the proof we must also take into account copy constraints. In this circuit we have for instance: $a_1 = 5$, $a_2 = c_0, \ldots$, but, for simplicity, we do not aim at giving all the details of the proof system in this thesis.

Let us mention that $\mathcal{P}$lon$\mathcal{K}$ can be augmented by using so-called *custom gates* when a specific operation is reused several times. The aim in using such custom gates is to evaluate some complex operations with a lower cost than in R1CS.

1.4.2.3 Algebraic Intermediate Representation

In the original STARK Protocol, the output of the arithmetization is an Algebraic Intermediate Representation (AIR) of a computation [Ben+18]. Such a representation has two main components: an execution trace and a set of polynomial constraints. The execution trace is a matrix for which each line represents the states of a calculation at different time points, and each column corresponds to an algebraic register tracked over all the steps of the calculation. The execution trace size is given by its number of rows t and its number of columns w. The set of polynomial constraints is built such that all the constraints are satisfied if and only if the trace gives a valid computation. It is worth noticing that while the execution trace might be very long, we aim at giving a succinct set of polynomial constraints.

Example 1.6. Let us consider a simple algorithm that computes the Fibonacci sequence.

Algorithm 1.1 Computing the n^{th} term of the Fibonacci sequence for a given n.

```
a = 1
b = 0
for i in range(n):
    a, b = a + b, a
return a
```

Then the trace of Algorithm 1.1 is given in Table 1.5. Here we have $t = n$ and $w = 2$.

i	a_i	b_i
0	1	0
1	1	1
2	2	1
3	3	2
$\vdots$	$\vdots$	$\vdots$
$n-1$	a_{n-1}	b_{n-1}

Table 1.5: Execution trace of the Fibonacci sequence.

We observe that it is easy to check if intermediate computations are correct. For example, let us consider rows 3 and 4 (i.e. $i = 2$ and $i = 3$). Then we can easily be convinced of the validity of this step since

$$a_3 = 3 = 2 + 1 = a_2 + b_2 \quad \text{and} \quad b_3 = 2 = a_2\,.$$

This table finally yields the following system of constraints:

$$\begin{cases} a_0 = 1 & \text{in first row,} \\ b_0 = 0 & \text{in first row,} \\ a_{i+1} = a_i + b_i & \text{for } 0 \leqslant i \leqslant n-2\,, \\ b_{i+1} = a_i & \text{for } 0 \leqslant i \leqslant n-2\,, \\ a_{n-1} = Fib(n-1) & \text{in row } n-1\,. \end{cases}$$

The procedure is the same for more sophisticated algorithms.

1.5 A succinct state of the art of the new primitives

In this section we present primitives, such as Poseidon, *Rescue*, Reinforced Concrete or Griffin[2], that will be used as a basis to evaluate our own design, Anemoi, that will be introduced in Chapter 3. We will also discuss more about these primitives in Chapter 4 on algebraic attacks, with a focus on Feistel–MiMC, Poseidon and *Rescue*. An important part of this thesis will also be dedicated to the study of the algebraic degree of MiMC in Chapters 5, 6 and 7.

While most of the primitives studied in this thesis are specifically designed for zero-knowledge proofs, we will also study two other primitives: Chaghri and Ciminion, that we will introduce at the end of this section.

For the sake of consistency in this thesis, q will represent either a power of 2, or a prime number p, the exponent will be d, the number of branches will be m.

1.5.1 Primitives for ZKP

First, let us give an overview of the primitives designed for Zero-Knowledge Proofs in recent years. In Table 1.6 we give a list of such primitives.

Primitive	Reference	Type	Alphabet
Anemoi	[Bou+23]	II	$\mathbb{F}_{2^n}^m$ or $\mathbb{F}_p^m$ with m even
Arion	[RST23]	II	$\mathbb{F}_p^m$
Feistel–MiMC	[Alb+16]	I	$\mathbb{F}_{2^n}^2$ or $\mathbb{F}_p^2$
Friday	[AD18]	II	$\mathbb{F}_{2^n}^m$
GMiMC	[Alb+19b]	I	$\mathbb{F}_{2^n}^m$
Grendel	[Sze21]	II	$\mathbb{F}_p^m$
Griffin	[Gra+23a]	II	$\mathbb{F}_p^m$ with $m \in \{3, 4m'\}$
Jarvis	[AD18]	II	$\mathbb{F}_{2^n}$
MiMC	[Alb+16]	I	$\mathbb{F}_{2^n}$ or $\mathbb{F}_p$
MiMCHash	[Alb+16]	I	$\mathbb{F}_{2^n}^m$
Monolith	[Gra+23b]	III	$\mathbb{F}_p^m$ with $m \geqslant 8$ and $p \in \{2^{64} - 2^{32} + 1, 2^{31} - 1\}$
Neptune	[Gra+22b]	I	$\mathbb{F}_p^m$ with m even
Poseidon	[Gra+21]	I	$\mathbb{F}_p^m$
Poseidon2	[GKS23]	I	$\mathbb{F}_p^m$
Reinforced Concrete	[Gra+22a]	III	$\mathbb{F}_p^3$
Rescue	[Aly+20]	II	$\mathbb{F}_p^m$
Rescue–Prime	[SAD20]	II	$\mathbb{F}_p^m$
Tip5	[Sze+23]	III	$\mathbb{F}_p^{16}$ with $p = 2^{64} - 2^{32} + 1$
Tip4	[Sal23]	III	$\mathbb{F}_p^{16}$ or $\mathbb{F}_p^{12}$ with $p = 2^{64} - 2^{32} + 1$
Vision	[Aly+20]	II	$\mathbb{F}_{2^n}^m$

Table 1.6: *Arithmetization-Oriented Primitives.*

[2] As for constraints systems we also aim at giving the font proposed by the designers

This table reflects the known primitives at the time of writing and is obviously not exhaustive. The idea is mainly to introduce the primitives that will be discussed later in this manuscript while, at the same time, giving an overview of the different design principles. We classify them in three categories as proposed by Christian Rechberger [Rec23] and commonly used in the literature.

Type I corresponds to the first wave of primitives, based on low degree permutations, we will present some of them in Section 1.5.1.1.

Type II corresponds to primitives, based on equivalences, or other design strategies to have a high-degree evaluation and low-degree verification. We introduce some of them in Section 1.5.1.2 and we will give more details on `Anemoi` in Chapter 3.

Type III corresponds to more recent primitives based on look-up tables, we will give some examples in Section 1.5.1.3.

We also propose Figure 1.11 to help us identify the different types.

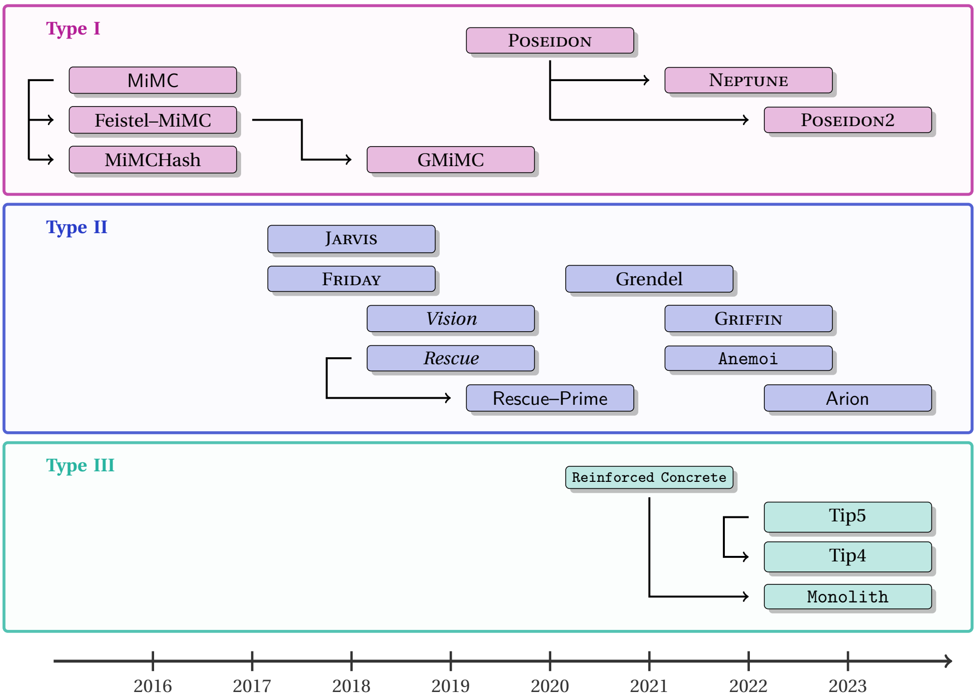


Figure 1.11: *Overview of Arithmetization-Oriented Primitives.*

1.5.1.1 Type I: low-degree functions

The first Arithmetization-Oriented primitives aimed at limiting the number of nonlinear operations. The approach was to use a round function of low degree, so that it is trivial to verify the result using low-degree functions.

MiMC and variants: Feistel–MiMC, MiMCHash and GMiMC

MiMC is a block cipher that was introduced by Albrecht *et al.* [Alb+16] and is defined over $\mathbb{F}_q$ where q is either a prime number, p, or a power of 2, 2^n with n odd and $n \approx 128$. The primitive consists of r iterations of an extremely simple round function:

$$F = F_{r-1} \circ \ldots F_0, \text{ where } F_{i,0 \leqslant i < r} : x \mapsto x^d + k + c_i$$

where $c = (c_0, \ldots, c_{r-1})$ is a sequence of r round constants, with $c_0 = 0$, and where d is coprime with $(q-1)$ in order to ensure that the round function is bijective, the d chosen is usually the smallest integer satisfying such condition. It follows that the round function is fully described by the exponent d and by the sequence c of round constants. The design of MiMC is given in Figure 1.12.

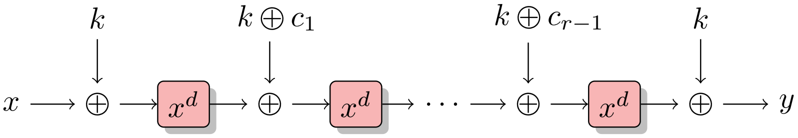


Figure 1.12: *MiMC with r rounds.*

The authors also proposed a hash function, MiMCHash, as depicted in Figure 1.13. It is based on the use of MiMC$_d$ within the sponge framework. They proposed in particular two variants of MiMCHash, one over a binary field of extension degree $n = 1025$, the other one with $n = 769$.

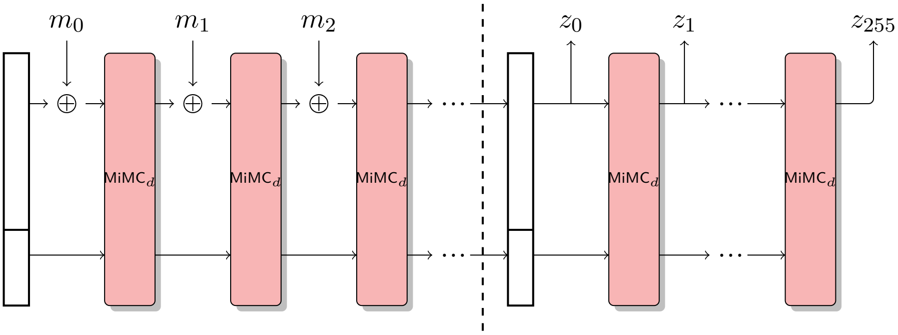


Figure 1.13: *MiMCHash.*

In the same paper, a Feistel-based variant is proposed. It operates on $\mathbb{F}_q^2$ using a basic r-round Feistel structure with the i-th round function $x \mapsto (x + c_i)^d$. This Feistel construction is depicted on Figure 1.14.

Feistel–MiMC has then been generalized to obtain the ciphers in the GMiMC family designed by Albrecht *et al.* [Alb+19b], which are based on generalized Feistel structures.

Poseidon and variants: Poseidon2, Neptune

Poseidon [Gra+21] is a family of hash functions, based on the HADES design strategy [Gra+20] and defined over $\mathbb{F}_p^m$. The internal permutation also relies on a small-degree function $x \mapsto x^d$. Note that, in this thesis, for the sake of consistency, we will always denote by d the exponent

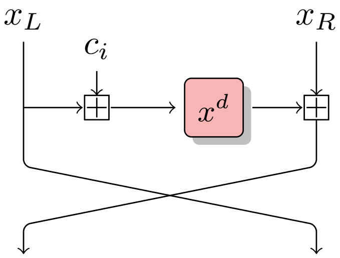


Figure 1.14: *Round i of Feistel–MiMC.*

of the involved power function, while it may differ from the notation used in the specifications. Poseidon is composed of $r = \mathsf{RF} + \mathsf{RP}$ rounds of two different types for the non-linear layer: full rounds have m S-box functions, and partial rounds have only one S-box and $m-1$ identity functions. Each round function consists in adding the round constants (that we will denote "AddC"), in applying partial or full S-box layers S, and then in multiplying the state by an MDS matrix. The permutation starts with $\mathsf{Rf} = \mathsf{RF}/2$ full rounds, followed by RP partial rounds, and finally $\mathsf{Rf} = \mathsf{RF}/2$ full rounds. Figure 1.15 gives an overview of such a construction.

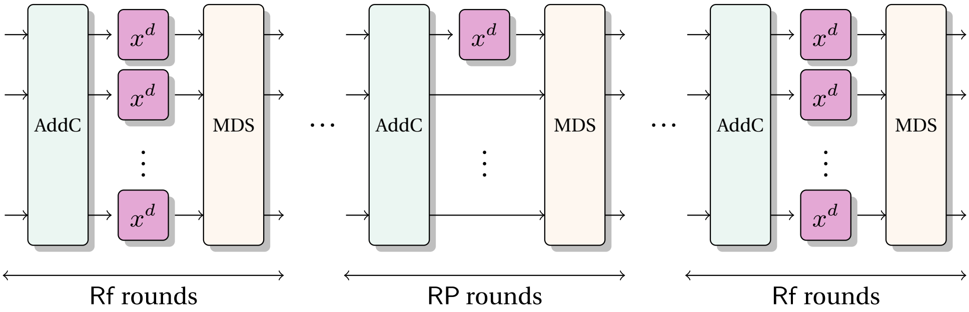


Figure 1.15: *Overview of Poseidon.*

Poseidon2, a more efficient version of Poseidon, has been recently proposed in [GKS23]. While Poseidon is a sponge hash function, Poseidon2 can be either a sponge or a compression function depending on the use case. The other difference with the original construction is that Poseidon2 is instantiated by more efficient linear layers.

Another variant of the sponge hash function Poseidon is Neptune presented in [Gra+22b]. The design of Neptune is highly inspired by the design of Poseidon, since the middle rounds are partial rounds with only one branch with the power map $x \mapsto x^d$. The full rounds of Poseidon are then replaced by external rounds for which the non-linear layer is defined as follows, and requires the number of branches to be even:

$$\mathcal{S} = (x_0, x_1, \ldots, x_{m-2}, x_{m-1}) = \mathcal{S}'(x_0, x_1) || \ldots || \mathcal{S}'(x_{m-2}, x_{m-1}) \,.$$

The function $\mathcal{S}'$ is defined as $\mathcal{S}'(x_{2i}, x_{2i+1}) = y_{2i}||y_{2i+1}$, where the y_{2i}, y_{2i+1} are such that:

$$\begin{aligned} y_{2i} &= \alpha^2(2x_{2i} + x_{2i+1}) + 3\alpha(x_{2i} - x_{2i+1})^2 \\ &\quad + \left(\gamma + \alpha(x_{2i} - 2x_{2i+1}) - (x_{2i} - x_{2i+1})^2\right)^2 , \\ y_{2i+1} &= \alpha^2(x_{2i} + 3x_{2i+1}) + 4\alpha(x_{2i} - x_{2i+1})^2 \\ &\quad + \left(\gamma + \alpha(x_{2i} - 2x_{2i+1}) - (x_{2i} - x_{2i+1})^2\right)^2 , \end{aligned}$$

for arbitrary $\alpha, \gamma \in \mathbb{F}_p \backslash \{0\}$. In this paper the authors show that this variant leads to a reduction of multiplications compared to POSEIDON.

1.5.1.2 Type II: low-degree equivalence

Let us introduce the second type of primitives, based on low-degree equivalence or other design strategies. We will not discuss the `Anemoi` construction in this section, since the primitive will be introduced in more details in Chapter 3.

MARVELLOUS design strategy: Jarvis and Friday

MARVELLOUS[3] [AD18] is a family of cryptographic primitives specifically designed for STARK efficiency. This family is composed of the block cipher JARVIS and the hash function FRIDAY defined over binary fields.

Each round of JARVIS consists in applying the inverse function $x \mapsto x^{-1}$, the affine layer A and adding the corresponding sub-key. A is an $\mathbb{F}_2$-linearized affine polynomial given by

$$A(x) = a_{-1} + \sum_{i=0}^{n-1} a_i x^{2^i} .$$

Let us notice that, for efficiency, A is decomposed into two steps: $A = C \circ B^{-1}$ so that the layers B and C are STARK-efficient and evaluated separately using their low-degree variants. An overview of the JARVIS construction is given in Figure 1.16.

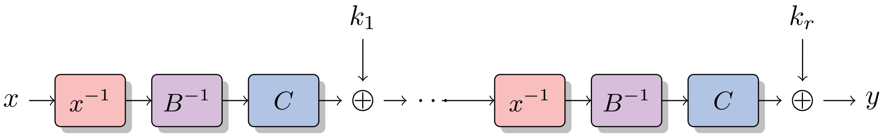


Figure 1.16: Overview of JARVIS.

FRIDAY is a hash function based on the Merkle-Damgård construction and instantiated with JARVIS as its compression function. It has been shown in [Alb+19a] that both JARVIS and FRIDAY were particularly vulnerable to Gröbner basis attacks.

[3] Note that there are two Marvellous design strategies, hence our choice to respect the font of the designers.

Marvellous design strategy: *Vision* and *Rescue*

The *Marvellous* design [Aly+20] is an SPN construction defined over $\mathbb{F}_q^m$, where q is either a prime number or a power of 2. The construction is decomposed by steps such that one round represents two steps. Then each step is composed of the addition of a key and round constant, the multiplication by an MDS matrix, and one S-box that is different depending on the step: a first S-box is applied on even steps and a second one is applied on odd steps. We will briefly introduce two examples of such designs, namely *Rescue* and *Vision*.

Rescue has the particularity of using both a low degree S-box and its inverse. Indeed, each round of *Rescue*, consists of two steps: while the first one involves an S-box S, the second one replaces S with its inverse S^{-1}. The two steps in each round are described in Figure 1.17. For consistency with other primitives we denote by AddK the addition of the key in each step. Note that the sub-keys are derived from the master key and round constants.

In [SAD20] the authors proposed a hash function called *Rescue–Prime* based on the design of *Rescue*. For our study, we will use the specifications of *Rescue–Prime* [SAD20], which means in particular that in each round, we first apply S that corresponds to the power function $x \mapsto x^d$ where d is of low degree and then S^{-1} (rather than the contrary as described in the original paper [Aly+20]).

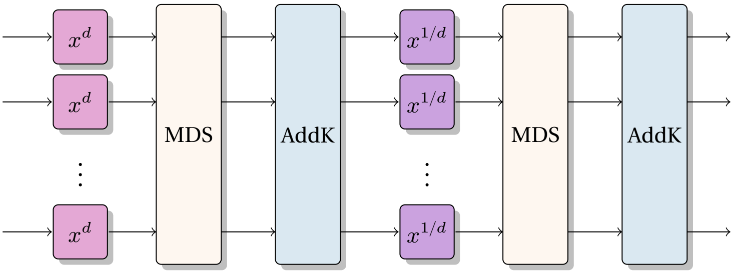


Figure 1.17: *One round of Rescue.*

Let us note that if s is the required security level then *Rescue–Prime* requires $1.5 \cdot \max\{5, \lceil (s+2)/4m \rceil\}$ rounds when $d = 3$ and $1.5 \cdot \max\{5, \lceil (s+3)/5.5m \rceil\}$ rounds when $d = 5$.

As opposed to *Rescue*, *Vision* is meant to operate on binary fields $\mathbb{F}_{2^n}$. Let B be an $\mathbb{F}_2$-linearized affine polynomial

$$B(x) = b_{-1} + \sum_{i=0}^{n-1} b_i x^{2^i} .$$

In *Vision*, the S-boxes are of the form $B(x^{-1})$ and $B^{-1}(x^{-1})$, where B is of univariate degree 4. We describe the construction in Figure 1.18.

Grendel

In [Sze21], the author proposes a new design based on an SPN construction over $\mathbb{F}_p^m$ where the S-box uses the Legendre symbol. Indeed, the non-linear layer of this primitive is a low-degree power-map $x \mapsto x^d$, with a possible sign flip given by the Legendre symbol, defined for each

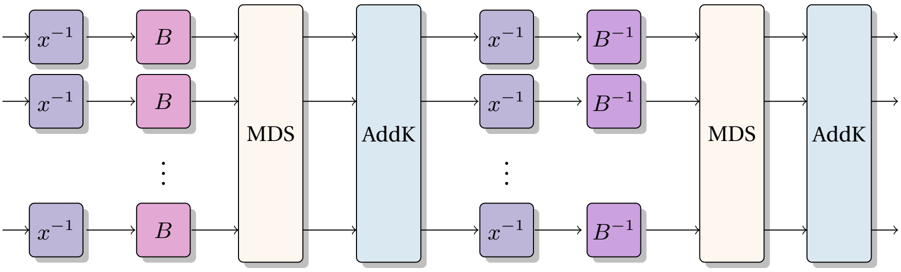


Figure 1.18: *One round of Vision.*

prime-field element $a \in \mathbb{F}_p$ as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \equiv b^2 \bmod p, \text{ for some } b \in \mathbb{F}_p^*, \\ 0 & \text{if } a \equiv 0 \bmod p, \\ -1 & \text{otherwise.} \end{cases}$$

The round function of Grendel is depicted in Figure 1.19.

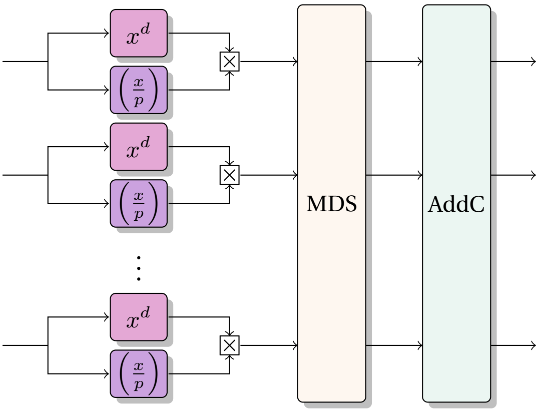


Figure 1.19: *Round function of Grendel.*

Griffin

Griffin has been designed by Grassi *et al.* [Gra+23a]. The specific features of Griffin impose that the primitive is only suitable for finite fields $\mathbb{F}_p^m$ where $m \in \{3, 4m'\}$. Each round function is composed of a non-linear layer, the addition of a constant, and a linear layer defined by a matrix multiplication. Following the choice made in `Anemoi` (see Chapter 3), the authors of Griffin have then updated their design with MDS matrices from [DL18]. Indeed, this work presents matrix constructions with a minimal number of additions.

Then, the non-linear layer is defined as follows:

$$y_i = \begin{cases} x_0^{1/d} & \text{for } i = 0\,, \\ x_1^d & \text{for } i = 1\,, \\ x_2 \left(L_2(y_0, y_1, 0)^2 + \alpha_2 L_2(y_0, y_1, 0) + \beta_2\right) & \text{for } i = 2\,, \\ x_i \left(L_i(y_0, y_1, x_{i-1})^2 + \alpha_i L_2(y_0, y_1, x_{i-1}) + \beta_i\right) & \text{otherwise,} \end{cases}$$

where $(\alpha_i, \beta_i) \in \mathbb{F}_p^2 \backslash \{(0,0)\}$ are such that $\alpha_i^2 - 4\beta_i$ is not a square in $\mathbb{F}_p$. The non-linear layer of Griffin is depicted in Figure 1.20, where to simplify the construction we denote by F_i the last two equations of the above description.

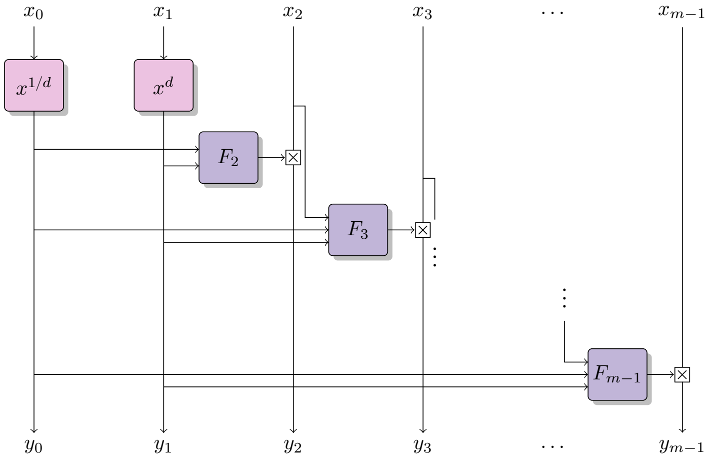


Figure 1.20: Non-linear layer of Griffin.

For a security level s, Griffin requires at least $\lceil 1.2 \max\{6, 1 + R_{\text{GB}}\} \rceil$ rounds where R_{GB} is the smallest integer such that

$$\min \left\{ \binom{R_{\text{GB}} \cdot (d+m) + 1}{1 + m \cdot R_{\text{GB}}}, \binom{d^{R_{\text{GB}}} + 1 + R_{\text{GB}}}{1 + R_{\text{GB}}} \right\} \geqslant 2^{s/2}\,.$$

Arion

The block cipher Arion and its corresponding hash function ArionHash have been proposed in [RST23]. This design can be seen as a mix of Griffin and `Anemoi`. Indeed, as we have seen previously, the non-linear layer of Griffin uses a high-degree polynomial on one branch and low-degree polynomials on the others. The non-linear layer of Arion is built based on the same idea. Let p be a prime number and d_1 the smallest integer such that $\gcd(d_1, p-1) = 1$. Then the high-degree permutation $x \mapsto x^e$ applied to the last branch is defined as follows: if d_2 is an arbitrary integer such that $\gcd(d_2, p-1) = 1$, then $e \equiv d_2^{-1} \bmod (p-1)$. Let us suppose that $x_1, \dots x_n$ are the inputs of the non-linear layer, and $y_1, \dots y_n$ the outputs, then we have:

$$y_i = \begin{cases} x_n^e & \text{for } i = n\,, \\ f_i(x_1, \dots x_n) = x_i^{d_1} \cdot g_i(\sigma_{i+1,n}) + h_i(\sigma_{i+1,n}) & \text{otherwise.} \end{cases}$$

where g_i, h_i and $\sigma_{i+1,n}$ are defined as follows:

$$\begin{aligned} g_i(x) &= x^2 + \alpha_{i,1}x + \alpha_{i,2} \ , \\ h_i(x) &= x^2 + \beta_i x \ , \\ \sigma_{i+1,n} &= \sum_{j=i+1}^{n} (x_j + y_j) \ . \end{aligned}$$

$\alpha_{i,1}, \alpha_{i,2}$ and β_i are constants in $\mathbb{F}_p$ such that $\alpha_{i,1}^2 - 4\alpha_{i,2}$ is not a square in $\mathbb{F}_p$. We illustrate the construction of this non-linear layer in Figure 1.21, where for the sake of clarity we only represent the function f_i without the details of g_i, h_i and $\sigma_{i+1,n}$.

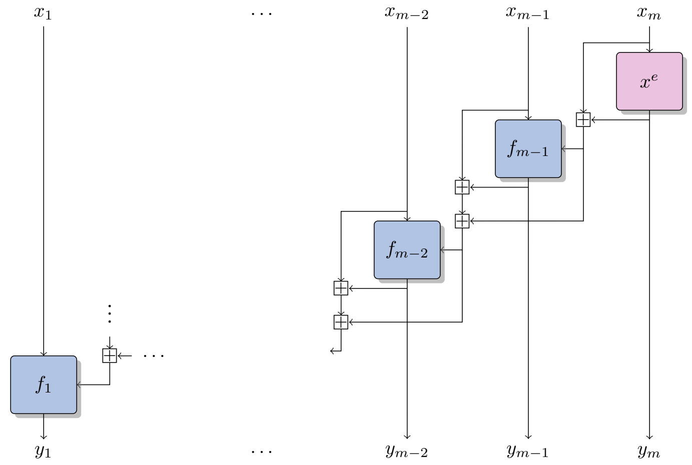


Figure 1.21: Non-linear layer of Arion.

As we will see in Chapter 3, the `Anemoi` family of hash functions relies on the CCZ-equivalence, which allows better performances by implementing a non-linear layer of low degree that is CCZ-equivalent to the high-degree one. The authors of Arion also use the CCZ-equivalence between their non-linear layer and another function of lower degree to have a more efficient verification.

1.5.1.3 Type III: look-up tables

More recently, new primitives have been proposed, based on look-up tables. This additional requirement for lookup tables however reduces the compatibility of these hash functions within the space of proving systems. Let us introduce this third wave of Arithmetization-Oriented primitives.

`Reinforced Concrete` and `Monolith`

The first design in this direction is `Reinforced Concrete` [Gra+22a]. This primitive operates on three prime field elements and uses three different layers: `Concrete`, `Bricks`, and `Bar`. Lookup tables are used for the `Bar` layer. The non-linear layer is the `Bricks` function

$$\texttt{Bricks}(x_1, x_2, x_3) = \left(x_1^d, x_2(x_1^2 + \alpha_1 x_1 + \beta_1), x_3(x_2^2 + \alpha_2 x_2 + \beta_2)\right) \ ,$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_p$ are such that $\alpha_i^2 - 4\beta_i$ is not a square in $\mathbb{F}_p$. The exponent d is chosen such that $\gcd(d, p-1) = 1$.The Concrete function denotes the linear layer which is composed of a matrix multiplication and addition of constants.

Finally, the main novelty of Reinforced Concrete is its Bar layer that divides $\mathbb{F}_p$ into a Cartesian product of smaller sets, and then an S-box is applied on each of these sets. This layer is applied only once in the middle on the Reinforced Concrete permutation, as described in Figure 1.22. The function Bars operates separately on each branch, so that on each branch the function Bar is applied. Bar then consists of three operations: the decomposition, the S-box and the composition, and the S-box is derived from the MiMC cipher.

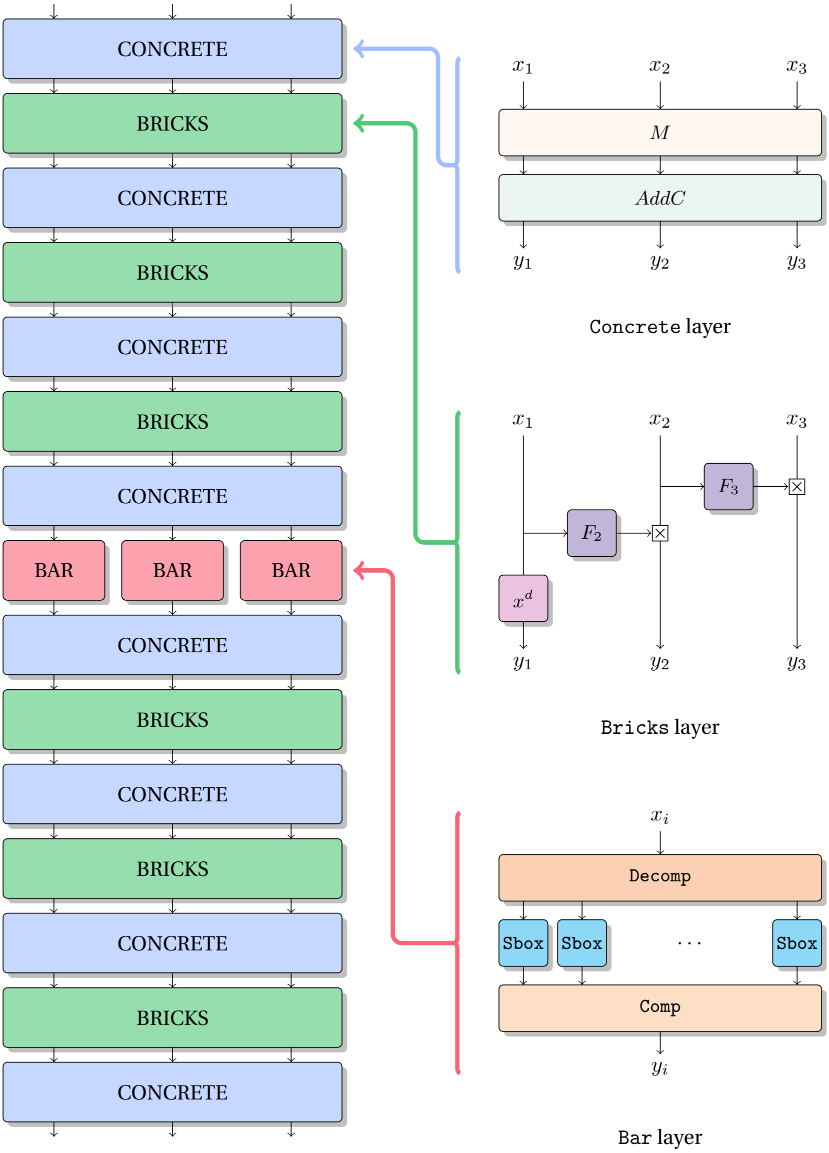


Figure 1.22: Overview of Reinforced Concrete.

A very recent construction highly inspired by `Reinforced Concrete` has been proposed under the name `Monolith` [Gra+23b] for smaller fields, namely the Goldilocks field with $p = 2^{64} - 2^{32} + 1$ and Mersenne field with $p = 2^{31} - 1$. `Monolith` is also decomposed into: `Concrete`, `Bricks`, and `Bar`. However some changes have been made compared to `Reinforced Concrete`. For instance, the `Bricks` layer no longer has multiplications between branches:

$$\texttt{Bricks}(x_1, x_2, \dots, x_m) = (x_1, x_2 + x_1^2, \dots x_m + x_{m-1}^2)\ .$$

Moreover, the overall design consists in alternating layers of `Concrete`, `Bricks`, and `Bar`, implying that there is more than only one `Bars` layer.

Tip5 and Tip4

Tip5 [Sze+23] is a primitive that has been specifically designed to be efficient over the Goldilocks field $\mathbb{F}_p$ with $p = 2^{64} - 2^{32} + 1$. Tip5 is highly inspired by its predecessors. Indeed the non-linear layer is composed of two types of S-boxes: the first one, S, is taken from a lookup table, as it was already proposed in `Reinforced Concrete`, and the second one, T, is the classical power function $x \mapsto x^d$, as used in *Rescue* or Poseidon (here $d = 7$). The first type of S-box is similar to the `Bars` layer of `Reinforced Concrete` with decomposition and composition operations to work in a smaller field: the lookup table is defined over $\mathbb{F}_{2^8+1}$.

The overall construction is a 5-round SPN with a circulant MDS matrix as linear layer. Note that the linear layer and the round constants are derived from the ASCII string “Tip5”. Among the 16 branches, 4 are of the first type S, and 12 of the second type T. An overview of the design is proposed in Figure 1.23.

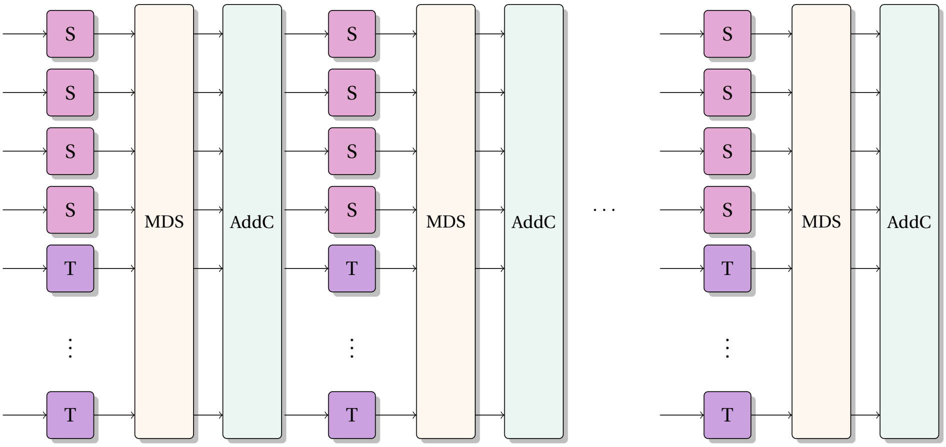


Figure 1.23: *Overview of Tip5.*

While most of the applications require 128 bits of security, Tip5 is targeting a security level of 160 bits. Then, two variants achieving 128 bits of security, have been proposed by Salen [Sal23] called Tip4 and Tip4’. Combined with the `Jive` compression mode, that will be presented in Chapter 3, they are offering better performances for native hashing and digest compression, but also for in-circuit computation.

1.5.2 Primitives for FHE and MPC

1.5.2.1 Fully Homomorphic encryption

Homomorphic Encryption (HE) is an advanced cryptographic technique allowing users to evaluate any circuit on encrypted data without decrypting it. Indeed, *homomorphic* means that one set of data is transformed into another while preserving the relationships between the elements in both sets. As a consequence, in a homomorphic encryption scheme, whether the operation is performed on encrypted or decrypted data, mathematical operations produce equivalent results. Fully homomorphic encryption (FHE) is then the strongest notion of HE since it allows the evaluation of arbitrary circuits with an infinite number of additions or multiplications for the ciphertext. To prevent the expansion factor associated with FHE, the aim is to combine symmetric encryption with FHE. This involves transmitting encrypted data using the symmetric algorithm and then evaluating the decryption of the symmetric algorithm through homomorphic encryption.

Different symmetric designs, targeting such applications, have been proposed like for example LowMC [Alb+15], Rasta [Dob+18], Pasta [Dob+23], Kreyvium [Can+18] ..., to name a few. In the following, we will describe the construction of Chaghri [AMT22].

The example of Chaghri

Chaghri is an SPN construction defined over $\mathbb{F}_{2^{63}}$ with three field elements as vector state. Chaghri takes *Vision* as a starting point but while the two steps of a *Marvellous* round employ different S-boxes, every round of Chaghri is composed of two similar steps. Then each step of Chaghri in the decryption direction consists of a linear layer (multiplication by an MDS matrix), subkeys injection and a non-linear layer $B \circ G$ where G is a Gold exponent $G(x) = x^{2^{32}+1}$, and B is an affine polynomial. Let us notice that in a first version of the paper, the authors used $B(x) = c_1 + c_2 x^8$. However, it has been shown by Liu *et al.* in [Liu+23a] that such a choice implies a linear increase of the algebraic degree leading to a practical higher-order differential attack. As a consequence, the author of Chaghri moved to another affine layer $B(x) = c'_1 + c'_2 x + c'_3 x^4 + c'_4 x^{256}$, that is expected to lead to an exponential increase of the algebraic degree. We describe one round of Chaghri decryption (i.e. two steps) in Figure 1.24 as proposed in the original paper. Indeed the authors aimed at optimizing the decryption since it realized homomorphically on the server side, while encryption happens on the client side.

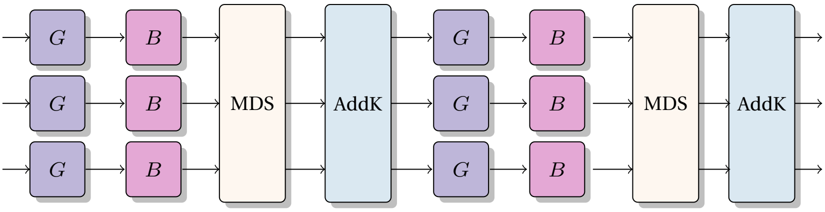


Figure 1.24: *Round function of Chaghri (decryption).*

1.5.2.2 Multi-party computation

Multi-Party Computation (MPC) is a cryptographic protocol dividing a computation among multiple parties where no single party can see the data of the other parties. For such protocols, the multiplicative depth of the circuit, like in ZKP, also appears to be an important feature. Then, primitives like MiMC or GMiMC are also relevant in this context. In the following, we will present a more recent one, namely Ciminion [Dob+21].

The example of Ciminion

Ciminion is a symmetric encryption scheme designed by Dobraunig *et al.* aiming at minimizing the number of multiplications in large finite fields. Unlike other primitives like Feistel–MiMC, Poseidon or *Rescue*, Ciminion does not use a power map as S-box. The non-linearity instead comes from the use of Toffoli gates $(a, b, c) \mapsto (a, b, c + ab)$. In addition, Ciminion uses a light linear layer instead of an MDS matrix. The round function of Ciminion is described in Figure 1.25, where the indices ℓ depend on the permutation.

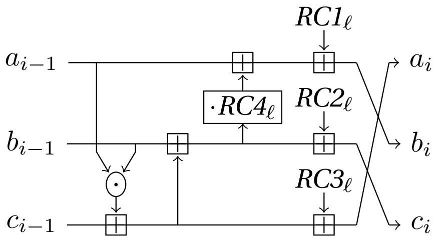


Figure 1.25: *Round function of Ciminion.*

For a nonce $\aleph$ and subkeys K_1 and K_2, we then give an overview of the entire encryption scheme in Figure 1.26. For the sake of consistency with previous figures, we describe it on $\mathbb{F}_p$ rather than $\mathbb{F}_{2^n}$, as presented in the original paper.

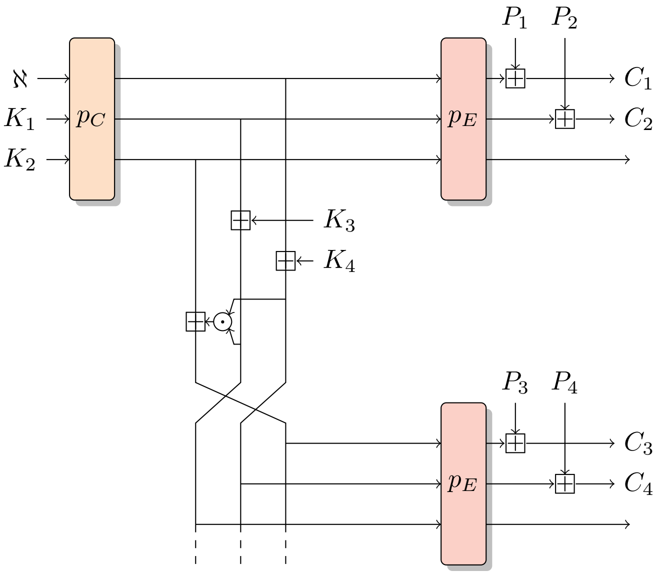


Figure 1.26: *Overview of Ciminion in* $\mathbb{F}_p$.

Here p_C and p_E are both permutations based on the round function of Figure 1.25. For a security level of s, p_C possesses $N = s + 6$ rounds and p_E has $R = \max\{\lceil \frac{s+37}{12} \rceil, 6\}$ rounds. It follows that, in Figure 1.25, we have $\ell = i$ for p_C and $\ell = i + N - R$ for p_E.

A need for some foundations

In this chapter we introduced some of the specific features of the new proof systems that have emerged in recent years. In particular, we have seen that the use of transformations having a simple representation in univariate form is one of the main constraints determining the design of the primitives used for such applications. Therefore, it is necessary to analyze the weaknesses introduced by the simplicity of this structure. While it is already quite straightforward to appreciate the fast evolution of this field and the large number of primitives that have been proposed, there is still a lack of cryptanalysis work to better understand the properties of these primitives.

Thus, the main objective of the following chapters is to contribute to the filling of this gap in order to have a deeper insight of the peculiarities of these new tools. After presenting a new vision for designing such primitives, introducing `Anemoi`, a new family of hash function based in the notion of CCZ-equivalence, we will focus on cryptanalysis. More precisely, we will propose both practical and theoretical perspectives. We will first investigate the security of some Arithmetization-Oriented primitives, like Feistel–MiMC, Poseidon, *Rescue–Prime*, Ciminion or `Anemoi`, against algebraic attacks. Then, thanks to a better understanding of the univariate polynomial representation of the MiMC block cipher, we will give a detailed analysis of the algebraic degree of this construction.

Chapter 2
CCZ-equivalence and Flystel

In this chapter we push further the understanding of Arithmetization-Oriented primitives by introducing a link between their design principles and CCZ-equivalence. Based on this idea we propose to study the relevance of the butterfly construction [PUB16] in this context. While butterflies were originally defined over binary fields $(\mathbb{F}_{2^n})^2$ for n odd, the problem remained entirely open for fields of odd characteristics. This leads us to propose a new non-linear layer: the `Flystel`, which takes inspiration from the well-studied butterfly structure. The `Flystel` was originally designed to be the main component of `Anemoi`, a new family of hash functions that will be presented in Chapter 3, however this is a standalone component that could be used for other designs.

First, in Section 2.1.2 we introduce some definitions and equivalence relations, from which we deduce a link with Arithmetization-Oriented primitives. We then present some examples of CCZ-equivalent functions in Section 2.2. More precisely we investigate the properties of the butterfly structure in the context of Arithmetization-Orientation, studying both cryptographic properties and performances in terms of R1CS constraints. Finally, in Section 2.3 we introduce `Flystel`, the new S-box highly inspired by the butterfly structure and a Feistel network. We define two variants: the open and closed `Flystel`, seeing both of them for fields of even and odd characteristics. We present an investigation of the `Flystel`'s differential and linear properties, as well as its R1CS and $\mathcal{P}\mathfrak{lon}\mathcal{K}$ cost.

The work presented in this chapter and Chapter 3, as well as the algebraic cryptanalysis of `Anemoi`, briefly introduced in Chapter 4, have been obtained with Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems, and published in the proceedings of the conference *CRYPTO* in 2023 [Bou+23].

Contents

2.1 On CCZ-Equivalence and Arithmetization-Orientation

CCZ-equivalence is widely used in the study of Boolean functions, and more specifically for the well-known Big APN problem [Dil06]. Its aim is to find an APN permutation, i.e. a permutation with differential uniformity equal to 2, over $\mathbb{F}_{2^n}$ where n is even and strictly bigger than 6. In this section, we show that CCZ-equivalence also has other applications by introducing a new link with arithmetization-orientation.

2.1.1 Definition

The notion of CCZ-equivalence was introduced by Carlet, Charpin and Zinoviev in 1998 [CCZ98], and the name came latter in [BCP06]. To better understand the specificities of such an equivalence relation, we give some preliminary definitions. We first describe linear and affine equivalences. In what follows we let q be a power of a prime number.

Definition 2.1 (Linear equivalence)**.** Let $F : \mathbb{F}_q \to \mathbb{F}_q$ and $G : \mathbb{F}_q \to \mathbb{F}_q$ be two functions. We say that F and G are *linear equivalent* if there exist linear permutations A and B such that

$$F = B \circ G \circ A\,.$$

Let us show a very simple example of this equivalence.

Example 2.1. Let $F : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^3$ and $G : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^5$. We have

$$F(x) = (B \circ G \circ A)(x) \quad \text{where } B(x) = x^2 \text{ and } A(x) = x\,,$$

implying that F and G are linear equivalent. Note that A and B are not unique since we can also choose $A(x) = x^2$ and $B(x) = x$.

Then linear equivalence can naturally be extended to affine equivalence as follows.

Definition 2.2 (Affine equivalence)**.** Let $F : \mathbb{F}_q \to \mathbb{F}_q$ and $G : \mathbb{F}_q \to \mathbb{F}_q$ be two functions. We say that F and G are *affine equivalent* if there exist affine permutations A and B such that

$$F = B \circ G \circ A\,.$$

The affine equivalence can be generalized to the extended affine equivalence by adding an affine function C in the equation.

Definition 2.3 (Extended-Affine equivalence)**.** Two functions $F : \mathbb{F}_q \to \mathbb{F}_q$ and $G : \mathbb{F}_q \to \mathbb{F}_q$ are *Extended Affine (EA) equivalent* if

$$F = B \circ G \circ A + C\,,$$

where A, B, C are affine functions with permutations A, B. It follows that the set of vectors $\begin{pmatrix} x \\ F(x) \end{pmatrix}$ for all $x \in \mathbb{F}_q$ corresponds to the set of vectors $\begin{pmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{pmatrix} \begin{pmatrix} x \\ G(x) \end{pmatrix}$.

In what follows we will denote by Γ_F the set of all vectors $\begin{pmatrix} x \\ F(x) \end{pmatrix}$ i.e. Γ_F is the graph of the function F. To simplify the notation, we will write the vectors in rows so that

$$\Gamma_F = \left\{ (x, F(x)) \mid x \in \mathbb{F}_q \right\}.$$

EA-equivalence is then a particular case of CCZ-equivalence.

Definition 2.4 (CCZ-equivalence)**.** Let $F : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $G : \mathbb{F}_q \rightarrow \mathbb{F}_q$ be two functions. F and G are *CCZ-equivalent* if the graph of F is affine equivalent to the graph of G. In other words, we have

$$\Gamma_F = \left\{ (x, F(x)) \mid x \in \mathbb{F}_q \right\} \ = \ \mathcal{A}(\Gamma_G) = \left\{ \mathcal{A}\left(x, G(x)\right) \mid x \in \mathbb{F}_q \right\} ,$$

where $\mathcal{A}$ is an affine permutation.

One particularity of EA-equivalence and CCZ-equivalence is that they preserve differential and linear properties. Let F and G be two CCZ equivalent functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, in [BCP06] it is proved that

$$\delta_G(a,b) \ = \ \delta_F(\mathcal{L}^{-1}(a,b)) \quad \text{and} \quad \mathcal{W}_G(\alpha,\beta) \ = \ (-1)^{c\cdot(\alpha,\beta)}\mathcal{W}_F(\mathcal{L}^T(\alpha,\beta)) \ ,$$

where $\mathcal{L}$ is the linear part of $\mathcal{A}$, i.e. $\mathcal{A}(x) = \mathcal{L}(x) + c$ for some constant $c \in \mathbb{F}_2^{n+m}$.

EA-equivalence preserves the degree but CCZ-equivalence does not. For example we note that a permutation is CCZ-equivalent to its inverse since the function $(x, y) \mapsto (y, x)$ is linear.

Example 2.2. Let $F : \mathbb{F}_{2^{11}} \rightarrow \mathbb{F}_{2^{11}}, x \mapsto x^3$. Since the inverse of 3 modulo $2^{11} - 1$ is 1365, we have $F^{-1} : \mathbb{F}_{2^{11}} \rightarrow \mathbb{F}_{2^{11}}, x \mapsto x^{1365}$. We see that we have $\deg(F^{-1}) \gg \deg(F)$ while they are CCZ-equivalent since

$$\begin{aligned}
\Gamma_{F^{-1}} &= \left\{\left(x, x^{1365}\right), x \in \mathbb{F}_{2^{11}}\right\} \\
&= \left\{\left(y^3, y\right), y \in \mathbb{F}_{2^{11}}\right\} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \left\{\left(y, y^3\right), y \in \mathbb{F}_{2^{11}}\right\} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_F \,.
\end{aligned}$$

Since EA-equivalence is a particular case of CCZ-equivalence, this raises the question of what else than EA-equivalence is needed to build CCZ-equivalence. For a long time, CCZ-equivalence was seen as EA-equivalence and inversion, but it is actually more complicated, involving another form of equivalence, namely the *twist*. Let us consider functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then using isomorphisms $\mathbb{F}_2^n \simeq \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$ and $\mathbb{F}_2^m \simeq \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$ we have the following definition.

Definition 2.5 (Twist-equivalence)**.** Let $F : \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \rightarrow \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$ and $G : \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \rightarrow \mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$ such that

$$F(x,y) = (T_y(x), U_x(y)) \,.$$

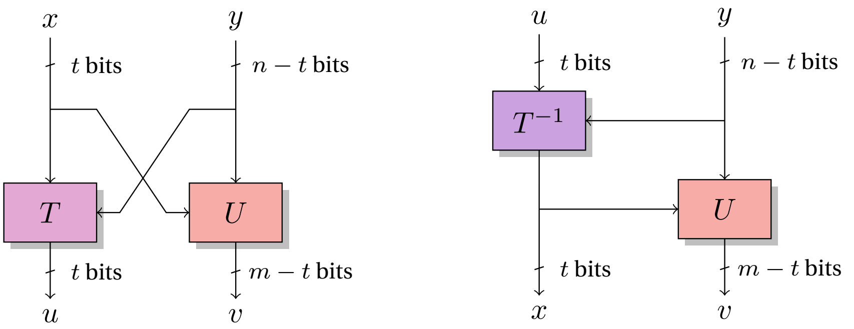
Then F and G are t-*twist-equivalent* if T_y is a permutation for all y and

$$G(u,y) \ = \ (T_y^{-1}(u), U_{T_y^{-1}(u)}(y)) \,.$$

When two functions F and G are t-twist equivalent there exists a swap matrix M_t, i.e. a matrix mapping the graph of the function F to the graph of the function G, such that

$$\Gamma_F \ = \ \left\{ (x, F(x)) \mid x \in \mathbb{F}_2^n \right\} \ = \ M_t\left\{ (x, G(x)) \mid x \in \mathbb{F}_2^n \right\} .$$

Such an equivalence is depicted in Figure 2.1.



(a) $F(x,y) = (T_y(x), U_x(y))$.

(b) $G(u,y) = (T_y^{-1}(u), U_{T_y^{-1}(u)}(y))$.

Figure 2.1: *t-twist equivalence.*

Example 2.3. One simple example of t-twist equivalence is the inverse transformation. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. The graph of F and F^{-1}, where

$$\Gamma_{F^{-1}} = \{(y, F^{-1}(y)), y \in \mathbb{F}_{2^n}\} = \{(F(x), x), x \in \mathbb{F}_{2^n}\} ,$$

are linked with the following relation

$$\begin{pmatrix} x \\ F(x) \end{pmatrix} = \begin{pmatrix} 0 & \mathcal{I}_n \\ \mathcal{I}_n & 0 \end{pmatrix} \begin{pmatrix} F(x) \\ x \end{pmatrix} ,$$

where $\mathcal{I}_n$ is the identity matrix of size n. This implies that F and F^{-1} are n-twist equivalent with the swap matrix

$$M_n = \begin{pmatrix} 0 & \mathcal{I}_n \\ \mathcal{I}_n & 0 \end{pmatrix} .$$

Theorem 2.1 (Theorem 3 in [CP19]). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be two CCZ-equivalent functions. We can obtain G from F or F from G by composing:*

1. *an EA transformation,*
2. *a t-twist, and*
3. *an EA transformation.*

It follows that if F and G are two CCZ-equivalent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ then, their graphs are connected by the following relation:

$$\Gamma_F = (A \cdot M_t \cdot B)(\Gamma_G) ,$$

with M_t a swap matrix and A, B EA-mappings.

2.1.2 Link with Arithmetization-Orientation

In the previous section, we have seen that CCZ-equivalence preserves differential and linear properties. Let us now show that this equivalence has also good properties for arithmetization-orientation. First, let us consider a function F defined over $\mathbb{F}_q$, where q is given by other parts of the protocol. In order for F to be arithmetization-oriented, it is usually necessary that the verification $y = F(x)$ can be done using a small number of multiplications in $\mathbb{F}_q$. A very straight-forward approach, and indeed the first considered for instance in MiMCHash [Alb+16] or Poseidon [Gra+21], consists in using a function F which, itself, can be evaluated using a few multiplications. This approach corresponds to the "type I" Arithmetization-Oriented primitives presented in Chapter 1. The downside of this approach is the use of a low-degree round function which may imply a vulnerability to some attacks based on polynomial system solving, also known as *algebraic attacks* (see Chapter 4). As a consequence, these algorithms have to use a high number of rounds.

A first breakthrough on this topic was made by the designers of *Rescue* [Aly+20]. They noticed that if F is a permutation, then the verification $y = F(x)$ is equivalent to the verification $x = F^{-1}(y)$. It allows them to use both x^d and $x^{1/d}$ over $\mathbb{F}_q$ in their round function, where $\gcd(d, q-1) = 1$ and where d is chosen to minimize the number of multiplications. It means that both operations can be verified using a cheap evaluation of x^d, and at the same time that the degree of the round function is very high as $1/d$ is a dense integer in $\mathbb{Z}/(q-1)\mathbb{Z}$. As a consequence, much fewer rounds are needed to prevent algebraic attacks.

In this chapter, we go further and propose a generalization of such insight. So far, we have seen that arithmetization-orientation implies that a function or its inverse must have a particular implementation property: a low number of multiplications. In fact, we claim the following

Claim 2.1. *A function is arithmetization-oriented if it is* CCZ-equivalent *to a function that can be verified efficiently.*

As a permutation and its inverse are known to be CCZ-equivalent, this insight is a natural generalization of the one proposed by the *Rescue* designers. To exploit this idea, we suppose that F and G are such that $\Gamma_G = \mathcal{L}(\Gamma_F)$, where $\mathcal{L} : (x, y) \mapsto (\mathcal{L}_L(x, y), \mathcal{L}_R(x, y))$ is a linear permutation, and where G can be efficiently verified. Then we can use F to construct an arithmetization-oriented algorithm since we show in the following proposition that checking if $y = F(x)$ is equivalent to checking if $\mathcal{L}_R(x, y) = G(\mathcal{L}_L(x, y))$.

Proposition 2.1. *Let F and G be two functions from $\mathbb{F}_q$ to $\mathbb{F}_q$ such that $\Gamma_G = \mathcal{L}(\Gamma_F)$. Then $y = F(x)$ if and only if $\mathcal{L}_R(x, y) = G(\mathcal{L}_L(x, y))$.*

Proof. Let us the notation $u = \mathcal{L}_L(x, y)$ and $v = \mathcal{L}_R(x, y)$. Then we have $(x, y) = \mathcal{L}^{-1}(u, v)$. First, let us assume that $y = F(x)$. We have

$$\Gamma_G = \{\mathcal{L}(x, F(x)), x \in \mathbb{F}_q\} = \{\mathcal{L}(x, y), x, y \in \mathbb{F}_q\} = \{(u, v), u, v \in \mathbb{F}_q\} ,$$

implying that $v = G(u)$, i.e. we have $\mathcal{L}_R(x, y) = G(\mathcal{L}_L(x, y))$. Similarly, if $\mathcal{L}_R(x, y) = G(\mathcal{L}_L(x, y))$, i.e. if $v = G(u)$, then we have

$$\Gamma_F = \{\mathcal{L}^{-1}(u, G(u)), u \in \mathbb{F}_q\} = \{\mathcal{L}^{-1}(u, v), u, v \in \mathbb{F}_q\} = \{(x, y), x, y \in \mathbb{F}_q\} ,$$

implying that $y = F(x)$. □

This verification implies that the evaluation is secure using a high-degree function F, and the verification is efficient since it only involves G and linear functions. In Table 2.1 we compare the three different approaches.

As we have already mentioned, the performance metrics for arithmetization-oriented algorithms differ substantially from the usual ones in symmetric cryptography. Neither the number of CPU cycles, nor the RAM consumption or the code size are the dominant factors. At the same

Approach		Operation	Cost
Poseidon-like	Evaluation	$y \leftarrow F(x)$	F is of low degree
	Verification	$y = F(x)$	F is of low degree
Rescue-like	Evaluation	$y \leftarrow F(x)$	F is of high degree
	Verification	$x = F^{-1}(y)$	F^{-1} is of low degree
our	Evaluation	$y \leftarrow F(x)$	F is of high degree
	Verification	$\mathcal{L}_R(x,y) = G\left(\mathcal{L}_L(x,y)\right)$	G is of low degree

Table 2.1: *Different approaches for AO.*

time, determining exactly what is needed for the various protocols relying on arithmetization is a difficult task as each protocol has its own subtleties. For instance, while $\mathcal{P}\mathfrak{lon}\mathcal{K}$ supports custom gates, a flexibility that other proof systems may not have, achieving the optimal arithmetic representation of a statement may be more difficult because of those degrees of freedom proof systems developers have. On the other hand, while additions and permutations of a sequence of field elements are likely to incur cost in $\mathcal{P}\mathfrak{lon}\mathcal{K}$, in the form of copy-constraints, they are free in R1CS. As a first approach, in this chapter we will mainly focus on the R1CS cost. Then, in the following we will investigate the efficiency of different CCZ-equivalent constructions for R1CS.

2.2 Butterflies

Our first idea to use the CCZ-equivalence to design an arithmetization-oriented function is to consider Butterflies. Butterflies were introduced by Perrin *et al.* in [PUB16] when they discovered that the only known APN permutations on an even number of bits [Bro+10] had this structure. Generalizations of this structure were then studied in more details by several teams [CDP17; Li+18; CPT19]. While butterflies were originally defined over binary fields $(\mathbb{F}_{2^n})^2$ for n odd, we propose a similar structure over any field.

In what follows, we let q be a power of a non-trivial prime number, and $\mathbb{F}_q$ be the finite field with q elements. Furthermore, let d be an exponent such that $\gcd(d, q-1) = 1$ (i.e. such that $x \mapsto x^d$ is a permutation of $\mathbb{F}_q$), and (α, β) be a pair of non-zero elements of $\mathbb{F}_q$.

Let us investigate the cryptographic properties (differential and linear properties) and the performance in terms of R1CS constraints of the butterfly.

2.2.1 Definition

Before generalizing butterflies to any field, we first recall classical definitions and properties.

Definition 2.6 (Butterflies)**.** A *closed butterfly* is a function of $(\mathbb{F}_q)^2$ defined by

$$\mathsf{V}_{\alpha,\beta} : \begin{cases} (\mathbb{F}_q)^2 & \to (\mathbb{F}_q)^2 \\ (x,y) & \mapsto \left((x+\alpha y)^d + \beta y^d, (y+\alpha x)^d + \beta x^d\right) , \end{cases}$$

or in other words $\mathsf{V}_{\alpha,\beta}(x,y) = (R(x,y), R(y,x))$ where $R(x,y) = (x+\alpha y)^d + \beta y^d$. This function is CCZ-equivalent to the corresponding *open butterfly*, a permutation (in fact, an involution) of

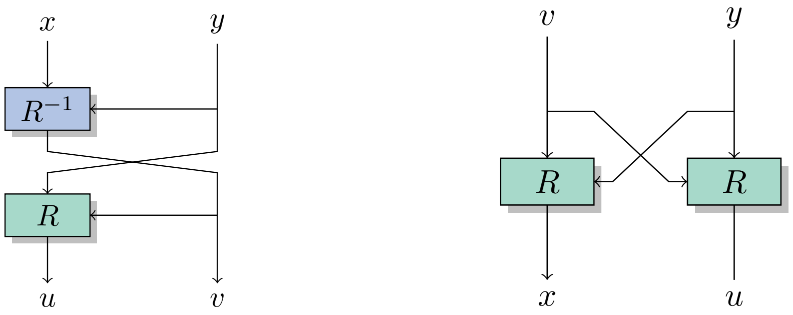
$(\mathbb{F}_q)^2$ defined by

$$\mathsf{H}_{\alpha,\beta} : \begin{cases} (\mathbb{F}_q)^2 \to & (\mathbb{F}_q)^2 \\ (x,y) \mapsto & \Big(\left(\alpha(x-\beta y^d)^{1/d} + (1-\alpha^2)y\right)^d + \beta\left((x-\beta y^d)^{1/d} - \alpha y\right)^d , \\ & \qquad\qquad (x-\beta y^d)^{1/d} - \alpha y \Big) . \end{cases}$$

Let us notice that we can simplify the definition of the open butterfly by using that $x \mapsto R(x,y)$ is a permutation for all y. If we write R_y this permutation and R_y^{-1} its inverse, so that $R_y^{-1}(x) = (x-\beta y^d)^{1/d} - \alpha y$, then we get that

$$\mathsf{H}_{\alpha,\beta}(x,y) = \left(R_{R_y^{-1}(x)}(y), R_y^{-1}(x) \right) .$$

These structures are presented in Figure 2.2.



(a) The open butterfly $\mathsf{H}_{\alpha,\beta}$ (bijective).

(b) The closed butterfly $\mathsf{V}_{\alpha,\beta}$.

Figure 2.2: The butterfly constructions, where $R_y(x) = (x+\alpha y)^d + \beta y^d$.

The detailed construction of butterflies is depicted in Figure 2.3.

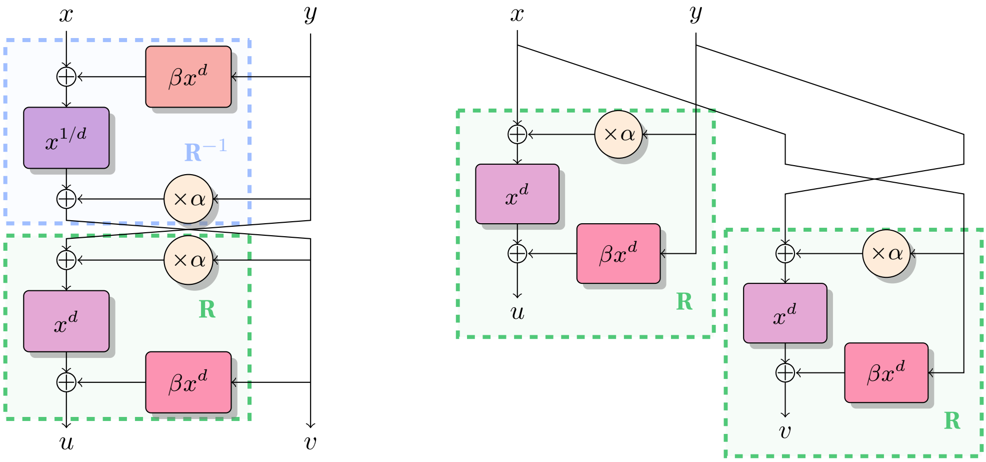
As stated in their definition, these two types of functions are *CCZ-equivalent*, meaning that there exists an affine permutation of $(\mathbb{F}_q)^2$ mapping the graph of $\mathsf{H}_{\alpha,\beta}$ to that of $\mathsf{V}_{\alpha,\beta}$. To see why, we simply notice that

$$\begin{aligned} \left\{ \left((x,y), \mathsf{H}_{\alpha,\beta}(x,y)\right), (x,y) \in \mathbb{F}_q^2 \right\} &= \left\{ \left((x,y), \left(R_{R_y^{-1}(x)}(y), R_y^{-1}(x)\right)\right), (x,y) \in \mathbb{F}_q^2 \right\} \\ &= \mathcal{L}\left\{ \left((R_y^{-1}(x), y), \left(x, R_{R_y^{-1}(x)}(y)\right)\right), (x,y) \in \mathbb{F}_q^2 \right\} \\ &= \mathcal{L}\left\{ \left((v,y), (x, R_v(y))\right), (v,y) \in \mathbb{F}_q^2 \right\} \\ &= \mathcal{L}\left\{ \left((v,y), \mathsf{V}_{\alpha,\beta}(v,y)\right), (v,y) \in \mathbb{F}_q^2 \right\} , \end{aligned}$$

where $\mathcal{L} : ((v,y),(x,u)) \mapsto ((x,y),(u,v))$ is linear. Therefore, this corresponds to a twist-equivalence, as defined in Section 2.1.1, where $T = U = R$.

In practice, another simple way of seeing CCZ-equivalence in the particular case of butterflies is

$$(u,v) = \mathsf{H}_{\alpha,\beta}(x,y) \Leftrightarrow (x,u) = \mathsf{V}_{\alpha,\beta}(v,y) .$$



(a) *Open.* **(b)** *Closed.*

Figure 2.3: *The two variants of the butterfly.*

2.2.2 Designs over binary fields

The case of binary fields is already well-studied and we know some of the butterfly properties in this context. In particular let us recall the theorem in [CDP17]. While the case $n = 3$ was of particular interest in this paper due to its relation with the big APN problem, it is not a value of n that is relevant here, so we restate the theorem in the case where $n > 3$.

Proposition 2.2 (Main Theorem of [CDP17]). *The cryptographic properties of the butterfly structures with $d = 3$ over $\mathbb{F}_{2^n}$, $n > 3$, are as follows:*

- *if $\beta = (\alpha + 1)^3$ then the differential uniformity is equal to 2^{n+1}, the linearity is equal to $2^{(3n+1)/2}$ and the algebraic degree of $\mathsf{H}_{\alpha,\beta}$ is equal to n;*
- *otherwise, the differential uniformity is equal to 4, the linearity to 2^{n+1}, and the algebraic degree of $\mathsf{H}_{\alpha,\beta}$ is equal to $n + 1$ unless $1 + \alpha\beta + \alpha^4 = (\beta + \alpha + \alpha^3)^2$, in which case it is equal to n.*

As a consequence, for any odd $n > 3$, choosing α and β such that

$$\begin{cases} (\alpha + 1)^3 + \beta & \neq \ 0 \\ 1 + \alpha\beta + \alpha^4 & \neq \ (\beta + \alpha + \alpha^3)^2 \end{cases}$$

yields a permutation $\mathsf{H}_{\alpha,\beta}$ with excellent cryptographic properties.

Since open and closed butterflies are CCZ-equivalent, they have the same differential and linear properties.

If $\mathsf{H}_{\alpha,\beta}(x, y) = (u, v)$, then it holds that $\mathsf{H}_{\alpha,\beta}(\lambda^d x, \lambda y) = (\lambda^d u, \lambda v)$. This makes open butterflies somewhat similar to power maps as those have the property that $(\lambda x)^d = \lambda^d x^d$. It was shown in [Bey+20b] that such a multiplicative property could potentially lead to some problem in the hash function *Rescue–Prime*.

However, this problem is easy to solve in the case of butterflies. For instance, we could simply compose $\mathsf{H}_{\alpha,\beta}$ with the linear permutation $(x, y) \mapsto (x + y, y)$ to get rid of this pattern.

2.2.3 Investigating new designs over prime fields

We generalize the butterfly constructions with the function R:

$$R(x,y) = (x+\alpha y)^d + \beta y^e\ .$$

In what follows we will use $\mathsf{H}^{d,e}_{\alpha,\beta}$ to denote the open butterfly with parameters α and β, using $x \mapsto x^e$ as a quadratic function and $x \mapsto x^d$ as a permutation. Consequently, $\mathsf{V}^{d,e}_{\alpha,\beta}$ will denote its corresponding closed variant. Then, the butterflies introduced before, $\mathsf{H}_{\alpha,\beta}$ and $\mathsf{V}_{\alpha,\beta}$, will now be denoted $\mathsf{H}^{d,d}_{\alpha,\beta}$ and $\mathsf{V}^{d,d}_{\alpha,\beta}$ respectively.

We will investigate different cases to see the influence of the exponents e and d in terms of cryptographic properties and performances. First experimental results indicate that there should always exist pairs (α,β) such that the corresponding butterflies with $d=3$ is differentially 4-uniform, though the "bad" cases are more common than in the binary field case.

For each case we also investigate the number of R1CS constraints for the verification, i.e. to check that

$$(u,v) = \mathsf{V}^{d,e}_{\alpha,\beta}(x,y)\ .$$

2.2.3.1 When $(d,e) = (3,3)$

Let us first investigate a construction close to the one in even characteristic. To do so, we let $d=e=3$, so that $R(x,y) = (x+\alpha y)^3 + \beta y^3$. This implies that $p \not\equiv 1 \bmod 3$.

The *closed butterfly* is then defined by

$$\mathsf{V}^{3,3}_{\alpha,\beta} : \begin{cases} (\mathbb{F}_p)^2 & \to (\mathbb{F}_p)^2 \\ (x,y) & \mapsto \left((x+\alpha y)^3 + \beta y^3, (y+\alpha x)^3 + \beta x^3\right)\ , \end{cases}$$

and the corresponding *open butterfly* is defined by:

$$\mathsf{H}^{3,3}_{\alpha,\beta} : \begin{cases} (\mathbb{F}_p)^2 \to & (\mathbb{F}_p)^2 \\ (x,y) \mapsto & \Big(\alpha^3(x-\beta y^3) + \beta\left((x-\beta y^2)^{1/3} - \alpha y\right)^3\ , \\ & \qquad (x-\beta y^2)^{1/3} - \alpha y\Big)\ , \end{cases}$$

The two variants of the butterfly are presented in Figure 2.4.

Then let us identify the pairs (α,β) such that the corresponding butterfly has differential uniformity at most 4. Investigating differential uniformity for such a construction is complicated since it highly depends on the values of α and β. Therefore, although we did not manage to identify pairs (α,β) leading to good differential properties, we propose some directions.

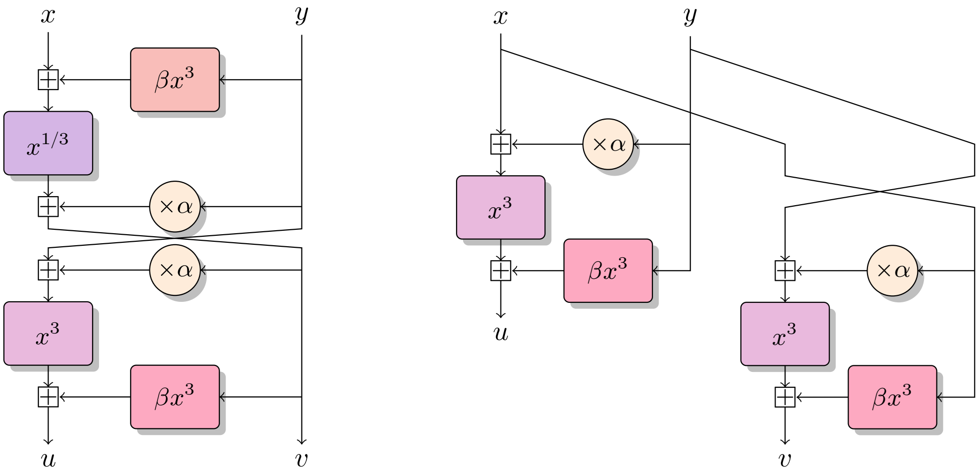
By looking at all pairs (α,β) for small values of p, i.e. $p \in \{11,17,23,29,41,47,53,59\}$ we notice that there is a symmetry between pairs (α,β) and $(-\alpha,-\beta)$. Indeed, let

$$R_{\alpha,\beta}(x,y) = (x+\alpha y)^3 + \beta y^3\ .$$

Then, we have:

$$R_{-\alpha,-\beta}(-x,y) = (-x-\alpha y)^3 - \beta y^3 = -R_{\alpha,\beta}(x,y)\ .$$

In Chapter 1 we saw that we can represent the DDT of a function with a picture. Here, we do not represent the DDT but the differential uniformity for all pairs (α,β) such that in row α and column β we have the differential uniformity of the open butterfly $\mathsf{H}^{3,3}_{\alpha,\beta}$. The idea behind



(a) *Open.* ***(b)*** *Closed.*

Figure 2.4: *The two variants of the butterfly when* $(d, e) = (3, 3)$.

Figure 2.5 is then to identify good pairs of (α, β). On this figure, the lightest color (yellow) refers to the case where the differential uniformity δ is at most 4, the intermediate colors (red) refer to cases $\delta \leqslant p$ and $\delta \leqslant p + 1$, and the darkest color (black) refers to the case $\delta \leqslant 2p - 1$. We can in particular recover the symmetry we have just mentioned between pairs (α, β) and $(-\alpha, -\beta)$.

Moreover in Figure 2.6 we represent the number of pairs (α, β) we obtain for each value of the differential uniformity.

Then, we notice four distinct cases:

1. The differential uniformity is at most 4 for around 60% of the pairs (α, β)
   In particular, it seems to occur for degenerate cases. It happens, for example, for pairs:

$$(\alpha, \beta) \in \left\{(1, 1), (-1, -1), (2, -2), (-2, 2), \left(\frac{p-1}{2}, \frac{p-1}{2}\right), \left(\frac{p+1}{2}, \frac{p+1}{2}\right)\right\} .$$

2. The differential uniformity is greater than 4 and at most p for around 35% of the pairs (α, β)
   It seems to occur for example when:

$$\beta \in \{(1-\alpha)^3, -(1+\alpha)^3, -\alpha^2 + \alpha\} .$$

3. The differential uniformity is at most $p + 1$ for around 2.5% of the remaining pairs (α, β).

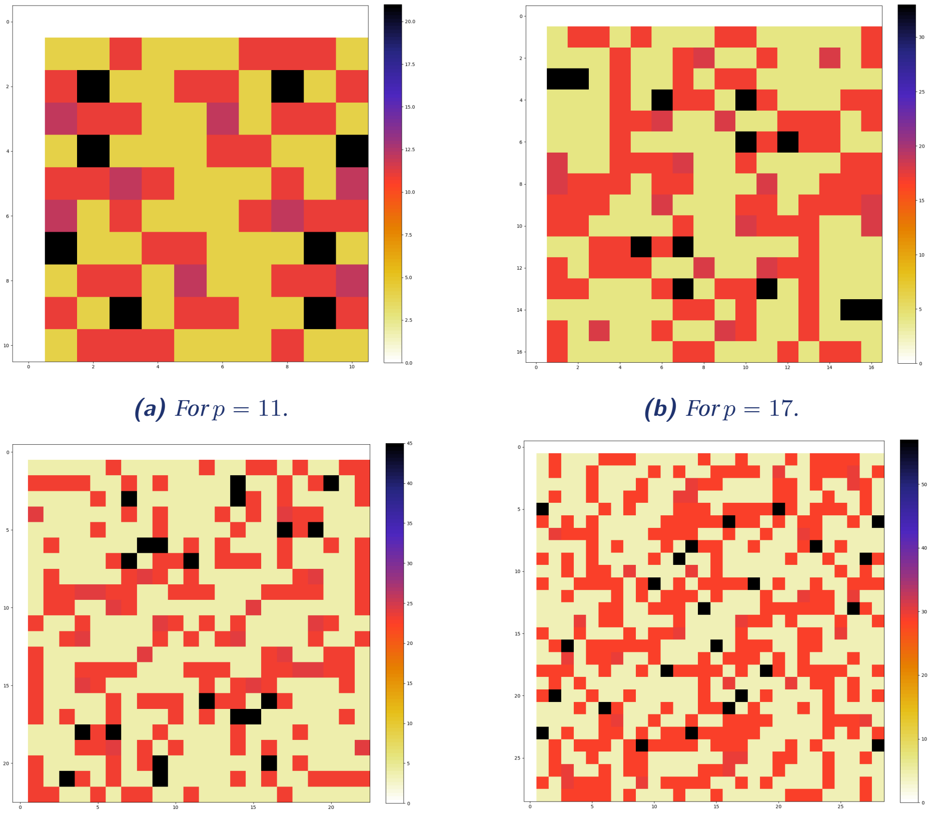
4. The differential uniformity is at most $2p - 1$ for around 2.5% of the remaining pairs (α, β).

However we did not manage to prove this observation.

Cost estimation

Let us investigate the R1CS cost of this butterfly structure. We recall that

$$\mathsf{V}^{3,3}_{\alpha,\beta}(x, y) = \big(R(x, y), R(y, x)\big) ,$$



(a) *For $p = 11$.*

(b) *For $p = 17$.*

(c) *For $p = 23$.*

(d) *For $p = 29$.*

Figure 2.5: *Differential uniformity for all pairs (α, β).*

where

$$\begin{cases} R(x,y) & = (x+\alpha y)^3 + \beta y^3 \ , \\ R(y,x) & = (y+\alpha x)^3 + \beta x^3 \ . \end{cases}$$

We have the following equations:

$$\begin{array}{llll} r_1 = x + \alpha y & & u_1 = y + \alpha x & \\ r_2 = r_1^2 & (+1) & u_2 = u_1^2 & (+1) \\ r_3 = r_1 \times r_2 & (+1) & u_3 = u_1 \times u_2 & (+1) \\ s_2 = y^2 & (+1) & v_2 = x^2 & (+1) \\ s_3 = y \times s_2 & (+1) & v_3 = x \times v_2 & (+1) \\ t = r_3 + \beta s_3 & & w = u_3 + \beta v_3 \ , & \end{array}$$

implying that $\mathsf{V}^{3,3}_{\alpha,\beta}(x,y) = (t,w)$. So, in this case, we need 8 constraints without expanding the polynomials. Then, by expanding the polynomials, we notice that we can save 2 constraints. We have

$$\begin{cases} R(x,y) & = x^3 + 3\alpha x^2 y + 3\alpha^2 x y^2 + \alpha^3 y^3 + \beta y^3 \\ R(y,x) & = y^3 + 3\alpha y^2 x + 3\alpha^2 y x^2 + \alpha^3 x^3 + \beta x^3 \ , \end{cases}$$

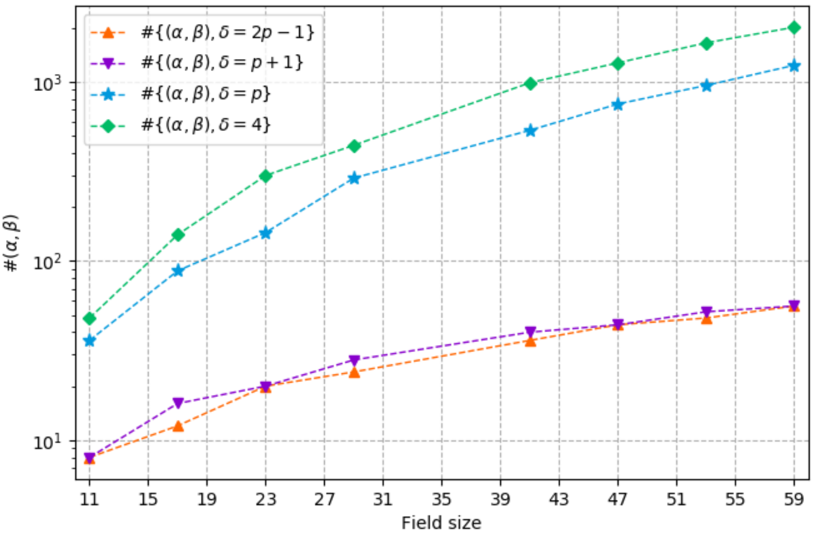


Figure 2.6: *Number of pairs (α, β) such that the differential uniformity has specific values.*

so that the equations for the verification are

$$\begin{array}{llll} r_2 = x^2 & \textit{(+1)} & t = y \times r_2 & \textit{(+1)} \\ r_3 = x \times r_2 & \textit{(+1)} & u = x \times s_2 & \textit{(+1)} \\ s_2 = y^2 & \textit{(+1)} & v = r_3 + 3\alpha t + 3\alpha^2 u + (\alpha^3 + \beta) s_3 & \\ s_3 = y \times s_2 & \textit{(+1)} & w = s_3 + 3\alpha u + 3\alpha^2 t + (\alpha^3 + \beta) r_3 \,. & \end{array}$$

This implies that $\mathsf{V}^{3,3}_{\alpha,\beta}(x, y) = (v, w)$ and we indeed have 6 R1CS constraints.

2.2.3.2 When $(d, e) = (3, 2)$

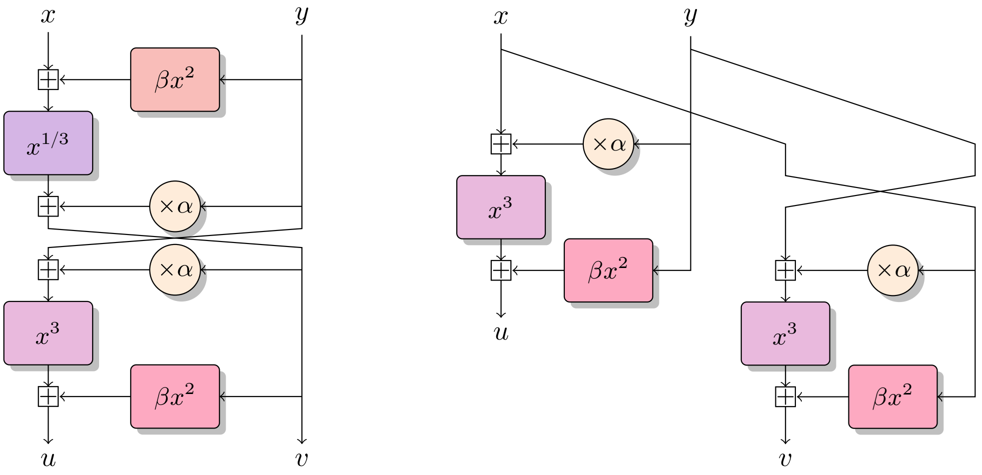
Since we did not manage to precisely investigate the differential uniformity of the previous design, we suggest to change the value of e to use a quadratic function instead, i.e. a function with univariate degree 2. While we do not use a square in $\mathbb{F}_{2^n}$ since it is linear, we can use it as a quadratic function in $\mathbb{F}_p$.

Then let $R(x, y) = (x + \alpha y)^3 + \beta y^2$. The *closed butterfly* is defined by

$$\mathsf{V}^{3,2}_{\alpha,\beta} : \begin{cases} (\mathbb{F}_p)^2 & \to (\mathbb{F}_p)^2 \\ (x, y) & \mapsto \left((x + \alpha y)^3 + \beta y^2, (y + \alpha x)^3 + \beta x^2\right) , \end{cases}$$

and the corresponding *open butterfly* is defined by:

$$\mathsf{H}^{3,2}_{\alpha,\beta} : \begin{cases} (\mathbb{F}_p)^2 \to & (\mathbb{F}_p)^2 \\ (x, y) \mapsto & \Big(\left(\alpha(x - \beta y^2)^{1/3} + (1 - \alpha^2) y\right)^3 + \beta \left((x - \beta y^2)^{1/3} - \alpha y\right)^2 , \\ & \qquad (x - \beta y^2)^{1/3} - \alpha y \Big) , \end{cases}$$



(a) *Open.* ***(b)*** *Closed.*

Figure 2.7: *The two variants of the butterfly when* $(d, e) = (3, 2)$.

where $\alpha^3 \neq \alpha$ and $\beta \neq 0$. Both variants are described in Figure 2.7.

For this variant we are now able to prove that the construction is differentially 4-uniform whatever the values of α and β are (except some sporadic cases).

Proposition 2.3. *Let* $R(x, y) = (x+\alpha y)^3+\beta y^2$*, where* $\alpha^3 \neq \alpha$ *and* $\beta \neq 0$*. Then, the corresponding butterfly has differential uniformity at most* 4.

Proof. First, we note that the condition $\alpha^3 \neq \alpha$ is equivalent to $\alpha^3 - \alpha \neq 0$, i.e. we need to ensure that $\alpha(\alpha + 1)(\alpha - 1) \neq 0$. Thus, it is equivalent to $\alpha \notin \{0, 1, p - 1\}$. Let a_1, a_2, b_1, b_2 be elements of $\mathbb{F}_p$ such that $(a_1, a_2) \neq (0, 0)$. Then, to investigate the differential uniformity of $\mathsf{V}^{3,2}_{\alpha,\beta}$, we need to determine the number of solutions of

$$\mathsf{V}^{3,2}_{\alpha,\beta}(x + a_1, y + a_2) - \mathsf{V}^{3,2}_{\alpha,\beta}(x, y) = (b_1, b_2)\,.$$

This is the same as looking at the number of solutions (x, y) of System (2.1):

$$\begin{cases} R(x + a_1, y + a_2) - R(x, y) = b_1 \\ R(y + a_2, x + a_1) - R(y, x) = b_2\,. \end{cases} \tag{2.1}$$

We have:

$$\begin{cases} R(x + a_1, y + a_2) - R(x, y) & = (x + a_1 + \alpha(y + a_2))^3 + \beta(y + a_2)^2 - (x + \alpha y)^3 - \beta y^2 \\ R(y + a_2, x + a_1) - R(y, x) & = (y + a_2 + \alpha(x + a_1))^3 + \beta(x + a_1)^2 - (y + \alpha x)^3 - \beta x^2\,. \end{cases}$$

Since $\alpha^2 \neq 1$, we can re-write this system using $u = a_1 + \alpha a_2$, and $v = \alpha a_1 + a_2$ i.e. we have $a_1 = (\alpha v - u)/(\alpha^2 - 1)$, and $a_2 = (\alpha u - v)/(\alpha^2 - 1)$:

$$\begin{cases} R(x + a_1, y + a_2) - R(x, y) = (x + \alpha y + u)^3 + \beta(y + a_2)^2 - (x + \alpha y)^3 - \beta y^2 \\ R(y + a_2, x + a_1) - R(y, x) = (y + \alpha x + v)^3 + \beta(x + a_1)^2 - (y + \alpha x)^3 - \beta x^2\,. \end{cases}$$

Let ℓ_1 and ℓ_2 be the rows of this system. Developing the first row yields

$$\begin{aligned}\ell_1 &= ((x+\alpha y)+u)^3 + \beta\,(y+a_2)^2 - (x+\alpha y)^3 - \beta y^2\\ &= (x+\alpha y)^3 + 3u(x+\alpha y)^2 + 3u^2(x+\alpha y) + u^3 + \beta y^2 + 2\beta a_2 y + \beta a_2^2 - (x+\alpha y)^3 - \beta y^2\\ &= 3ux^2 + 6u\alpha xy + 3\alpha^2 uy^2 + 3u^2x + 3\alpha u^2 y + u^3 + 2\beta a_2 y + \beta a_2^2\\ &= 3ux^2 + 3u^2x + 3\alpha^2 uy^2 + y(3\alpha u^2 + 2\beta a_2) + 6\alpha uxy + \underbrace{u^3 + \beta a_2^2}_{R(a_1,a_2)}\ .\end{aligned}$$

Similarly, the second row becomes

$$\ell_2 = 3vy^2 + 3v^2y + 3\alpha^2 vx^2 + x(3\alpha v^2 + 2\beta a_1) + 6\alpha vxy + \underbrace{v^3 + \beta a_1^2}_{R(a_2,a_1)}\ ,$$

and we obtain

$$\begin{cases}\ell_1 = R(a_1,a_2) + 3ux^2 + 3u^2x + 6u\alpha xy + 3u\alpha^2y^2 + y(3u^2\alpha + 2a_2\beta) = b_1\\ \ell_2 = R(a_2,a_1) + 3vy^2 + 3v^2y + 6v\alpha xy + 3v\alpha^2x^2 + x(3v^2\alpha + 2a_1\beta) = b_2\ .\end{cases}$$

By setting $c = b_1 - R(a_1,a_2)$, and $d = b_2 - R(a_2,a_1)$, the system becomes:

$$\begin{cases}c = 3ux^2 + 3u^2x + 6u\alpha xy + 3u\alpha^2y^2 + (3u^2\alpha + 2a_2\beta)y\\ d = 3vy^2 + 3v^2y + 6v\alpha xy + 3v\alpha^2x^2 + (3v^2\alpha + 2a_1\beta)x\ .\end{cases}$$

Recalling that α is a nonzero element of $\mathbb{F}_p$, we can write $x = \alpha^{-1}(z-y)$, so that

$$\begin{cases}c = 3u\alpha^{-2}(z-y)^2 + 3u^2\alpha^{-1}(z-y) + 6u(z-y)y + 3u\alpha^2y^2 + (3u^2\alpha + 2a_2\beta)y\\ d = 3vy^2 + 3v^2y + 6v(z-y)y + 3v(z-y)^2 + (3v^2\alpha + 2a_1\beta)\alpha^{-1}(z-y)\ ,\end{cases}$$

which implies:

$$\begin{cases}c &= 3u\alpha^{-2}z^2 + 3u^2\alpha^{-1}z + 6u(1-\alpha^{-2})zy + 3u(\alpha^{-2}+\alpha^2-2)y^2\\ &\quad +(3u^2(\alpha-\alpha^{-1}) + 2a_2\beta)y\\ d &= 3vz^2 + (3v^2 + 2a_1\alpha^{-1}\beta)z - 2a_1\alpha^{-1}\beta y\ .\end{cases} \tag{2.2}$$

We recall that $\alpha \neq 0$ and $\beta \neq 0$. If $a_1 \neq 0$, then the coefficient of y does not vanish in the second equation. Therefore, we obtain a relation of the form:

$$y = \mu_2 z^2 + \mu_1 z + \mu_0\ ,$$

where $\mu_0 = -d\alpha(2a_1\beta)^{-1}$, $\mu_1 = 3v^2\alpha(2a_1\beta)^{-1} + 1$, and $\mu_2 = 3v\alpha(2a_1\beta)^{-1}$. Then, replacing y in the first line of System (2.2), we get:

$$\nu_4 z^4 + \nu_3 z^3 + \nu_2 z^2 + \nu_1 z + \nu_0 = 0\ .$$

Now let us show that at least one coefficient is nonzero. For instance we have:

$$\begin{aligned}\nu_4 &= 3u(\alpha^{-2} + \alpha^2 - 2)\mu_2^2\\ &= 27uv^2(\alpha-\alpha^{-1})^2\alpha^2(2a_1\beta)^{-2}\ ,\end{aligned}$$

where $\alpha - \alpha^{-1} \neq 0$, $\alpha \neq 0$, $a_1 \neq 0$ and $\beta \neq 0$, implying that if u and v are different from 0 then $\nu_4 \neq 0$. Let us assume that $u = 0$ or $v = 0$, and let us consider another coefficient. We have

$$\nu_2 = 3u\alpha^2 + 6u(1-\alpha^{-2})\mu_1 + 3u(\alpha^{-2} + \alpha^2 - 2)(2\mu_2\mu_0 + \mu_1^2) + (3u^2(\alpha - \alpha^{-1}) + 2a_2\beta)\mu_2\,.$$

Then if $u = 0$, we have $a_2 = -a_1\alpha^{-1} \neq 0$ and $v = a_1(\alpha - \alpha^{-1}) \neq 0$ implying that

$$\nu_2 = 2a_2\beta\mu_2 = 6a_2\beta v\alpha(2a_1\beta)^{-1} \neq 0\,.$$

Similarly, if $v = 0$, we have $u = a_1(1-\alpha^2)$ and $\mu_1 = \mu_2 = 0$, implying that

$$\nu_2 = 3u\alpha^{-2} \neq 0\,.$$

Therefore, we have a nonzero polynomial of degree 4 in z, so at most four solutions z_0, z_1, z_2, z_3. Besides for each choice of z we have one solution for y and then one for x. It follows that we have at most four solutions (x, y).

If $a_1 = 0$, then $u = \alpha a_2$ and $v = a_2$, so that System (2.2) becomes:

$$\begin{cases} c &= 3a_2\alpha^{-1}z^2 + 3a_2^2\alpha z + 6a_2(\alpha-\alpha^{-1})zy + 3a_2(\alpha^{-1}+\alpha^3-2\alpha)y^2 \\ & \quad +(3a_2^2(\alpha^3-\alpha) + 2a_2\beta)y \\ d &= 3a_2z^2 + 3a_2^2z = d'\,. \end{cases}$$

Since $a_1 = 0$, we have necessarily $a_2 \neq 0$, implying that the coefficients in the second equation are nonzero. Then, from the second equation, we deduce that there are at most two solutions z_0, z_1 for z. Then by replacing z in the first equation, we get at most two solutions $y_{i,0}, y_{i,1}$ for each z_i. Finally, for each value $y_{i,j}$, there is one solution for x. As a consequence, we have at most four solutions (x, y).

We deduce that the differential uniformity is at most 4 when $R(x,y) = (x+\alpha y)^3 + \beta y^2$. □

We did not go into the details of linear cryptanalysis since as we will see in Section 2.3.3.2, such an analysis is rather complicated. In the example shown in Figure 2.8, the maximum value of the module of the Walsh transform is 34.65.

Cost estimation

Let us investigate the R1CS cost for such a construction. We aim at finding the number of constraints necessary to perform the verification:

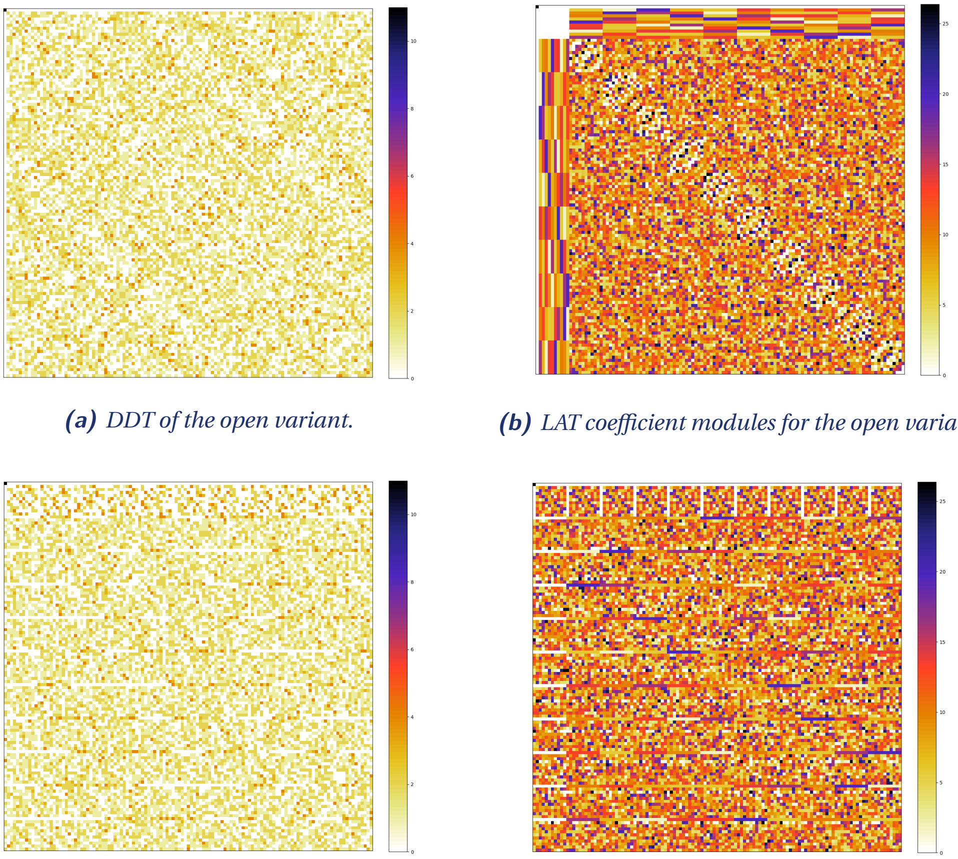
$$\mathsf{V}^{3,2}_{\alpha,\beta}(x,y) = \big(R(x,y), R(y,x)\big)\,,$$

where

$$\begin{cases} R(x,y) &= (x+\alpha y)^3 + \beta y^2, \\ R(y,x) &= (y+\alpha x)^3 + \beta x^2\,. \end{cases}$$

So to perform the verification we need the following equations:

$$\begin{array}{llllll} r_1 &= x + \alpha y & & u_1 &= y + \alpha x & \\ r_2 &= r_1^2 & \textit{(+1)} & u_2 &= u_1^2 & \textit{(+1)} \\ r_3 &= r_1 \times r_2 & \textit{(+1)} & u_3 &= u_1 \times u_2 & \textit{(+1)} \\ s &= y^2 & \textit{(+1)} & v &= x^2 & \textit{(+1)} \\ t &= r_3 + \beta s & & w &= u_3 + \beta v\,. & \end{array}$$



(a) *DDT of the open variant.*

(b) *LAT coefficient modules for the open variant.*

(c) *DDT of the closed variant.*

(d) *LAT coefficient modules for the closed variant.*

Figure 2.8: *DDT and representations of the modules of the coefficients in the LAT when* $p = 11$, $(d, e) = (3, 2)$ *and* $(\alpha, \beta) = (2, 1)$.

Then $\mathsf{V}^{3,2}_{\alpha,\beta}(x, y) = (t, w)$. Among all equations, 6 involve a multiplication, implying that such a verification requires 6 constraints.

Let us see if we can save some constraints by expanding the polynomials. We have

$$\begin{aligned} R(x, y) &= x^3 + 3\alpha x^2 y + 3\alpha^2 x y^2 + \alpha^3 y^3 + \beta y^2 \\ R(y, x) &= y^3 + 3\alpha y^2 x + 3\alpha^2 y x^2 + \alpha^3 x^3 + \beta x^2 \ . \end{aligned}$$

It follows that we need the following equations for the verification:

$$\begin{array}{lllllll} r_2 & = x^2 & \textit{(+1)} & \quad t & = y \times r_2 & & \textit{(+1)} \\ r_3 & = x \times r_2 & \textit{(+1)} & \quad u & = x \times s_2 & & \textit{(+1)} \\ s_2 & = y^2 & \textit{(+1)} & \quad v & = r_3 + 3\alpha t + 3\alpha^2 u + \alpha^3 s_3 + \beta s_2 & & \\ s_3 & = y \times s_2 & \textit{(+1)} & \quad w & = s_3 + 3\alpha u + 3\alpha^2 t + \alpha^3 r_3 + \beta r_2 \ . & & \end{array}$$

Then $\mathsf{V}^{3,2}_{\alpha,\beta}(x, y) = (v, w)$ and we also get 6 constraints.

2.2.3.3 $e = 2$ and $\alpha = \pm 1$

Since the cube is not always a permutation in $\mathbb{F}_p$, let us come back to the more general case where the main exponent is d. We keep $e = 2$ but to simplify computations we fix $\alpha = \pm 1$. Then the construction is a degenerate case of Butterfly corresponding to a 3-round Feistel network. In particular, it is relevant to study the butterflies with $e = 2$ since we have an interesting result on the differential uniformity. Note that such a 3-round Feistel network, in $\mathbb{F}_{2^n}$, was already studied in [LW14] when investigating S-boxes with good cryptographic properties for low hardware implementation cost.

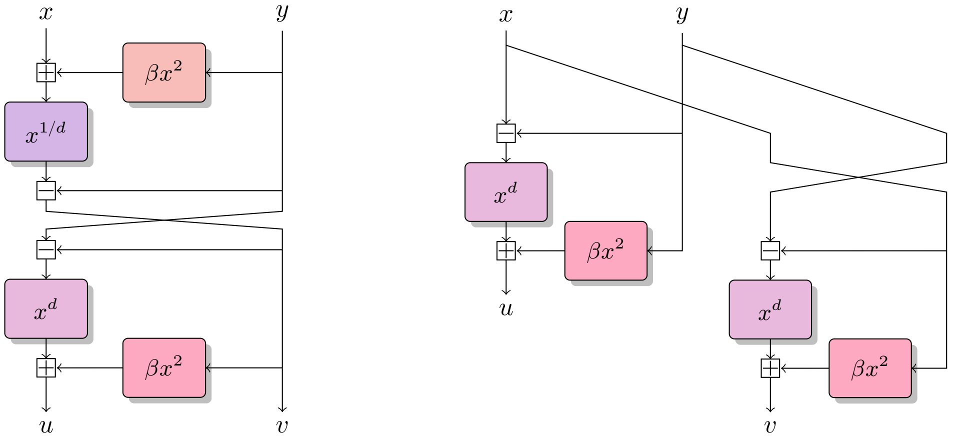
The *closed butterfly* is then defined by

$$\mathsf{V}_{\alpha,\beta}^{d,2} : \begin{cases} (\mathbb{F}_p)^2 & \to (\mathbb{F}_p)^2 \\ (x,y) & \mapsto \left((x+\alpha y)^d + \beta y^2, (y+\alpha x)^d + \beta x^2\right) , \end{cases}$$

And the corresponding *open butterfly* is defined by:

$$\mathsf{H}_{\alpha,\beta}^{d,2} : \begin{cases} (\mathbb{F}_p)^2 \to & (\mathbb{F}_p)^2 \\ (x,y) \mapsto & \Big(\alpha^d(x-\beta y^2) + \beta\left((x-\beta y^2)^{1/d} - \alpha y\right)^2 , \\ & \qquad (x-\beta y^2)^{1/d} - \alpha y\Big) , \end{cases}$$

The two butterflies are depicted in Figure 2.9 with $\alpha = -1$. Let us note that the open butterfly can be described as a 3-round Feistel network as described in Figure 2.10.



(a) *Open.* **(b)** *Closed.*

Figure 2.9: *The two variants of the butterfly when $e = 2$ and $\alpha = -1$.*

Let us investigate the differential properties of this construction.

Proposition 2.4. *Let $R(x,y) = (x+\alpha y)^d + \beta y^2$, where $\alpha = \pm 1$. Then, the corresponding butterfly has differential uniformity at most $d-1$.*

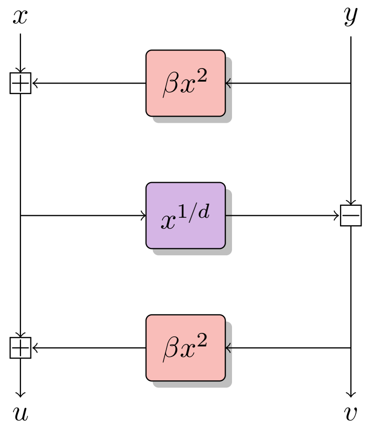


Figure 2.10: Simplified representation of the open butterfly when $e = 2$ and $\alpha = -1$

Proof. Let a_1, a_2, b_1, b_2 be elements of $\mathbb{F}_p$ such that $(a_1, a_2) \neq (0, 0)$. To investigate the differential uniformity of $\mathsf{V}^{d,2}_{\alpha,\beta}$, with $\alpha = \pm 1$, we look at the number of solutions (x, y) of System (2.3):

$$\begin{cases} R(x + a_1, y + a_2) - R(x, y) = b_1 \\ R(y + a_2, x + a_1) - R(y, x) = b_2 \, . \end{cases} \tag{2.3}$$

We have:

$$\begin{cases} R(x + a_1, y + a_2) - R(x, y) &= (x + a_1 + \alpha(y + a_2))^d + \beta(y + a_2)^2 - (x + \alpha y)^d - \beta y^2 \\ R(y + a_2, x + a_1) - R(y, x) &= (y + a_2 + \alpha(x + a_1))^d + \beta(x + a_1)^2 - (y + \alpha x)^d - \beta x^2 \, . \end{cases}$$

As d is odd, the second line gives:

$$R(y + a_2, x + a_1) - R(y, x) = \alpha(x + a_1 + \alpha(y + a_2))^d + \beta(x + a_1)^2 - \alpha(x + \alpha y)^d - \beta x^2 \, .$$

Denoting respectively by ℓ_1 and ℓ_2 the rows of the system, we then get:

$$\begin{aligned} \ell_1 - \alpha \ell_2 = {} & (x + a_1 + \alpha(y + a_2))^d + \beta(y + a_2)^2 - (x + \alpha y)^d - \beta y^2 \\ & - \alpha^2(x + a_1 + \alpha(y + a_2))^d - \alpha\beta(x + a_1)^2 + \alpha^2(x + \alpha y)^d + \alpha\beta x^2 \, . \end{aligned}$$

As $\alpha^2 = 1$, it follows that:

$$\ell_1 - \alpha \ell_2 = \beta(y + a_2)^2 - \beta y^2 - \alpha\beta(x + a_1)^2 + \alpha\beta x^2 = b_1 - \alpha b_2 \, .$$

If $a_2 \neq 0$, this is equivalent to:

$$y = (2a_2)^{-1} \left(\alpha(2a_1 x + a_1^2) - a_2^2 + \beta^{-1}(b_1 - \alpha b_2) \right) = \alpha a_2^{-1} a_1 x + \mu \, ,$$

where $\mu = (2a_2)^{-1} \left(\alpha a_1^2 - a_2^2 + \beta^{-1}(b_1 - \alpha b_2) \right)$. Then we know that y can be expressed as a bijective affine polynomial in x. Moreover, we have

$$\begin{aligned}\ell_2 &= \alpha(x + a_1 + \alpha(y + a_2))^d + \beta(x + a_1)^2 - \alpha(x + \alpha y)^d - \beta x^2 \\ &= \alpha \sum_{j=0}^{d} \binom{d}{j} (x + \alpha y)^j (a_1 + \alpha a_2)^{d-j} + \beta(2a_1 x + a_1^2) - \alpha(x + \alpha y)^d \\ &= \alpha \sum_{j=0}^{d-1} \binom{d}{j} (x + \alpha y)^j (a_1 + \alpha a_2)^{d-j} + \beta(2a_1 x + a_1^2)\,.\end{aligned}$$

Let us assume that ℓ_2 is the zero polynomial. If $a_1 = -a_2$, then $x + \alpha y = \alpha\mu$ so that

$$\ell_2 = 2\beta a_1 x + \nu\,,$$

where ν is a constant. We have a contradiction since the coefficient $2\beta a_1$ is nonzero. Now, let $a_1 \neq -a_2$, and let $C(x) = x + \alpha y$. We have $C^{-1}(x) = (1 + a_2^{-1} a_1)^{-1}(x - \alpha\mu)$. If ℓ_2 is the zero polynomial, then

$$\ell_2 \circ C^1(x) = \alpha \sum_{j=0}^{d-1} \binom{d}{j} x^j (a_1 + \alpha a_2)^{d-j} + \beta(2a_1 C^{-1}(x) + a_1^2)$$

also equals 0 for any x. This implies that the coefficient of x^{d-1} i.e. $(a_1 + \alpha a_2)$ is 0. Then it remains the term

$$2\beta a_1 C^{-1}(x) + a_1^2) = \beta(2a_1(1 + a_2^{-1} a_1)^{-1}(x - \alpha\mu) + a_1^2)\,.$$

However $\beta(2a_1(1 + a_2^{-1} a_1)^{-1} \neq 0$ so we also have a contradiction.

Therefore ℓ_2 is a nonzero polynomial and we have at most $d - 1$ solutions for x. Finally, we have at most $d - 1$ solutions (x, y) for the system (since for each value of x, there is a single y).

Now, let us assume that $a_2 = 0$. Then we have

$$\ell_1 - \alpha\ell_2 = -\alpha\beta(2a_1 x + a_1^2) = b_1 - \alpha b_2\,,$$

where the coefficient $2\alpha\beta a_1$ is nonzero, implying that we have a nonzero polynomial of degree 1 in x. Then by replacing x in ℓ_1, we obtain

$$\ell_1 = \sum_{j=0}^{d} \binom{d}{j} (x + \alpha y)^j a_1^{d-j} - (x + \alpha y)^d = \sum_{j=0}^{d-1} \binom{d}{j} (x + \alpha y)^j a_1^{d-j}.$$

The coefficient of the term x^{d-1} is $a_1 \neq 0$ so that we have at most $d - 1$ solutions for y.

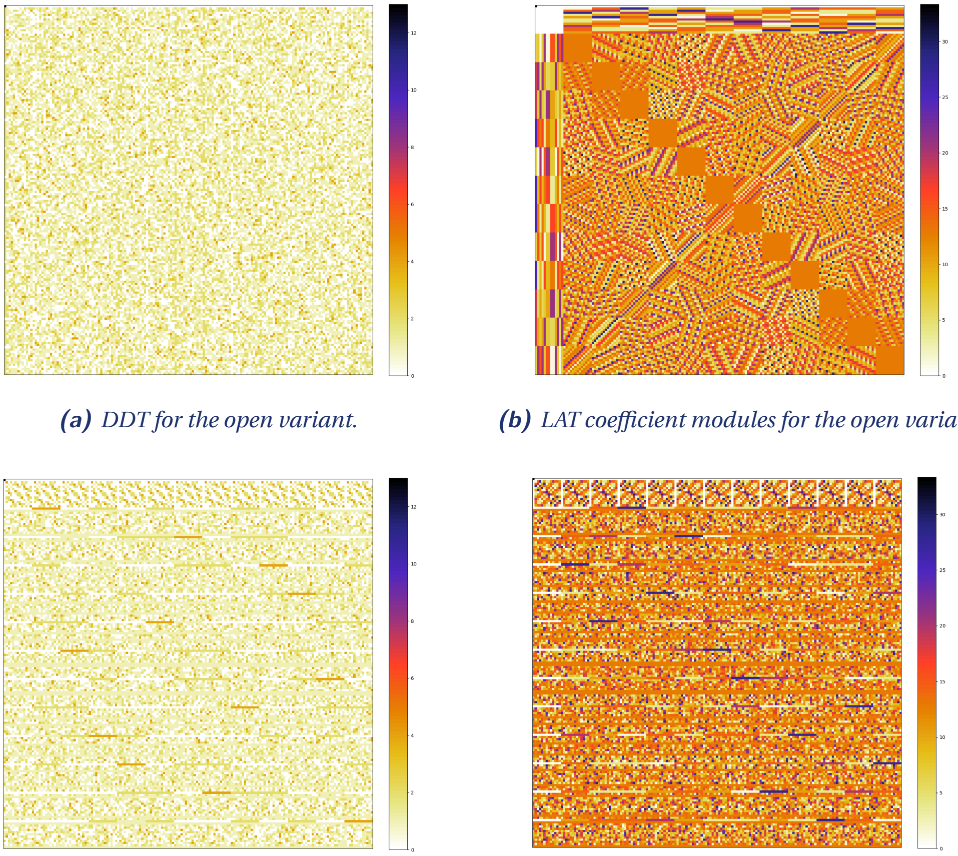
As a consequence, the differential uniformity is at most $d-1$ when $R(x, y) = (x \pm y)^d + \beta y^2$. □

We did not go into the details of linear cryptanalysis for the same reason as before. The maximum value of the module of the Walsh transform of the example chosen in Figure 2.11 is 29.91.

Cost estimation

Let us determine the R1CS cost of this construction. We recall that:

$$\mathsf{V}_{\alpha,\beta}^{d,2}(x, y) = \big(R(x, y), R(y, x)\big)\,.$$



(a) *DDT for the open variant.*

(b) *LAT coefficient modules for the open variant.*

(c) *DDT for the closed variant.*

(d) *LAT coefficient modules for the closed variant.*

Figure 2.11: *DDT and representations of the modules of the coefficients in the LAT when* $p = 13$, $(d, e) = (5, 2)$ *and* $(\alpha, \beta) = (-1, 1)$

where

$$\begin{cases} R(x, y) &= (x + \alpha y)^d + \beta y^2 \, , \\ R(y, x) &= (y + \alpha x)^d + \beta x^2 \, . \end{cases}$$

Since d is odd, let us notice that we can use the following relation

$$\alpha(x + \alpha y)^d = \alpha^d (x + \alpha y)^d = (\alpha x + y)^d \, ,$$

so that we save one exponentiation. Then, let us study some examples to see the influence of the exponent d. First, we investigate the cost of the butterfly with $d = 3$. In this case, it is more interesting to do not expand the polynomial $(x + \alpha y)^3$. The equations are:

$$\begin{aligned} r_1 &= x + \alpha y & & & s &= x^2 & &\textit{(+1)} \\ r_2 &= r_1^2 & &\textit{(+1)} & t &= y^2 & &\textit{(+1)} \\ r_3 &= r_1 \times r_2 & &\textit{(+1)} & u &= r_3 + \beta t & & \\ & & & & v &= \alpha r_3 + \beta s \, , & & \end{aligned}$$

so that $\mathsf{V}^{3,2}_{\alpha,\beta}(x,y) = (u,v)$. We have 4 constraints, while by expanding the polynomials we have

$$\begin{aligned} R(x,y) &= x^3 + 3\alpha x^2 y + 3\alpha^2 x y^2 + \alpha^3 y^3 + \beta y^2 \\ R(y,x) &= y^3 + 3\alpha y^2 x + 3\alpha^2 y x^2 + \alpha^3 x^3 + \beta x^2 \ , \end{aligned}$$

so that the verification can be performed with the following equations:

$$\begin{array}{llllll} r_2 & = x^2 & \textit{(+1)} & s_2 & = y^2 & \textit{(+1)} \\ r_3 & = x \times r_2 & \textit{(+1)} & s_3 & = y \times s_2 & \textit{(+1)} \\ t_1 & = y \times r_2 & \textit{(+1)} & t_2 & = x \times s_2 \ , & \textit{(+1)} \end{array}$$

and

$$\begin{aligned} u &= r_3 + 3\alpha t_1 + 3\alpha^2 t_2 + \alpha^3 s_3 + \beta s_2 \\ v &= s_3 + 3\alpha t_2 + 3\alpha^2 t_1 + \alpha^3 r_3 + \beta r_2 \ . \end{aligned}$$

We have $\mathsf{V}^{3,2}_{\alpha,\beta}(x,y) = (u,v)$ and we obtain 6 constraints.

Then, we investigate the cost of the butterfly with $d = 5$. As for the case $d = 3$, let us show that expanding the polynomials increases the number of constraints. If we expand the polynomial, we need 5 constraints, since we have the following equations:

$$\begin{array}{llllll} r_1 & = x + \alpha y & & s & = x^2 & \textit{(+1)} \\ r_2 & = r_1^2 & \textit{(+1)} & t & = y^2 & \textit{(+1)} \\ r_4 & = r_2^2 & \textit{(+1)} & u & = r_5 + \beta t & \\ r_5 & = r_1 \times r_4 & \textit{(+1)} & v & = \alpha r_5 + \beta s \ , & \end{array}$$

where $\mathsf{V}^{5,2}_{\alpha,\beta}(x,y) = (u,v)$.

By expanding the polynomials we obtain

$$\begin{aligned} R(x,y) &= x^5 + 5\alpha x^4 y + 10\alpha^2 x^3 y^2 + 10\alpha^3 x^2 y^3 + 5\alpha^4 x y^4 + \alpha^5 y^5 + \beta y^2 \\ R(y,x) &= y^5 + 5\alpha y^4 x + 10\alpha^2 y^3 x^2 + 10\alpha^3 y^2 x^3 + 5\alpha^4 y x^4 + \alpha^5 x^5 + \beta x^2 \ , \end{aligned}$$

leading to the following equations:

$$\begin{array}{llllll} r_2 & = x^2 & \textit{(+1)} & s_2 & = y^2 & \textit{(+1)} \\ r_3 & = x \times r_2 & \textit{(+1)} & s_3 & = y \times s_2 & \textit{(+1)} \\ r_4 & = r_2^2 & \textit{(+1)} & s_4 & = s_2^2 & \textit{(+1)} \\ r_5 & = x \times r_4 & \textit{(+1)} & s_5 & = y \times s_4 & \textit{(+1)} \\ t_1 & = r_4 \times s_1 & \textit{(+1)} & t_3 & = r_2 \times s_3 & \textit{(+1)} \\ t_2 & = r_3 \times s_2 & \textit{(+1)} & t_4 & = r_1 \times s_4 \ , & \textit{(+1)} \end{array}$$

and

$$\begin{aligned} u &= r_5 + 5\alpha t_1 + 10\alpha^2 t_2 + 10\alpha^3 t_3 + 5\alpha^4 t_4 + \alpha^5 s_5 + \beta s_2 \\ v &= s_5 + 5\alpha t_4 + 10\alpha^2 t_3 + 10\alpha^3 t_2 + 5\alpha^4 t_1 + \alpha^5 r_5 + \beta r_2 \end{aligned}$$

Then $\mathsf{V}^{5,2}_{\alpha,\beta}(x,y) = (u,v)$, so to perform the verification we need 12 constraints. More precisely, this corresponds to the cost of the exponentiation $x \mapsto x^5$ plus the cost of two squares. As a consequence, generalizing to all d, we have the following lemma.

Lemma 2.1. *The number of R1CS constraints we need for the verification*

$$\mathsf{V}^{d,2}_{\alpha,\beta}(x,y) = (u,v), \quad \textit{where } \alpha = \pm 1\,,$$

is the cost of two squares plus the cost of a fast exponentiation $x \mapsto x^d$.

Proof. As we saw in the previous examples, it is more efficient not to expand the polynomial when computing the number of constraints. Therefore, since

$$\mathsf{V}^{d,2}_{\alpha,\beta}(x,y) = \left((x+\alpha y)^d + \beta y^2, \alpha(x+\alpha y)^d + \beta x^2\right)\,,$$

we need one constraint for each of the two quadratics βy^2 and βx^2, and the number of constraints necessary to perform one exponentiation $(x+\alpha y)^d$. □

After studying different designs, we present the one we choose for the Anemoi permutations. The last approach studied in this section is so far the one leading to the best performances in terms of R1CS constraints, and good differential properties. Therefore it inspired the design of the Flystel structure. Our aim is to design a primitive as consistent as possible, using similar principles and round functions regardless of the field size or characteristic.

2.3 The Flystel Structure

In this section, we present a family of non-linear components that provide both the cryptographic properties that we need to ensure the security of our primitives, and efficient implementations across proof systems. We called it Flystel since it is highly inspired by the Butterfly structure and a Feistel network. The Flystel structure uses and highlights the connection between arithmetization-orientation and CCZ-equivalence.

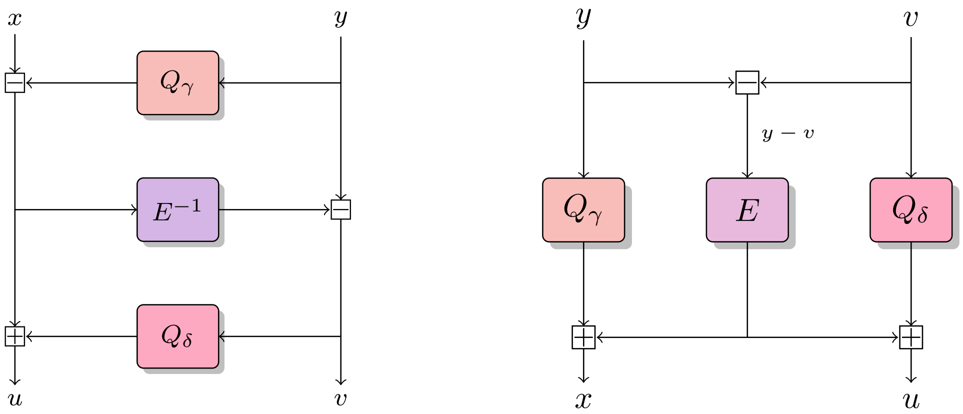
2.3.1 High-Level View of the Flystel Structure

We propose a design that works well for both fields of even and odd characteristics. Let $Q_\gamma : \mathbb{F}_q \to \mathbb{F}_q$ and $Q_\delta : \mathbb{F}_q \to \mathbb{F}_q$ be two quadratic functions (i.e. functions of algebraic degree 2 in $\mathbb{F}_{2^n}$ and of univariate degree 2 in $\mathbb{F}_p$) where γ and δ are constants of $\mathbb{F}_q$, and let $E : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation, where q is either a prime number or a power of 2. Then, the *Flystel* is a pair of functions relying on Q_γ, Q_δ and E. The *open Flystel* is the permutation of $\mathbb{F}_q^2$ obtained using a 3-round Feistel network with Q_γ, E^{-1}, and Q_δ as round functions, as depicted in Figure 2.12a. It is denoted $\mathcal{H}$, so that $\mathcal{H}(x,y) = (u,v)$ is evaluated as follows:

1. $x \leftarrow x - Q_\gamma(y)\,,$
2. $y \leftarrow y - E^{-1}(x)\,,$
3. $x \leftarrow x + Q_\delta(y)\,,$
4. $u \leftarrow x\,,\ v \leftarrow y\,.$

We define by $\mathcal{V} : (y,v) \mapsto (R_\gamma(y,v), R_\delta(y,v))$ the *closed Flystel* function over $\mathbb{F}_q^2$, where $R_\gamma : (y,v) \mapsto E(y-v) + Q_\gamma(y)$ and $R_\delta : (y,v) \mapsto E(y-v) + Q_\delta(v)$.

Our terminology of "open" for the permutation and "closed" for the function is based on the relationship between the Flystel and the butterfly structure, as detailed in Section 2.2. In particular, the two structures are CCZ-equivalent.



(a) Open `Flystel`, $\mathcal{H}$.

(b) Closed `Flystel`, $\mathcal{V}$.

Figure 2.12: The `Flystel` structure.

Proposition 2.5. *For a given tuple (Q_γ, E, Q_δ), the corresponding closed and open `Flystel` are CCZ-equivalent.*

Proof. Let $(u, v) = \mathcal{H}(x, y)$. Then it holds that $v = y - E^{-1}(x - Q_\gamma(y))$, so that we can write $x = E(y - v) + Q_\gamma(y)$. Similarly, we have that $u = Q_\delta(v) + E(y - v)$. Consider now the set $\Gamma_\mathcal{H} = \{((x, y), \mathcal{H}(x, y)), (x, y) \in \mathbb{F}_q^2\}$. By definition, we have

$$\Gamma_\mathcal{H} = \{((x, y), (u, v)), (x, y) \in \mathbb{F}_q^2\} = \mathcal{L}\big(\{((y, v), (x, u)), (x, y) \in \mathbb{F}_q^2\}\big)$$

where $\mathcal{L}$ is the permutation of $(\mathbb{F}_q^2)^2$ such that $\mathcal{L}^{-1}((x, y), (u, v)) = ((y, v), (x, u))$, which is linear. Using the equalities we established at the beginning of this proof, we can write:

$$\begin{aligned}
\mathcal{L}^{-1}(\Gamma_\mathcal{H}) &= \{((y, v), (x, u)), (x, y) \in \mathbb{F}_q^2\} \\
&= \big\{\big((y, v), (Q_\gamma(y) + E(y - v), Q_\delta(v) + E(y - v))\big), (y, v) \in \mathbb{F}_q^2\big\} \\
&= \big\{\big((y, v), \mathcal{V}(y, v)\big), (y, v) \in \mathbb{F}_q^2\big\} \\
&= \Gamma_\mathcal{V} .
\end{aligned}$$

We deduce that $\Gamma_\mathcal{H} = \mathcal{L}(\Gamma_\mathcal{V})$, so the two functions are CCZ-equivalent. □

This simple proposition has several crucial corollaries on which we will rely for the construction of `Anemoi`. The first one implies that it is sufficient to investigate the differential and linear properties of the closed butterfly to obtain results about the open one.

Corollary 2.1. *The open and closed `Flystel` structures have identical differential and linear properties. More precisely, the set of the values in the DDT of both functions is the same, and the set of the squares of the Walsh coefficients of the components is also the same.*

Proof. This follows from the CCZ-equivalence between both variants. □

The second corollary is the key reason behind the relevance of the `Flystel` structure in the arithmetization-oriented setting and is stated below.

Corollary 2.2. *Verifying that* $(u, v) = \mathcal{H}(x, y)$ *is equivalent to verifying that* $(x, u) = \mathcal{V}(y, v)$.

Proof. The proof follows from Proposition 2.1 since $\Gamma_{\mathcal{H}} = \mathcal{L}(\Gamma_{\mathcal{V}})$. □

Indeed, Corollary 2.2 means that it is possible to encode the verification of the evaluation of the high-degree open `Flystel` using the polynomial representation of the low-degree closed `Flystel`.

2.3.2 `Flystel`$_2$ and `Flystel`$_\mathrm{p}$

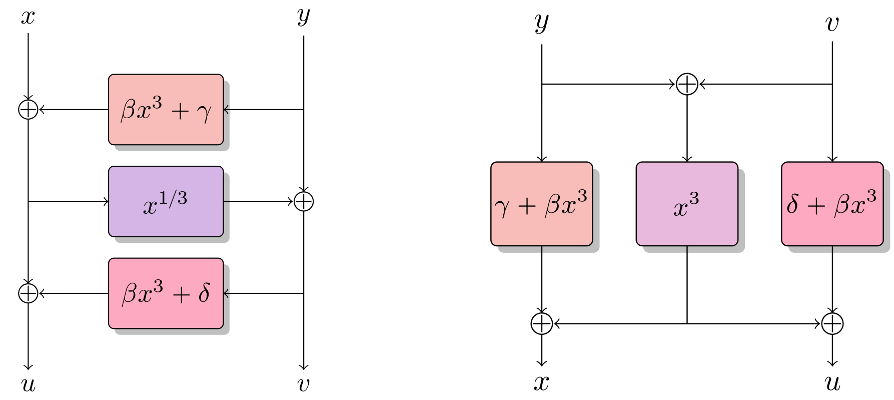
In characteristic 2, or in odd characteristic, quadratic mappings correspond to different exponents. As a consequence, when giving concrete instantiations of the `Flystel` structure, we need to treat each case separately. To highlight the difference, we call `Flystel`$_2$ the instances used in characteristic 2, and `Flystel`$_\mathrm{p}$ the instances used in prime characteristic p, with p odd.

For the sake of consistency with previous sections we do not use the same notation as in our original paper [Bou+23].

2.3.2.1 Characteristic 2

Let $q = 2^n$, with n odd. Furthermore, let $d = 2^j + 1$ be a Gold exponent such that $\gcd(j, n) = 1$, so that $x \mapsto x^d$ is a permutation of $\mathbb{F}_{2^n}$. In this case, the `Flystel`$_2$ structure with $Q_\gamma(x) = Q_\delta(x) = \beta x^d$, with $\beta \neq 0$, and with $E(x) = x^d$ is a degenerate generalized butterfly structure. It was studied in [Li+18] as a generalization of the structure introduced in [PUB16], which was also refined in [CDP17].

In practice, to prevent some attacks (see Section 3.3.3), we instead use $Q_\gamma(x) = \beta x^3 + \gamma$ and $Q_\delta(x) = \beta x^3 + \delta$, where γ and δ are constants of $\mathbb{F}_q$ such that $\gamma \neq \delta$. The resulting construction is depicted in Figure 2.13.



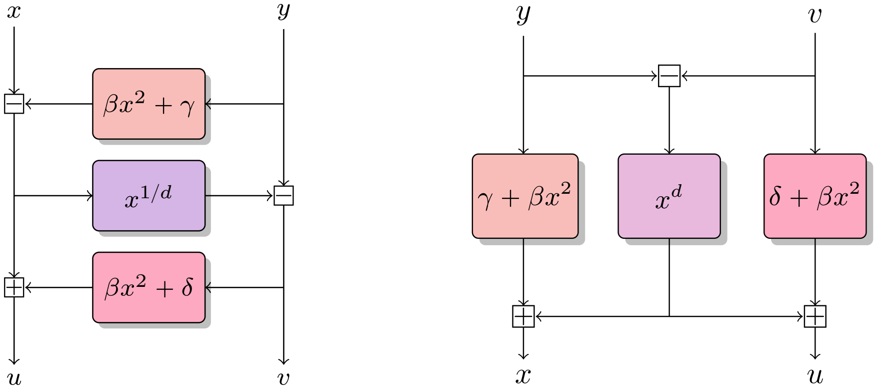
(a) *Open* `Flystel`$_2$. **(b)** *Closed* `Flystel`$_2$.

Figure 2.13: *The two variants of the* `Flystel`$_2$*, in characteristic 2.*

2.3.2.2 Odd Characteristic

Let $q = p$. In this case, the $\texttt{Flystel}_\texttt{p}$ structure uses three rounds functions: $Q_\gamma : x \mapsto \beta x^e + \gamma$, $E : x \mapsto x^{1/d}$, and $Q_\delta : x \mapsto \beta x^e + \delta$, where $\beta \in \mathbb{F}_p$ is non-zero, and where γ and δ are constants of $\mathbb{F}_p$. In odd characteristic, the square can be used as a quadratic function. Although the results still hold for any quadratic function, in what follows we fix $e = 2$.

We show the construction in Figure 2.14.



(a) *Open $\texttt{Flystel}_p$.* **(b)** *Closed $\texttt{Flystel}_p$.*

Figure 2.14: *The two variants of the $\texttt{Flystel}_p$, in odd characteristic.*

2.3.3 Cryptographic properties

Let us investigate the cryptographic properties of these constructions. For the $\texttt{Flystel}_2$, we will mainly rely on the result of Li *et al.* [Li+18], covering all generalized butterflies, not just those corresponding to Flystel structures.

2.3.3.1 Differential Properties

Such structures have a low differential uniformity. For the $\texttt{Flystel}_2$ the result by Li *et al.* for the differential uniformity hold only under some conditions, which in our context is equivalent to the fact that $\beta \neq 0$.

Proposition 2.6 (Theorem 3 in [Li+18]). *Let $q = 2^n$ with n odd, $E = x \mapsto x^d$, where $d = 2^j + 1$ is such that $\gcd(j, n) = 1$, and $Q_\gamma = Q_\delta = x \mapsto \beta x^d$, where $\beta \neq 0$. Then the $\texttt{Flystel}_2$ structures defined by the functions Q_γ, E, and Q_δ have a differential uniformity at most 4.*

In prime fields we also have a low differential uniformity. Such a property is actually a corollary of Proposition 2.4.

Corollary 2.3. *Let $q = p$ be a prime, $E = x \mapsto x^d$, where d is such that $\gcd(d, p-1) = 1$, and $Q_\gamma = x \mapsto \gamma + \beta x^2, Q_\delta = x \mapsto \delta + \beta x^2$ where $\beta \neq 0$. Then the $\texttt{Flystel}_p$ structures defined by the functions Q_γ, E, and Q_δ have a differential uniformity at most $d - 1$.*

Proof. The proof is similar to the one of Proposition 2.4. Let a_1, a_2, b_1, b_2 be elements of $\mathbb{F}_p$ such that $(a_1, a_2) \neq (0, 0)$. We investigate the number of solutions (y, v) of System (2.4):

$$\begin{cases} R_\gamma(y + a_1, v + a_2) - R_\gamma(y, v) = b_1 \\ R_\delta(y + a_1, v + a_2) - R_\delta(y, v) = b_2 \, , \end{cases} \tag{2.4}$$

where we have:

$$R_\gamma(y + a_1, v + a_2) - R_\gamma(y, v) = (y + a_1 - (v + a_2))^d + Q_\gamma(y + a_1) - (y - v)^d - Q_\gamma(y) \, ,$$

and similarly:

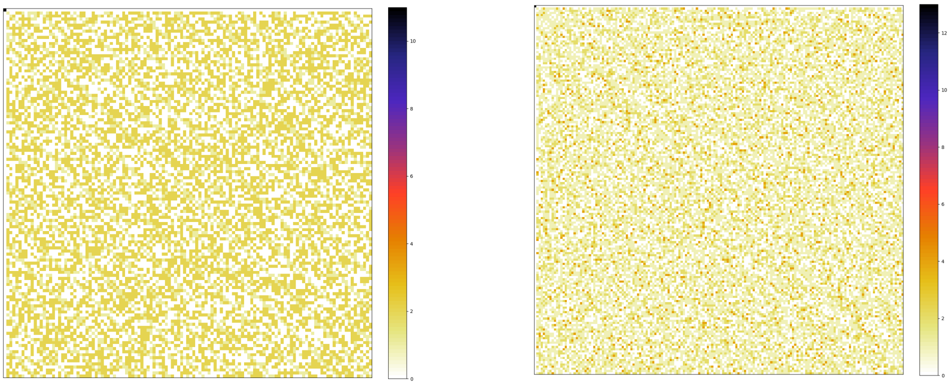
$$R_\delta(y + a_1, v + a_2) - R_\delta(y, v) = (y + a_1 - (v + a_2))^d + Q_\delta(v + a_2) - (y - v)^d - Q_\delta(v) \, .$$

Denoting respectively by ℓ_1 and ℓ_2 the rows of the system, we get:

$$\begin{aligned} \ell_1 - \ell_2 &= Q_\gamma(y + a_1) - Q_\gamma(y) - Q_\delta(v + a_2) + Q_\delta(v) \\ &= \gamma + \beta(y + a_1)^2 - \gamma - \beta y^2 - \delta - \beta(v + a_2)^2 + \delta + \beta v^2 \\ &= \beta(y + a_1)^2 - \beta y^2 + \beta v^2 - \beta(v + a_2)^2 \, . \end{aligned}$$

The end of the proof is then identical to that of Proposition 2.4, so that we have at most $d - 1$ solutions (y, v) for the system. □

In Figure 2.15 we show examples of the DDT representations for some instances of the $\texttt{Flystel}_\texttt{p}$.



(a) *$p = 11$ and $d = 3$.*

(b) *$p = 13$ and $d = 5$.*

Figure 2.15: *DDT of some open $\texttt{Flystel}$ instances.*

Interestingly, we have solved one open problem on Boolean functions, raised in [Zha+14], that was finding APN permutations over $\mathbb{F}_p^2$. Indeed we have exhibited such a function for all possible p with $p \not\equiv 1 \bmod 3$.

Theorem 2.2. *Let p be a prime number such that $\gcd(3, p - 1) = 1$, then the $\texttt{Flystel}_\texttt{p}$ with $E : x \mapsto x^3$ is an APN permutation over $\mathbb{F}_p^2$.*

Proof. According to Corollary 2.3, if the $\texttt{Flystel}_\texttt{p}$ is such that $E : x \mapsto x^3$ then the differential uniformity is at most $d - 1 = 2$, meaning that the $\texttt{Flystel}_\texttt{p}$ is an APN permutation. □

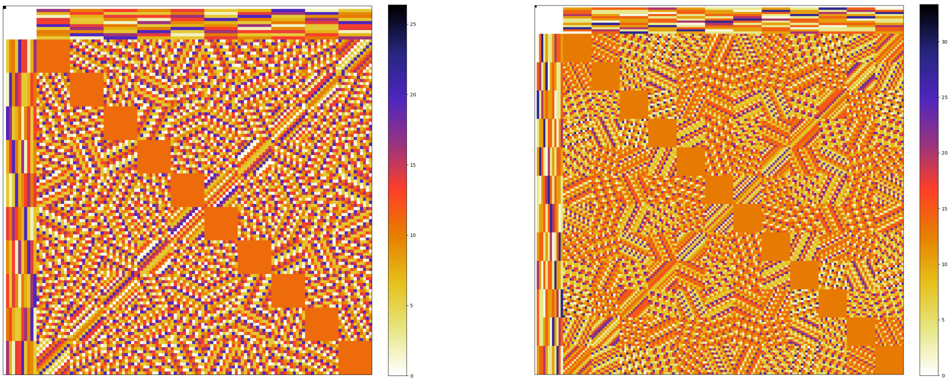
2.3.3.2 Linear Properties

In even characteristic we rely on the following proposition.

Proposition 2.7 (Theorem 4 in [Li+18])**.** *Let $q = 2^n$ with n odd, $E = x \mapsto x^d$, where $d = 2^j + 1$ is such that $\gcd(j, n) = 1$, and $Q_\gamma = Q_\delta = x \mapsto \beta x^d$, where $\beta \neq 0$. Then the $\texttt{Flystel}_2$ structures defined by the functions Q_γ, E, and Q_δ have a linearity equal to 2^{n+1}.*

Let us notice that, as for the differential uniformity, this proposition only holds when $\beta \neq 0$.

However, for prime fields, we do not have a theoretical bound on the linearity for the $\texttt{Flystel}_\texttt{p}$ structure. Nevertheless, we will argue that we do not expect any attack to come from this direction. In Figure 2.16 we show examples of representations of the module of the coefficients in the LAT for some instances of the $\texttt{Flystel}_\texttt{p}$. It is worth noticing that the LATs seem structured and this suggests that it could be possible to have a deeper understanding than the one we are proposing.



(a) *$p = 11$ and $d = 3$.*

(b) *$p = 13$ and $d = 5$.*

Figure 2.16: *Representations of the modules of the coefficients in the LAT for some open `Flystel` instances.*

Let us first notice that the $\texttt{Flystel}_\texttt{p}$ is defined by the functions Q_γ, E^{-1} and Q_δ, where Q_γ and Q_δ are quadratic. Given that the function x^2 is bent (i.e. that its correlations are the lowest possible), we can argue somewhat informally that a linear trail that would activate just one of these functions should be expected to have a very low correlation.

Second, our experiments indicate that the correlation increases slowly with the field size p. In fact, we have obtained the following conjecture for the maximum value of the module of its Walsh transform.

Conjecture 2.1. *If $q = p$ is a prime number, then the maximum module of the Walsh transform of $\mathcal{H}$ satisfies*

$$\max_{a \in \mathbb{F}_p^m, b \in \left(\mathbb{F}_p^m\right)^*} |\mathcal{W}_{\langle b, \mathcal{H} \rangle}(a)| \leqslant p \log p \,.$$

This conjecture has been verified experimentally for different values of p and d as shown in Figure 2.17. More precisely, it appears that for any value of d, $4p + 6$ might even be a better bound, but for $d = 3$, it seems that the most suitable bound is $2p$, and for $d = 5$, $3.5p$ as shown in Figure 2.18, where we go further, investigating the maximum value of the module of the Walsh transform for more values of p, selecting only the smallest d such that $x \mapsto x^d$ is a permutation in

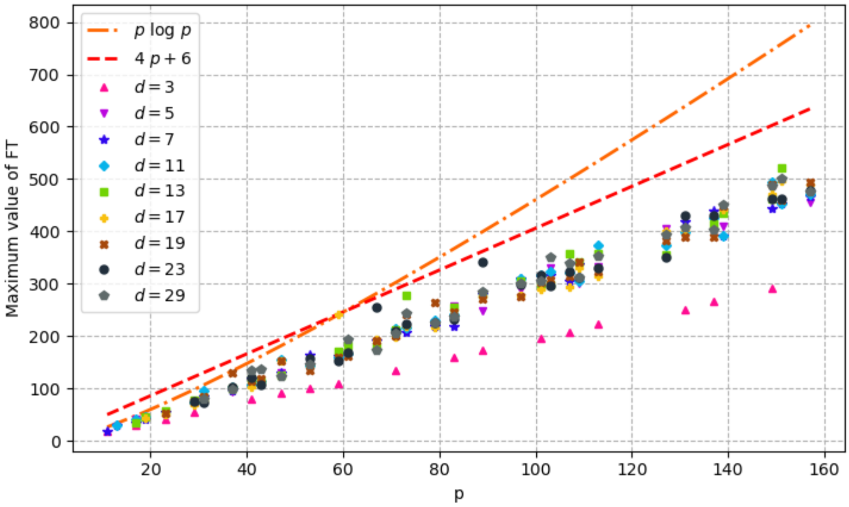


Figure 2.17: *Maximum value of the module of the Walsh transform of $\mathcal{H}$ for different exponent d.*

$\mathbb{F}_p$. While the most general case remains a conjecture at the time of writing, this result holds for small values of p ($p \leqslant 809$).

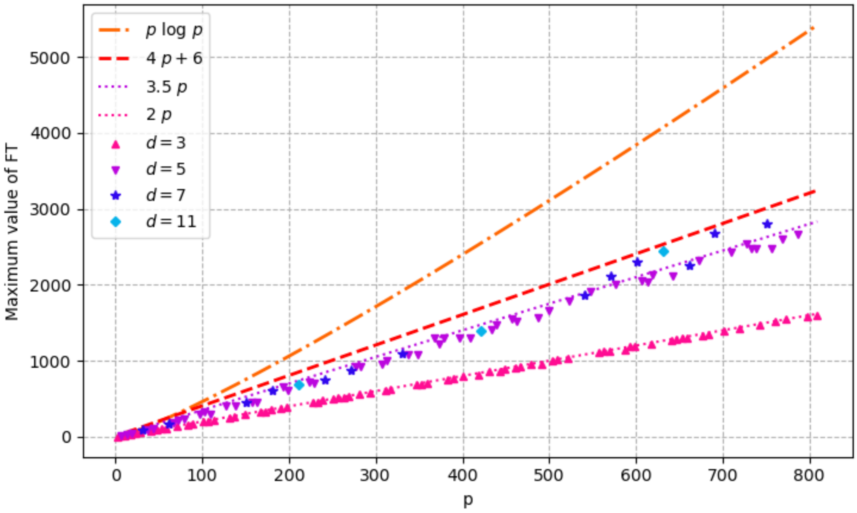


Figure 2.18: *Maximum value of the module of the Walsh transform of $\mathcal{H}$ for the smallest exponent d.*

2.3.3.3 Algebraic degree

Let us notice that for the algebraic degree, the condition given in [Li+18] to have a degree equal to $n+1$ degenerates into $\beta^{2^{j+1}} = \beta^{2^j+1}$, which never occurs as $j > 0$. Then we have the following proposition.

Proposition 2.8 (Theorem 5 in [Li+18])**.** *Let $q = 2^n$ with n odd, $E = x \mapsto x^d$, where $d = 2^j + 1$ is such that $\gcd(j, n) = 1$, and $Q_\gamma = Q_\delta = x \mapsto \beta x^d$, where $\beta \neq 0$. Then the $\texttt{Flystel}_2$ structures defined by the functions Q_γ, E, and Q_δ have an algebraic degree equal to n.*

Moreover, in odd characteristic, given the structure of the open $\texttt{Flystel}_\texttt{p}$, its degree is lower bounded by the inverse of d modulo $p-1$, a quantity which in practice corresponds to a dense integer of $\mathbb{Z}/(p-1)\mathbb{Z}$. We deduce that one call to this permutation is sufficient to thwart all attacks that would exploit the low degree of a component, such as higher-order differential attacks.

2.3.3.4 Invariant Subset

Regardless of the characteristic, it holds that $\mathcal{H}\left(Q_\gamma(x), x\right) = \left(Q_\delta(x), x\right)$. Thus, setting $Q_\gamma = Q_\delta$ would mean that the Flystel is the identity over a subset of size q, which is why we added constant additions to ensure that $Q_\gamma \neq Q_\delta$. Nevertheless, this only ensures that the open Flystel is a translation over the set $\{\left(Q_\gamma(x), x\right), x \in \mathbb{F}_q\}$, which remains cryptographically weak.

While a priori undesirable, the impact of this property can be mitigated. First, the subset over which it has a simple expression is not an affine space. Second, we will see in Chapter 3 that the propagation of such patterns can be broken using the linear layer.

In practice, and for simplicity, we will set, for both $\texttt{Flystel}_2$ and $\texttt{Flystel}_\texttt{p}$, $\beta = g$, $\gamma = g^{-1}$ and δ, where g is a generator of the multiplicative subgroup of the field $\mathbb{F}_q$.

2.3.4 Performances

2.3.4.1 R1CS cost

Let us estimate the number of constraints for R1CS. Using the closed Flystel of Figure 2.14b, we obtain the following verification equations:

$$\begin{cases} (y-v)^d + \beta y^2 + \gamma - x = 0 \\ (y-v)^d + \beta v^2 + \delta - u = 0\,. \end{cases}$$

Then, as a direct consequence of Lemma 2.1, the cost of evaluating one closed Flystel is the cost of one exponentiation $x \mapsto x^d$, and one constraint for each of the two squares.

2.3.4.2 $\mathcal{P}$lon$\mathcal{K}$ cost

As opposed to R1CS, additions now have a cost in $\mathcal{P}$lon$\mathcal{K}$. Therefore, evaluating the Flystel costs one constraint for each addition of a square, and one for each of the sums of x and u. We also need one constraint to derive $y - v$, and the cost of one exponentiation $x \mapsto x^d$.

Conclusion

In this chapter, we have shown the relevance of CCZ-equivalence in the context of Arithmetization-Orientation. After studying different constructions of butterflies, whose open and closed variants are known to be CCZ-equivalent, we finally opted for a degenerated case of such a construction that can be easily represented as a three-round Feistel network. The Flystel is the first non-linear component explicitly based on the link between Arithmetization-Orientation and CCZ-equivalence. Its strength lies in the fact that the open Flystel, composed of quadratic functions and a high-degree permutation, offers a good security level, while the closed Flystel allows an efficient verification using both quadratic functions and a low-degree permutation. We have proposed two variants, one in even-characteristic fields, $\texttt{Flystel}_2$, the other in odd-characteristic fields, $\texttt{Flystel}_\texttt{p}$. In the case of $\texttt{Flystel}_\texttt{p}$, we have proved that the differential uniformity of Flystel is at most $d-1$ when the permutation $x \mapsto x^d$ is used. Interestingly, by choosing $d = 3$, we answer the previously open problem of finding an APN function over $\mathbb{F}_p^2$, which then inspired recent works on Arithmetization-Oriented APN functions [BP23].

It is worth mentioning that Anemoi, that will be presented in the next chapter and which relies on Flystel as a non-linear layer, is the first primitive using the link between CCZ-equivalence and Arithmetization-Orientation. Such a discovery has already influenced the design of another Arithmetization-Oriented primitive, namely Arion [RST23]. Furthermore, we hope that further research in discrete mathematics will lead to new non-linear components that are even better suited to this use case: we need more permutations with good cryptographic properties (including a high degree) that are CCZ-equivalent to functions with a low number of multiplications. In particular, note that an SPN construction using the Flystel structure as non-linear layer must have an even-sized internal state. Therefore, it would be interesting to obtain a design with more than two branches to give more freedom in the choice of the size of the internal state.

Chapter 3
Designing Anemoi and Jive

In this chapter we present a new family of ZK-friendly hash-functions called Anemoi. More precisely, Anemoi can be used to construct efficient hash functions and compression functions, using dedicated modes. Anemoi relies on two new components: the Flystel, introduced in Chapter 2, and Jive, a new mode of operation inspired by the “Latin dance” symmetric algorithms like Salsa [Ber08b] or ChaCha [Ber08a]. Since the Anemoi permutation is an SPN construction relying on the Flystel for the non-linear layer, Anemoi is the first primitive using explicitly the link between CCZ-equivalence and Arithmetization-Orientation. In this chapter we aim at giving a precise view of the Anemoi construction and its relevance as an Arithmetization-Oriented primitive, investigating its security and performances within different proof systems.

In Section 3.1 we first present the two purposes of hash functions in ZK protocols, introducing Jive, our new mode for compression functions and one of the building blocks of Anemoi. Then, in Section 3.2 we present the Anemoi family of hash functions, describing the different components of the SPN construction. Section 3.3 is dedicated to the cryptanalysis of Anemoi, except algebraic attacks that will be discussed in Chapter 4. Finally, in Section 3.4 we show, via detailed benchmarks for different proof systems (R1CS, $\mathcal{P}$lon$\mathcal{K}$, AIR), that combining the Anemoi permutation with the Jive compression mode enables us to compete with the other Arithmetization-Oriented primitives in the literature.

Contents

3.1 Purposes of `Anemoi` hash functions

In advanced protocols, hash functions are used for two purposes. The first one is to emulate a random oracle, in particular to return the "fingerprint" or digest of a message of arbitrary length. The idea is that this fixed-length digest is simpler to sign than the full message. The second one is as a compression function within a Merkle-tree: in this case, the hash function H is used to map two inputs of size n to an output of size n, and the security of the higher-level scheme relies on its collision resistance.

While the sponge construction [Ber+07] is an elegant way to build a hash function from a permutation, we argue below that this approach may not be the most efficient in the specific case of a Merkle-tree. Indeed, to improve efficiency, we propose dedicated functions for each purpose. In Section 3.1.1 we propose to use a classical sponge construction for the random oracle. Then, since the specific constraints of the Merkle-tree case can be satisfied more efficiently using a dedicated structure that remains permutation-based, we introduce the `Jive` mode in Section 3.1.2.

3.1.1 Random Oracle: the Sponge Structure

A random oracle is essentially a theoretical function that picks each output uniformly at random while keeping track of its previous outputs in order to remain a deterministic function. The sponge construction is a convenient approach to try to emulate this behaviour. First introduced by Bertoni *et al.* in [Ber+07], this method was most notably used to design SHA-3 [Nat15]. It is also how most arithmetization-oriented hash functions have been designed, e.g. *Rescue–Prime* [SAD20], GMiMCHash [Alb+19b], Poseidon [Gra+21], and `Reinforced Concrete` [Gra+22a].

In this chapter, we slightly modify the original approach, introduced in Chapter 1 to operate on elements of $\mathbb{F}_q$ instead of $\mathbb{F}_2$. The overall principle of this modified sponge construction is depicted in Figure 3.1. Let us describe in more details the construction. The main component of the structure is a permutation P operating on $\mathbb{F}_q^{r+c}$, where both r and c are non-zero integers. We recall that r is the *rate* and corresponds to the size of the *outer part* of the state, while c is the *capacity* and corresponds to the size of the *inner part* of the state. The digest consists of h elements of $\mathbb{F}_q$. Then, to process a message m consisting of elements of $\mathbb{F}_q$, we apply three operations.

First, a basic *padding* is performed as follows: we append $1 \in \mathbb{F}_q$ to the message followed by enough zeroes so that the total length is a multiple of r, and then we split the result into blocks $m_0,\ldots,m_{t-1}$ of r elements in $\mathbb{F}_q$. However, this approach may lead to one more call to P in the case where the length of the message was already a multiple of r. A more efficient approach is presented in [Hir16]. If the length of the message is already a multiple of r, then we do not append further blocks to it. Instead, we add a constant to the capacity before squeezing. This is summarized as the addition of σ which is equal to 0 if the message length is not a multiple of r, and to 1 otherwise (see Figure 3.1). This variant also has the advantage of gracefully handling the case where $r = 1$.

Then, the *absorption* and *squeezing* work as described in Chapter 1. Indeed, for the absorption of each message block m_i, is added to the outer part of the state, and then P is applied to the full state. Finally, for the squeezing, we extract $\min(h, r)$ elements from the outer part of the state to generate the first elements of the digest. If $h > r$, we apply P and then extract additional elements again from the rate registers, repeating this process until the desired digest length is reached.

The security of a sponge relies on the properties of its permutation. Informally, the only special property of the permutation should be the existence of an efficient implementation. Its differential, linear, algebraic, etc. properties should be similar to those expected from a permutation picked uniformly at random from the set of all permutations.

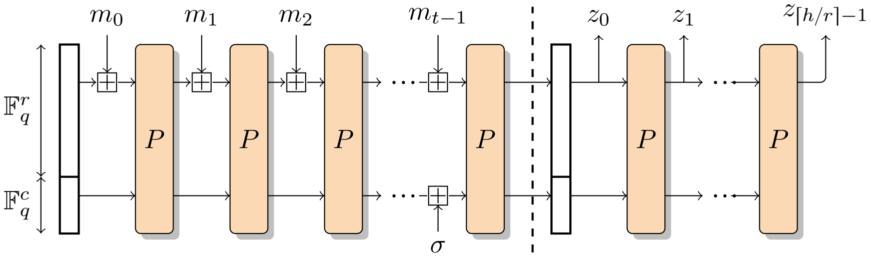


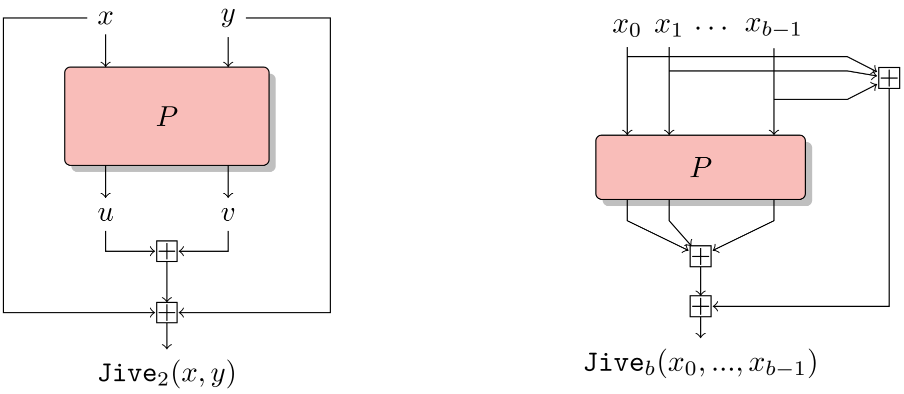
Figure 3.1: Sponge construction with the modification proposed by [Hir16].

Following a *flat sponge claim* [Ber+07] (a simplification such that only the worst-case probability of an attack is considered), the designers of such an algorithm can essentially claim that any attack against it will have a complexity equivalent to at least $q^{c/2}$ calls to the permutation (provided $h \geqslant c$, $h \log_2 q \geqslant 2s$ and $c \log_2 q \geqslant 2s$, where s is the required security level). Thus, a flat sponge claim states that a sponge-based hash function provides $c\lfloor \log_2 q \rfloor / 2$ bits of security.

3.1.2 Merkle Compression Function: the Jive Mode

One of the main use cases for an arithmetization-oriented hash function is the same as a compression function in a Merkle tree. This case could be easily handled using a regular hashing mode, such as the sponge structure discussed above. This perspective is also the one that was used so far. However, due to the specifics of this use case, it is possible to use a more efficient mode.

In a Merkle tree, the elements considered are in $\mathbb{F}_q^m$, where m is chosen so that $m\lfloor \log_2 q \rfloor \geqslant n$, so that n is the intended security level. We then need to hash two such elements to obtain a new one. As a consequence, unlike in the usual case, the input size is fixed, and is equal to exactly twice the digest size. More generally, given a permutation of $(\mathbb{F}_q^m)^b$, we can thus construct a suitable hash function, allowing a compression from b elements to one, by plugging it into the following mode. This mode is presented in Figure 3.2.


x
y
P
u
v
$\texttt{Jive}_2(x, y)$
x_0 x_1 $\cdots$ x_{b-1}
P
$\texttt{Jive}_b(x_0, ..., x_{b-1})$

(a) *Jive$_2$, which maps $(\mathbb{F}_q^m)^2$ to $\mathbb{F}_q^m$.*

(b) *Jive$_b$, which maps $(\mathbb{F}_q^m)^b$ to $\mathbb{F}_q^m$.*

Figure 3.2: The Jive mode turning a permutation into a compression function.

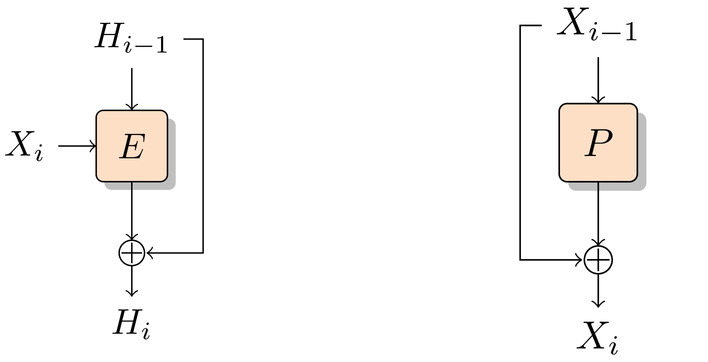
Definition 3.1 (Jive). Consider a permutation P defined as follows:

$$P : \begin{cases} (\mathbb{F}_q^m)^b & \rightarrow (\mathbb{F}_q^m)^b \\ (x_0, ..., x_{b-1}) & \mapsto (P_0(x_0, ..., x_{b-1}), ..., P_{b-1}(x_0, ..., x_{b-1})) \ , \end{cases}$$

so that it operates on bm elements of $\mathbb{F}_q$, where for all $0 \leqslant i < b$, $P_i(x_0, \ldots, x_{b-1})$ refers to the i-th element in $\mathbb{F}_q^m$ of the output $P(x_0, \ldots, x_{b-1})$. The `Jive` mode is built from P by defining the following one-way function $\texttt{Jive}_b(P)$:

$$\texttt{Jive}_b(P) : \begin{cases} (\mathbb{F}_q^m)^b & \rightarrow \mathbb{F}_q^m \\ (x_0, ..., x_{b-1}) & \mapsto \sum_{i=0}^{b-1} (x_i + P_i(x_0, ..., x_{b-1})) \ . \end{cases}$$

This approach can be seen as a permutation-based variant of the Davies-Meyer mode [Pre11] which, like the latter, crucially relies on a feedforward to ensure one-wayness. The Davies-Meyer compression function relies on a block cipher. The output of the previous compression H_{i-1} is encrypted with the current message block X_i. A xor is then applied to the output of the compression function, as shown in Figure 3.3a, so that $H_i = E_{X_i}(H_{i-1}) \oplus H_{i-1}$.



(a) The Davies-Meyer mode.

(b) The ChaCha mode.

Figure 3.3: *Variants that have inspired `Jive`.*

In fact, we named it `Jive` after another fast Latin dance. Indeed, this mode can, alternatively, be interpreted as a truncated instance of the mode used in the "Latin dance" ciphers Salsa [Ber08b], and its variant ChaCha [Ber08a], which is also based on a public permutation combined with a feedforward, as shown in Figure 3.3b.

If the `Jive` mode is used inside a Merkle tree, some computations can be saved. For example, in the case of a 2-to-1 compression function, a sponge would use a permutation operating on $(\mathbb{F}_q^m)^3$ in order to leave one vector of $\mathbb{F}_q^m$ free for the capacity. Using $\texttt{Jive}_2$ instead, we only need a permutation of $(\mathbb{F}_q^m)^2$. The trade-off of course is that, unlike a sponge-based approach, the relevance of `Jive` is restricted to some specific cases.

Following the terminology of [Dam90], a compression function must be secure against collisions. Then, since the output of `Jive` is an element of $\mathbb{F}_q$, we can state that a compression function using `Jive` mode provides $\lfloor \log_2 q \rfloor / 2$ bits of security.

3.2 Description of Anemoi

3.2.1 On the name "Anemoi"

First of all, let us tell the story behind the name Anemoi. In Greek mythology, Anemoi is a family of Gods of winds. Each was assigned a cardinal direction from which their respective winds blew, and each was associated with different seasons and weather conditions: *Borea* is the God of North wind, symbolizing the cold breath of winter, *Zephyrus* is the God of West Wind, representing the light breezes of spring, *Notus* is the God of South Wind, symbolizing summer, and *Eurus* is the God of East Wind, representing the storms of autumn. Therefore, this family of Gods has loose connection to butterflies which fly in the air. Let us recall that butterflies are what inspired the design of the Flystel, which is, as we will see in this section, the main component of Anemoi. Moreover, the four wind directions also symbolize the spread geographical location of the Anemoi team. The team is indeed composed of 7 members with a total of 8 affiliations and 5 countries: Pierre Briaud and myself from Sorbonne Université and Inria Paris (France), Pyrros Chaidos from National & Kapodistrian University of Athens (Greece), Léo Perrin from Inria Paris (France), Robin Salen from Toposware Inc. in Boston (United States), Vesselin Velichkov from University of Edinburgh (Scotland) and Clearmatics in London (England) and Danny Willems from Nomadic Labs in Paris and LIX (France).

In this section, we present new primitives, and the way to deterministically construct all of their variants. At their core are the Anemoi permutations, that operate on $\mathbb{F}_q^{2\ell}$ for any field size q that is either a prime number or a power of two, and for positive integer ℓ. The round function of these permutations is presented in Section 3.2.2. Aiming at having design consistency, using similar principles regardless of the parameters, there is a unique round function for all values of ℓ, and for all values of q,

In order to build the primitives themselves, we need also to consider the security level required as it will influence the number of rounds of the permutation (note that the security level will also influence the size of the internal state). The procedures to follow to define higher-level algorithms are described in Section 3.2.3, from which we suggest some specific instances.

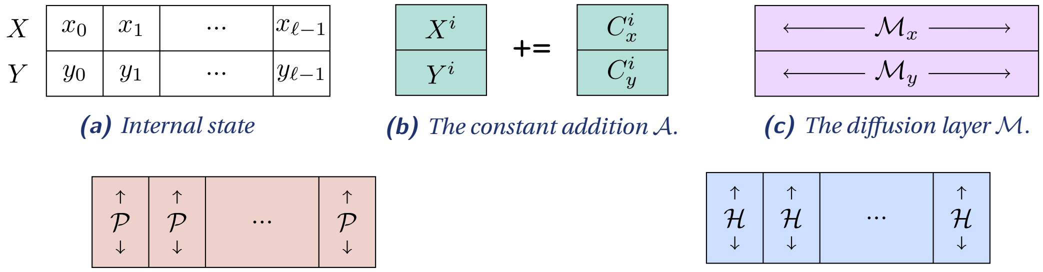
3.2.2 The SPN construction

Our design is a conservative one: it uses a very classical Substitution-Permutation Network structure. Aiming at giving consistent notation throughout this manuscript, those proposed in this chapter are not necessarily following our original paper [Bou+23]. In particular, while the exponent of the power function defining the permutation E in the Flystel is α in the paper, we will use d in what follows for consistency with other chapters.

A round function is a permutation of $\mathbb{F}_q^{2\ell}$, where $\ell > 0$ is an integer, and where q is either a prime number or a power of 2. The field order must have a bitlength of at least 10 bits. The aim of this restriction is to ensure that e.g. MDS matrices can be found as those might not exist for small field sizes.

In order to define it, we organize its state into a rectangle of elements of $\mathbb{F}_q$ of dimension $2 \times \ell$. The elements in the first row are denoted $(x_0, ..., x_{\ell-1})$, and those in the second row are $(y_0, ..., y_{\ell-1})$ (see Figure 3.4a). We refer to vectors of $\mathbb{F}_q^\ell$ using the same upper-case letters, e.g. $(x_0, ..., x_{\ell-1})$ is denoted X, and $(y_0, ..., y_{\ell-1})$ is denoted Y. Subscripts correspond to indices within a vector of $\mathbb{F}_q^\ell$, and superscripts to round indices, so X^i and Y^i are the top and bottom part respectively of the state at the start of round i. We let g be a specific generator of the multiplicative subgroup of the field $\mathbb{F}_q$. If q is prime, then g is the smallest such generator using the usual integer ordering. Otherwise, we have that $\mathbb{F}_q = \mathbb{F}_{2^n} = \mathbb{F}_2[x]/p(x)$, where p is an irreducible polynomial of degree n, in which case we let g be one of its roots.

The function applied at round r is denoted R_r. It has the structure of a classical Substitution-Permutation Network, whose components are described below: first the constant addition, then the linear layer, and finally the S-box layer. The overall action of each of these operations on the state is summarized in Figure 3.4.



(a) *Internal state*

(b) *The constant addition $\mathcal{A}$.*

(c) *The diffusion layer $\mathcal{M}$.*

(d) *The PHT $\mathcal{P}$.*

(e) *The S-box layer $\mathcal{S}$.*

Figure 3.4: *The internal state of* `Anemoi` *and its basic operations.*

A complete round is represented in Figure 3.5.

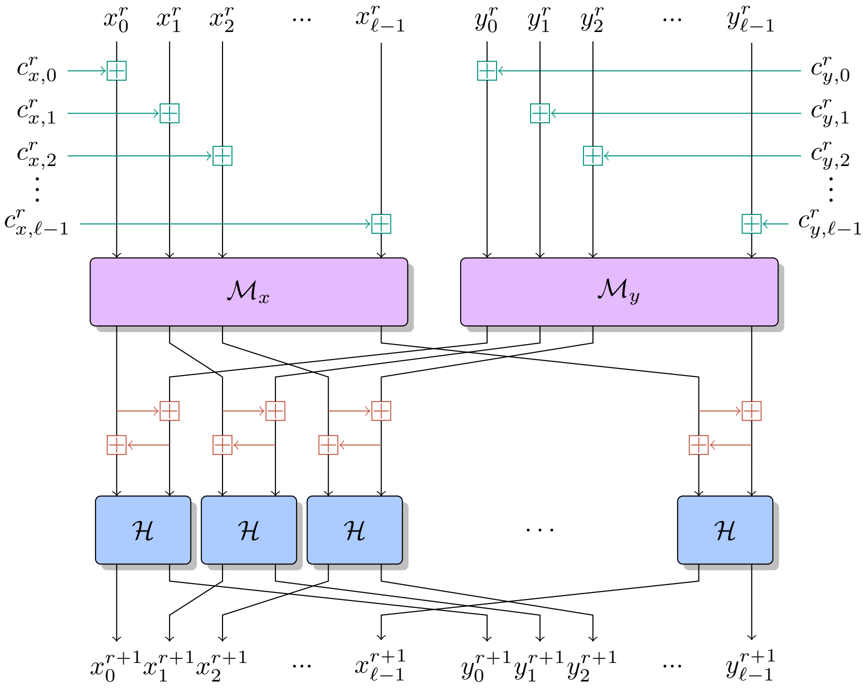


Figure 3.5: R_r*, the r-th round of* `Anemoi`*, applied on the state $(X, Y) \in \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell$.*

Constant Additions $\mathcal{A}$

When specifying round constants we aimed at limiting the reliance on randomness. Indeed, while dense round constants need to be generated to ensure resilience against algebraic attacks, we want to limit our reliance on pseudo-randomly generated components in order to ease both implementation and cryptanalysis.

We let $x_j \leftarrow x_j + c^i_{x,j}$ and $y_j \leftarrow y_j + c^i_{y,j}$, where $c^i_{x,j} \in \mathbb{F}_q$ and $c^i_{y,j} \in \mathbb{F}_q$ are round constants[1] depending on both the position (index j) and the round (index i). The aim is to increase the complexity of the algebraic expression of multiple rounds of the primitive and to prevent the appearance of patterns that an attacker could leverage in their attack. Then they are derived using the digits of π using the following procedure. We let

$$\begin{aligned}&(\pi_0, \pi_1) = \\ &(1415926535897932384626433832795028841971693993751058209749445923078164062862089986280348253421170679, \\ &8214808651328230664709384460955058223172535940812848111745028410270193852110555964462294895493038196)\end{aligned}$$

be the first and second blocks of 100 digits of π. We derive the round constants $c^i_{x,j}$ and $c^i_{y,j}$ by applying a function inspired by the open Flystel with the same parameters as in the round function on the pair (π_0^i, π_1^j), where superscripts are exponents, so that

$$\begin{cases} c^i_{x,j} & = g(\pi_0^i)^2 + \left(\pi_0^i + \pi_1^j\right)^d \\ c^i_{y,j} & = g(\pi_1^j)^2 + \left(\pi_0^i + \pi_1^j\right)^d + g^{-1} \,, \end{cases}$$

where the computations are done in $\mathbb{F}_q$. When $q = 2^n$, π_0 and π_1 are cast to field elements using the usual mapping sending $\sum_{k=0}^{n-1} x_i 2^i$ to $\sum_{k=0}^{n-1} x_i g^i$, where $(x_0, ..., x_{n-1})$ is the binary representation of x modulo 2^n.

Diffusion Layer $\mathcal{M}$

If $\ell > 1$, then the diffusion layer $\mathcal{M}$ operates on X and Y separately, so that

$$\mathcal{M}(X, Y) = \left(\mathcal{M}_x(X), \mathcal{M}_y(Y)\right) \,,$$

as summarized in Figure 3.4c. The linear permutations $\mathcal{M}_x$ and $\mathcal{M}_y$ are closely related, but differ in order to break the column structure imposed by the non-linear layer. More precisely, we impose that $\mathcal{M}_x$ is a matrix of size $\ell \times \ell$ of $\mathbb{F}_q$ with maximum diffusion, i.e. such that its branch number is equal to $\ell + 1$. Let us recall that the (differential) branch number of a linear permutation L is the minimum over $x \neq 0$ of $\mathrm{wt}(x) + \mathrm{wt}\left(L(x)\right)$, where $\mathrm{wt}(x)$ denotes the Hamming weight of x [Dae95].

We then construct $\mathcal{M}_y$ as follows:

$$\mathcal{M}_y = \mathcal{M}_x \circ \rho \quad \text{such that } \rho(x_0, ..., x_{\ell-1}) = (x_1, ..., x_{\ell-1}, x_0) \,,$$

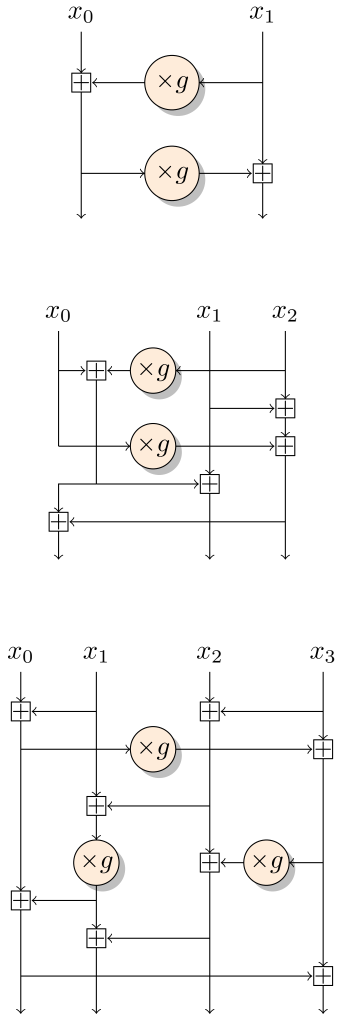
meaning that ρ is a simple word permutation.

The specifics of the linear permutation $\mathcal{M}_x$ then depend on the value of ℓ. Furthermore, in order for our permutation to best satisfy different proof systems, we use different techniques to construct $\mathcal{M}_x$. At a high level, there are two different situations.

[1] Note that to avoid confusion with the exponents of the permutation $x \mapsto x^d$ used in the Flystel we use different notations from our original paper [Bou+23].

First, if ℓ is small, then the field size is expected to be large in order for the permutation to operate on a state large enough to offer security against generic attacks. Such requirements imply that this case is expected to happen when using pairing-based proof systems like Groth16 or standard $\mathcal{P}$lon$\mathcal{K}$ which require large scalar fields for security.

In the $\mathcal{P}$lon$\mathcal{K}$ case, additions have a non-negligible cost during verification. As a consequence, when ℓ is at most equal to 4, we use linear layers requiring a number of additions as small as possible. To this end, we adapt results from [DL18] where Duval and Leurent present generic matrix constructions with a minimal number of additions. In practice, when $\ell \in \{2, 3, 4\}$, we use the matrix $\mathcal{M}_x^\ell$ given in Figure 3.6, with their corresponding diagrams. If $\ell = 1$, then there is a unique column in the internal state, so $\mathcal{M}_x^1$ is the identity. As [DL18] provides several matrices for each number of inputs, we based our matrices on their candidates that have the lowest number of additions, and the least symmetries.



$$\mathcal{M}_x^2 = \begin{pmatrix} 1 & g \\ g & g^2+1 \end{pmatrix}$$

(a) When $\ell = 2$.

$$\mathcal{M}_x^3 = \begin{pmatrix} g+1 & 1 & g+1 \\ 1 & 1 & g \\ g & 1 & 1 \end{pmatrix}$$

(b) When $\ell = 3$.

$$\mathcal{M}_x^4 = \begin{pmatrix} 1 & g^2 & g^2 & 1+g \\ 1+g & g+g^2 & g^2 & 1+2g \\ g & 1+g & 1 & g \\ g & 1+2g & 1+g & 1+g \end{pmatrix}$$

(c) When $\ell = 4$.

Figure 3.6: *Diagram representations of $\mathcal{M}_x$ for $\ell \in \{2, 3, 4\}$.*

We also give their efficient implementation in Algorithm 3.1.

Algorithm 3.1 Linear layers of Anemoi.

```
# Linear layer when l = 2
def M_2(X, g):
    X[0] += g * X[1]
    X[1] += g * X[0]

    return X

# Linear layer when l = 3
def M_3(X, g):
    t = X[0] + g * X[2]
    X[2] += x_1
    X[2] += g * X[0]
    X[0] = t + X[2]
    X[1] += t

    return X

# Linear layer when l = 4
def M_4(X, g):
    X[0] += X[1]
    X[2] += X[3]
    X[3] += g * X[0]
    X[1] = g * (X[1] + X[2])
    X[0] += X[1]
    X[2] += g * X[3]
    X[1] += X[2]
    X[3] += X[0]

    return X
```

Second, if ℓ is large, then the situation is the opposite, meaning that we would expect the field size to be smaller and thus to correspond, for example, to fields used in FRI-based proving systems.

In the AIR case, for instance, linear operations are essentially free. Thus, the dominating constraint on a linear layer is its native implementation cost, i.e. the time it takes for a C or Rust program to evaluate $\mathcal{M}_x(X)$. To minimize this cost, we need to minimize the value of the coefficients appearing in the matrix. To this end, we use the circulant matrix where the first row is the smallest in the lexicographic order, and such that the overall matrix is MDS.

Pseudo-Hadamard transform $\mathcal{P}$

To destroy some undesirable involutive patterns at the S-box level, we use a linear layer, namely the Pseudo-Hadamard transform (PHT), to have diffusion on the rows. In particular, this means that we still have a linear layer when $\ell = 1$. The PHT has good properties since it can be easily implemented with: $Y \leftarrow Y + X$ and $X \leftarrow X + Y$ and is also relevant against algebraic attacks (see Chapter 4).

S-box Layer $\mathcal{S}$

Let $\mathcal{H}$ be an open `Flystel`, as introduced in Chapter 2, operating over $\mathbb{F}_q^2$. Let us recall that $\mathcal{H}$ is defined as follows

$$\mathcal{H}(x, y) = \left(x - Q_\gamma(y) + Q_\delta(y - E^{-1}(x - Q_\gamma(y))), y - E^{-1}(x - Q_\gamma(y))\right) ,$$

where in $\mathbb{F}_{2^n}$ we have

$$Q_\gamma(x) = \gamma + \beta x^3, \quad E(x) = x^3 \quad \text{and} \quad Q_\delta(x) = \delta + \beta x^3 ,$$

while in $\mathbb{F}_p$ we have

$$Q_\gamma(x) = \gamma + \beta x^2, \quad E(x) = x^d \quad \text{and} \quad Q_\delta(x) = \delta + \beta x^2 .$$

Then we let

$$\mathcal{S}(X, Y) = \left(\mathcal{H}(x_0, y_0), ..., \mathcal{H}(x_{\ell-1}, y_{\ell-1})\right) ,$$

as summarized in Figure 3.4e. A `Flystel` instance is defined by 4 parameters, regardless of whether it is a $\texttt{Flystel}_\texttt{p}$ or $\texttt{Flystel}_2$: the exponent d, the multiplier β, and the two added constants γ and δ. First, as mentioned in Section 2.3.2.1, we let $\beta = g$. Indeed, setting $\beta = 1$ would imply that the space $\{(x^2, x), x \in \mathbb{F}_q\}$ is invariant, which we deem too simple. As a consequence g is the most natural non-trivial constant. Furthermore, in order to break the symmetry of the `Flystel`, we impose that $\gamma \neq \delta$. We thus let $\gamma = 0$ and $\delta = g^{-1}$ as this value is both different from 1 and g while retaining a simple definition.

All that remains is to choose the exponent d. If $q = 2^n$, then we let $d = 3$ since we have to use a Gold exponent (i.e. an exponent of the form $2^j + 1$), and 3 always works since n is odd. Otherwise, when q is prime, the process is a bit more involved as a higher value allows using fewer rounds to thwart Gröbner-basis-based attacks, but is also more expensive. Users should use the value of d that yields the most efficient algorithm according to their metrics, while keeping $x \mapsto x^d$ a permutation. In practice, zero-knowledge proof systems will favor permutations with the smallest exponent.

We describe the round function with pseudo-code in Algorithm 3.2.

3.2.3 Higher-Level Algorithms

3.2.3.1 The permutation: `Anemoi`.

The `Anemoi` permutation iterates n_r rounds of the round function described in the previous section and depicted in Figure 3.5. In addition, we use a last call to the linear layer $\mathcal{M}$. In symmetric cryptography, we usually *remove* outer linear layers, e.g. in the AES. That is because they don't contribute to the cryptographic strength of a block cipher (e.g. can be removed “for free” by an adversary). In the case of a sponge construction however, the adversary only controls a part of the state, namely the outer part (the rate). Thus, starting and finishing with a diffusion layer ensures that this control is spread across the full state in a way which is not aligned with the non-linear layer. Note that a similar goal could be achieved using *indirect injection*, as done in Esch [Bei+20], a family of hash function of the SPARKLE suite.

It follows that the `Anemoi` permutation corresponds to the following function:

$$\texttt{Anemoi}_{q,d,\ell} = (\mathcal{P} \circ \mathcal{M}) \circ \mathsf{R}_{n_r-1} \circ ... \circ \mathsf{R}_0 .$$

Algorithm 3.2 Round function of `Anemoi`.

```
# Constant addition A
for i in range(l):
    X[i] = X[i] + Cx[r][i]
    Y[i] = Y[i] + Cy[r][i]

# Linear layer M
X = Mx (X)
Y = Mx (p(Y))

# PHT P
Y = Y + X
X = X + Y

# S-box layer H
for i in range(l):
    X[i]  = X[i] - g * Q(Y[i]) - g**(-1)
    Y[i]  = Y[i] - X[i]**(1/d)
    X[i]  = X[i] + g * Q(Y[i])

return (X, Y)
```

The number of rounds n_r is derived from our security analysis in Chapter 4. More precisely, we focus on algebraic attacks since it appears to be the bottleneck. Indeed, we only need to activate few S-boxes to prevent statistical attacks. In prime characteristic we have an upper bound that is $(d-1)/p^2$ for the probability of a differential transition for one S-box, and that is conjectured to be $\log p/p$ for a linear transition. In the case where $q = 2^n$, similar arguments hold: the best differential probability is $4/2^{2n}$, and the best linear probability is around 2^{-n}. More details will be given in Section 4.3.2.

Let s be the required security level, and (q, ℓ, d) be the parameters imposed by the use case. As we believe that a construction with more branches gives more freedom to the attacker, we choose a security margin that increases with the size of the internal state, but setting a maximum of 5 additional rounds. In Section 4.3.2, we will study two models for algebraic attacks. We fix the number of rounds by considering the first model, which is easier to study, and add a security margin of 2 rounds to take into account the second model. Whilst it is not clear whether the second model actually outperforms the first one, its complexity is more difficult to estimate and we opt to increase the security margin as a conservative measure. Then the number of rounds n_r is the smallest value satisfying the following conditions:

$$n_r \geqslant \max \left\{ 8\,,\ \underbrace{\min(5, 1+\ell)}_{\text{security margin}} + \underbrace{2 + \min\left\{ r \in \mathbb{N} \;\middle|\; \mathcal{C}_{\mathrm{ALG}(r)} \geqslant 2^s \right\}}_{\text{to prevent algebraic attacks, see Section 4.3.2}} \right\}\,, \tag{3.1}$$

where the cost of algebraic attacks $\mathcal{C}_{\mathrm{ALG}(r)}$ is defined as follows:

$$\mathcal{C}_{\mathrm{ALG}(r)} = \begin{cases} \dbinom{4\ell r + \kappa_d}{2\ell r}^2 & \text{when } q = p \\ \ell r \cdot 9^{2\ell r} & \text{when } q = 2^n, \end{cases}$$

where κ_d is a constant depending on d. We have for example: $\kappa_3 = 1, \kappa_5 = 2, \kappa_7 = 4$ and $\kappa_{11} = 9$. Then, in Table 3.1, we derived the number of rounds needed for various values of ℓ and d, for fields of even and odd characteristics, both for a security level of 128 bits and of 256 bits. Note that the values of the digest size h and of the state size $2\ell n = 2\ell \log_2(q)$ must be consistent with the desired security level.

ℓ	1	2	3	4	6	8
$d = 3$	21	14	12	12	10	10
$d = 5$	21	14	12	12	10	10
$d = 7$	20	13	12	11	10	9
$d = 11$	19	13	11	11	10	9

(a) *When $q = p$ and $s = 128$.*

ℓ	1	2	3	4	6	8
$d = 3$	37	22	17	16	13	12
$d = 5$	37	22	17	16	13	12
$d = 7$	36	21	17	15	13	11
$d = 11$	35	21	17	15	13	11

(b) *When $q = p$ and $s = 256$.*

ℓ	1	2	3	4	6	8
n_r	24	15	13	12	11	10

(c) *When $q = 2^n$ and $s = 128$.*

ℓ	1	2	3	4	6	8
n_r	44	25	20	17	14	12

(d) *When $q = 2^n$ and $s = 256$.*

Table 3.1: *Number of Rounds of `Anemoi`.*

3.2.3.2 Specific instances

Let us present some examples of functions in the `Anemoi` family that are defined over different fields, aiming at different APIs (both `AnemoiSponge` and `AnemoiJive`), and a security level of 127 bits. We focus on the scalar fields $\mathbb{F}_q$ used by the elliptic curves BLS12-381 and BN-254. In the case of BLS12-381 curve, we have $(\lceil \log_2(q) \rceil, d, g) = (255, 5, 7)$, while in the case of BN-254 curve, $(\lceil \log_2(q) \rceil, d, g) = (254, 5, 2)$.

The compression function: `AnemoiJive`

We can construct a compression function mapping b-to-1 vectors of $\mathbb{F}_q^t$ elements, using `Jive`$_b$ and an `Anemoi` instance operating on bt elements of $\mathbb{F}_q$. The only constraint is that bt must be even.

`AnemoiJive`-BLS12-381 and `AnemoiJive`-BN-254 are Merkle Compression functions mapping two elements of $\mathbb{F}_q$ to a unique one. In order to reach a security level of 127 bits, $\ell = 1$ is sufficient in both cases. The underlying permutations of the compression functions then use the following components.

- **Round Constants.** These are generated as described in Section 3.2.2.
- **Linear layer.** As $\ell = 1$, we use the Pseudo-Hadamard transform, which is given by:

$$\mathcal{P} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

- **S-box.** $\mathcal{H}$ uses the parameters g and d corresponding to the elliptic curve.

- **Number of Rounds.** Using Equation (3.1), we obtain that 21 rounds are needed for a security level of 127 bits.

Round r is then defined as $\mathsf{R}_r : (x, y) \mapsto \mathcal{H} \circ \mathcal{P} \circ \mathcal{M}(x + c_r, y + d_r)$, and we define the compression functions as follows. Let (x, y) be the input, and P be the `Anemoi` instance defined by

$$\mathsf{P} := \mathcal{P} \circ \mathcal{M} \circ \mathsf{R}_{20} \circ \ldots \circ \mathsf{R}_0 \ .$$

Then $\texttt{AnemoiJive}(x, y)$ is evaluated as follows:

1. let $(u, v) \leftarrow P(x, y)$,
2. return $x + y + u + v$.

The hash function: `AnemoiSponge`

`AnemoiSponge` is a “regular” hash function, in the sense that it should be able to process messages of arbitrary length. We therefore rely on the sponge construction detailed in Section 3.1.1, where r words are used as the rate, c are used as the capacity, and where the permutation is the `Anemoi` instance operating on $\mathbb{F}_q^{r+c}$. Note that the inner workings of `Anemoi` imply that $r + c$ must be even.

`AnemoiSponge`-BLS12-381 and `AnemoiSponge`-BN-254 are hash functions mapping a sequence $\{x_i\}_{0 \leqslant i < t}$ of elements of $\mathbb{F}_q$ to an element of $\mathbb{F}_q$, where t is a positive integer. It is constructed using a sponge which relies on `Anemoi` as the permutation. We aim to provide about 127 bits of security, meaning that a capacity of 1 word of $\mathbb{F}_q$ is enough in both cases. We then pick an identical rate, so that $r = c = 1$, and thus $\ell = 1$. The permutations used are then the same as for `AnemoiJive`-BLS12-381 and `AnemoiJive`-BN-254.

Security Claims

All the `Anemoi` permutations generated as defined above can be used safely to construct cryptographic primitives with the given security level. In particular, we make a “hermetic sponge” claim[2] about all the hash functions `AnemoiSponge` generated as above, so that `AnemoiSponge`-BLS12-381 and `AnemoiSponge`-BN-254 provide 127 bits of security against all known attacks.

The best way to find collisions in `AnemoiJive`-BLS12-381 (respectively `AnemoiJive`-BN-254) is to rely on a generic collision search. Since the output is an element of $\mathbb{F}_q$ with $\log_2(q) \geqslant 254$, this is expected to require about 2^{127} function calls on average. Thus, we claim that all the `AnemoiJive` functions are secure b-to-1 compression functions (provided of course that the state size is chosen correctly).

3.2.4 Implementation Aspects

For direct computation, or witness calculation, we can simply implement the open `Flystel`. However, for the verification, we also have the option to use the closed `Flystel` structure, since there is no requirement for the various verification steps to be performed in a particular order as long as consistency is enforced. In this case, the cost is of one multiplication for Q_γ and Q_δ, and as many as are needed to compute $x \mapsto x^d$. This computation can be implemented using a technique that is slightly more subtle than the basic fast exponentiation algorithm, and instead

[2] Our claim is in the sense of `https://keccak.team/sponge_duplex.html` meaning that there is no structural distinguisher on the `Anemoi` permutations with complexity below $2^{c/2}$.

relies on addition chains as discussed for example in [BC90]. We used `addChain` [McL21] to find the best such chains for small values of d. An *addition chain* for an integer n is a sequence of integers from 1 to n such that every term is a sum of two integers appearing earlier in the sequence. Addition chains appear in the optimization of exponentiation algorithms with fixed exponents. For instance, an addition chain for 5 is $1, 2, 4, 5$ and corresponds to the following sequence of multiplications to compute x^5:

$$\begin{aligned} x^2 &= x \cdot x \\ x^4 &= x^2 \cdot x^2 \\ x^5 &= x \cdot x^4 \,, \end{aligned}$$

implying that 3 multiplications are required to perform the exponentiation. It is worth mentioning that an addition chain is not unique. For example $1, 2, 3, 4, 8, 11$ and $1, 2, 4, 5, 10, 11$ are two additions chains for 11. Both of them lead to a cost of 5 multiplications to perform the exponentiation x^{11}.

$$\begin{array}{llll} x^2 &= x \cdot x & \qquad x^2 &= x \cdot x \\ x^3 &= x \cdot x^2 & \qquad x^4 &= x^2 \cdot x^2 \\ x^4 &= x^2 \cdot x^2 & \qquad x^5 &= x \cdot x^4 \\ x^8 &= x^4 \cdot x^4 & \qquad x^{10} &= x^5 \cdot x^5 \\ x^{11} &= x^3 \cdot x^8 & \qquad x^{11} &= x \cdot x^{10} \,. \end{array}$$

We list the corresponding results in Table 3.2, and denote $\mathcal{C}_d$ the cost of such an exponentiation.

# multiplications	d
2	$\{3\}$
3	$\{5\}$
4	$\{7, 9\}$
5	$\{11, 13, 15, 17\}$
6	$\{19, 21, 23, 25, 27, 33\}$
7	$\{29, 31, 35, 37, 39, 41, 43, 45, 49, 51, 65\}$
8	$\{47, 53, 55, 57, 59, 61, 63, 67, 69, 73, 75, 77, 81, 83, 85, 97, 99\}$
9	$\{71, 79, 87, 89, 91, 93, 95, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125\}$
10	$\{127\}$

Table 3.2: *The values* d *for which computing $x \mapsto x^d$ requires a given number of multiplications.*

We remark that the cost of the exponentiation increases slowly, and that for example $d = 17$ is less than twice as expensive as $d = 5$. As a consequence we also consider $d = 17$ as a good exponent for the permutation $E : x \mapsto x^d$ in the `Flystel`. However, we did not choose it since algebraic attacks were becoming too costly to carry out experiments, even on smaller instances. Furthermore, we will see in Chapter 5 that the higher the exponent of a gold function, the more uncertain its security appears to be, because of the sparse univariate representation when iterating it. Although the study carried out in Chapter 5 does not apply directly, it does imply that using such functions seems less secure.

3.3 Cryptanalysis of Anemoi

3.3.1 Statistical attacks on Anemoi

In this part, we argue that differential and linear attacks can be prevented by the Flystel construction, thanks to the differential and linear properties of the scheme as presented in Section 2.3.3.

3.3.1.1 Differential cryptanalysis

As introduced in Chapter 1, differential attacks exploit the probability of a given non-zero input difference leading to a given output difference after a certain number of rounds. As established in Proposition 2.8 for the $\texttt{Flystel}_2$ and in Corollary 2.3 for the $\texttt{Flystel}_\texttt{p}$, the differential uniformity of a Flystel is low (namely at most 4 in the former case and $(d-1)$ in the latter). As a consequence, the probability of a differential transition is small. More precisely, this probability is upper bounded by:

$$\mathbb{P}(\mathcal{H}(x+a_1, y+a_2) - \mathcal{H}(x,y) = (b_1,b_2)) \leqslant \begin{cases} \dfrac{4}{2^{2n}} & \text{if } q = 2^n\,, \\ \dfrac{d-1}{p^2} & \text{if } q = p\,. \end{cases}$$

Given that q is typically bigger than 2^{63}, we only need to activate 3 S-boxes to obtain more than 128 bits of security, and 5 for 256 bits.

The activation of many S-boxes is further helped by our use of MDS diffusion matrices when $\ell \geqslant 2$. The structure of $\mathcal{M}$, based on two parallel MDS matrices $\mathcal{M}_x$ and $\mathcal{M}_y$, ensures that at least $\ell+1$ S-boxes are active in every pair of consecutive rounds.

3.3.1.2 Linear cryptanalysis

A similar argument holds for linear attacks. As for the differential uniformity, the correlation increases slowly with q according to Conjecture 2.1. More precisely, the best probability is conjectured to be $\log(p)/p$ for a linear transition in prime fields, while it is around 2^{-n} for a linear transition in binary fields.

Therefore, it is again sufficient to activate a few S-boxes to prevent the existence of high-correlation linear trails. Indeed, as established in [BSV07], a linear attack against F becomes possible when the squared modulus of $\mathcal{W}_{\langle b,F \rangle}(a)$ for some $a, b \in \mathbb{F}_q^m$ is high enough. Roughly speaking, the data complexity of a linear attack is around $1/|\mathcal{W}_{\langle b,F \rangle}(a)|^2$, so activating a few S-boxes will be sufficient for this squared modulus to drop below 2^{-s}, where s is the intended security level.

The activation of many S-boxes is further helped by our use of MDS diffusion matrices. Again, the structure $\mathcal{M}$, based on two parallel MDS matrices $\mathcal{M}_x$ and $\mathcal{M}_y$, ensures that at least $\ell+1$ S-boxes are active in every pair of consecutive rounds.

3.3.2 Higher-order differential attacks

In binary fields, primitives with low algebraic degree are potentially vulnerable to higher-order differential cryptanalysis [Knu95]. The open $\texttt{Flystel}_2$ is an efficient counter-measure against such attacks since open butterflies operating on $(\mathbb{F}_{2^n})^2$ are known to have an algebraic degree equal to n (see Proposition 2.8). As shown in [Bey+20a], a low degree can also be leveraged in the case where q is prime. Still, a similar argument will hold: the degree of $x \mapsto x^{1/d}$ is too high to allow any meaningful pattern to emerge.

3.3.3 Invariant Subspaces

Remember that, regardless of the characteristic, it always holds that $\mathcal{H}\left(Q_\gamma(y), y\right) = \left(Q_\delta(y), y\right)$. For each `Flystel` instance in the round function (i.e., for each column in the state), the probability that an input is in this set is equal to $1/q$. As this pattern is non-linear, we deem it unlikely that it is preserved by the combination of the constant addition and the linear layer with a probability higher than chance, meaning that this pattern will be activated in inner rounds with a negligible probability.

This pattern can be used to simplify the equations modeling a call to `Anemoi` during an algebraic attack: if an attacker has some degrees of freedom, then forcing the emergence of such a pattern within some `Flystel` instances is the best strategy to simplify these equations.

3.4 Some benchmarks

In this section, we compare various instances of *Rescue–Prime*, Poseidon, Griffin and `Anemoi` with respect to SNARK metrics: R1CS (Section 3.4.1.1) and $\mathcal{P}$lon$\mathcal{K}$ (Section 3.4.1.2), and STARK: AIR (Section 3.4.1.3). For $\mathcal{P}$lon$\mathcal{K}$ performance, we will also conduct a comparison with `Reinforced Concrete`.

Due to the increasing number of applications revolving around zk-STARKs, which do not require an algebraic group as large as scalar fields of elliptic curves, we also illustrate native performance comparison of 2-to-1 compression functions based on *Rescue–Prime*, Poseidon, Griffin and `Anemoi` on a 64-bit field used in various applications ([Mid22], [Zer22]).

3.4.1 Number of constraints

Let us set the parameters. We let $\mathbb{F}_q$ be a prime field where $q = p$, and m be the number of field elements we operate on so that $m = 2\ell$ for `Anemoi`. Besides, let s denote the security level in bits, n_r the number of rounds, and $\mathcal{C}_d$ the cost of an exponentiation $x \mapsto x^d$.

Let us recall that the verification for the `Flystel` is performed as follows:

$$\begin{cases} (y-v)^d + \beta y^2 + \gamma - x = 0 \\ (y-v)^d + \beta v^2 + \delta - u = 0\,. \end{cases} \tag{3.2}$$

In the following, we use the n_r values from Section 3.2.3 for `Anemoi` and we derive, in Table 3.3, those for *Rescue–Prime*, Poseidon and Griffin as defined in Chapter 1. Note that for Poseidon, which has $n_r = \mathsf{RF} + \mathsf{RP}$ rounds, while the bound is a complex expression in the original paper [Gra+21], in our setting and for the security margin recommended by the authors, it holds that $\mathsf{RF} = 8$, and that RP must be higher than (or equal to)

$$1.075 \cdot \left(\lceil \log_d(2) \cdot \min\{s, \log_2(p)\}\rceil + \lceil \log_a m \rceil - \mathsf{RF}\right)\,.$$

m	RP	Poseidon	Griffin	Anemoi
2	26	$(8+83)$	-	21
3	18	$(8+83)$	16	-
4	14	$(8+84)$	14	14
6	9	$(8+84)$	-	12
8	8	$(8+84)$	11	12

(a) *when* $d=3$.

m	RP	Poseidon	Griffin	Anemoi
2	20	$(8+56)$	-	21
3	14	$(8+56)$	12	-
4	11	$(8+56)$	11	14
6	8	$(8+57)$	-	12
8	8	$(8+57)$	9	12

(b) *when* $d=5$.

Table 3.3: *Number of rounds for each hash function considered.*

3.4.1.1 R1CS Systems

We first estimate the number of constraints for R1CS. As shown in Section 2.3.4.1, the R1CS cost for the *closed* `Flystel` of `Anemoi` is: $\mathcal{C}_d$ constraints to obtain $(y-v)^d$, and one constraint for each of the two quadratic function Q_γ and Q_δ.

For *Rescue–Prime* and Poseidon, each S-box costs $\mathcal{C}_d$ constraints, where for *Rescue–Prime* there are $2m$ S-boxes per round while for Poseidon there are m S-boxes per full round, and only 1 per partial round. For Griffin, each S-box costs $2 \cdot \mathcal{C}_d$ constraints for the first two words, and 1 constraint for each squaring of L and each word of the remaining state. As a consequence, when using *Rescue–Prime*, Poseidon, Griffin and `Anemoi` as hash functions, the number of constraints is respectively:

$$\begin{aligned}
\textit{Rescue–Prime}: &\quad \mathcal{C}_d \cdot 2m \cdot n_r \,, \\
\textsc{Poseidon}: &\quad \mathcal{C}_d \cdot (m\mathsf{RF} + \mathsf{RP}) \,, \\
\textsc{Griffin}: &\quad (\mathcal{C}_d + m - 2) \cdot 2n_r \,, \\
\texttt{Anemoi}: &\quad (\mathcal{C}_d + 2) \cdot \left(\frac{m}{2} \cdot n_r\right) \,.
\end{aligned}$$

We compare the number of constraints for those four schemes in Table 3.4. As we can see, the `Anemoi` permutations are consistently much more efficient than both Poseidon and *Rescue–Prime* by about a factor 2. `Anemoi` and Griffin are on par, and `Anemoi` takes the advantage for $d = 3$.

3.4.1.2 $\mathcal{P}$lon$\mathcal{K}$

For ease of exposition, we will consider rounds to be shifted so that constant additions and linear operations come after the S-box. First, let us investigate the cost in standard $\mathcal{P}$lon$\mathcal{K}$, that is with 3 wires and no custom gates.

As for R1CS, we again investigate System (3.2). For `Anemoi`, in Section 2.3.4.2, we have shown that evaluating an S-box costs 1 constraint to derive $w = y - v$ and $\mathcal{C}_d$ constraints to obtain w^d, 1 constraint for each of the two quadratics, and 1 for each of the addition of x and of u. The total cost for the S-box layer with 3 wires[3] is $(\mathcal{C}_d + 5)\frac{m}{2}$. The constant additions can be folded into the $n_r + 1$ linear layers and can thus be disregarded. For $m = 2$, the linear layer consists of the PHT, which requires 2 constraints. For $m > 2$, the linear layer itself consists of 2 separate matrix-vector multiplications, each producing $\frac{m}{2}$ sums of $\frac{m}{2}$ terms, requiring $m \cdot (\frac{m}{2} - 1)$ constraints, in

[3] The 3-wire setting corresponds to the classic $\mathcal{P}$lon$\mathcal{K}$, i.e. with 2 inputs and 1 output. The 4-wire setting is for an additional input or output.

	m	*Rescue-P*	Poseidon	Griffin	Anemoi
R1CS	2	208	198	-	**76**
	3	216	214	**96**	-
	4	224	232	112	**96**
	6	216	264	-	**120**
	8	256	296	176	**160**
$\mathcal{P}$lon$\mathcal{K}$	2	312	380	-	**191**
	3	432	594	**197**	-
	4	560	832	**260**	316
	6	756	1344	-	**460**
	8	1152	1920	**574**	648
AIR	2	156	300	-	**126**
	3	162	324	**144**	-
	4	**168**	348	**168**	**168**
	6	**162**	396	-	216
	8	**192**	456	264	288

(a) *when* $d = 3$.

	m	*Rescue-P*	Poseidon	Griffin	Anemoi
R1CS	2	240	216	-	**95**
	3	252	240	**96**	-
	4	264	264	**110**	120
	6	288	315	-	**150**
	8	384	363	**162**	200
$\mathcal{P}$lon$\mathcal{K}$	2	320	344	-	**212**
	3	420	512	**173**	-
	4	528	696	**222**	344
	6	768	1125	-	**496**
	8	1280	1609	**492**	696
AIR	2	**200**	360	-	210
	3	210	405	**180**	-
	4	**220**	440	**220**	280
	6	**240**	540	-	360
	8	**320**	640	360	480

(b) *when* $d = 5$.

Table 3.4: *Total R1CS, $\mathcal{P}$lon$\mathcal{K}$ and AIR cost for several hash functions ($s = 128$).*

addition to a cost of m constraints for the PHT. However, the number of constraints per matrix multiplication can be reduced by choosing MDS matrices lowering the number of additions. For the matrices given for $m = 6$ and $m = 8$ (i.e. for $\ell = 3$ and $\ell = 4$ respectively) in Section 3.2.2, we have respectively a cost of 10 and 16 per linear layer.

Poseidon uses simpler S-boxes, each costing $\mathcal{C}_d$ constraints. Full rounds use m S-boxes whereas partial ones use only one. Using the optimization described in the Supplementary Material of [Gra+21], the linear layer costs $m \cdot (m-1)$ constraints for the full rounds and $2m-2$ constraints for the partial rounds.

Rescue–Prime uses m standard and m inverted S-boxes, each costing $\mathcal{C}_d$. Each round also utilizes 2 independent linear layers each costing $m \cdot (m-1)$ constraints for every round.

For Griffin, the cost of the S-box is $2 \cdot \mathcal{C}_d + 3 + 4 \cdot (m-3)$. Regarding the linear layer, the matrix used for $m = 3$ can be computed in 5 constraints. For $m = 4$, the cost of one multiplication by the matrix they chose is 8. By observing intermediate variables from the S-box computation which can be reused in the linear layer computation, Griffin gives 260 constraints for $m = 4$ (resp. 574 for $m = 8$) when $d = 3$, and 222 constraints for $m = 4$ (resp. 492 for $m = 8$) when $d = 5$.

As a consequence, summarizing the number of $\mathcal{P}$lon$\mathcal{K}$ constraints using *Rescue–Prime*, Poseidon, Griffin and Anemoi as hash functions, we get respectively:

$$\begin{aligned}
\textit{Rescue–Prime}: &\quad \mathcal{C}_d \cdot 2m \cdot n_r + 2n_r \cdot m(m-1)\,, \\
\text{Poseidon}: &\quad \mathcal{C}_d \cdot (m\mathsf{RF} + \mathsf{RP}) + m(m-1) \cdot \mathsf{RF} + (2m-2) \cdot \mathsf{RP}\,, \\
\text{Griffin}: &\quad n_r \cdot (2 \cdot \mathcal{C}_d + 3 + 4 \cdot (m-3)) + (n_r + 1) \cdot \mathcal{C}_{\mathcal{L}}\,, \\
\texttt{Anemoi}: &\quad n_r \cdot (\mathcal{C}_d + 5) \cdot \frac{m}{2} + (n_r + 1) \cdot \mathcal{C}_{\mathcal{L}}\,,
\end{aligned}$$

where the cost of the linear layer $\mathcal{L}$ for Griffin is:

$$\mathcal{C}_{\mathcal{L}} = \begin{cases} 5 & \text{if } m = 3\,, \\ 8 & \text{if } m = 4\,, \\ 24 & \text{if } m = 8\,, \end{cases}$$

while for `Anemoi` we have:

$$\mathcal{C}_{\mathcal{L}} = \begin{cases} 2 & \text{if } m = 2\,, \\ 4+4 & \text{if } m = 4\,, \\ 6+10 & \text{if } m = 6\,, \\ 8+16 & \text{if } m = 8\,, \end{cases}$$

We then compare the number of constraints for these four schemes in Table 3.4. `Anemoi` is consistently ahead of *Rescue–Prime* and Poseidon with a significant margin, but for larger m, our performances are slightly worse than Griffin, since our strategy to compute the security margin is different: we try to take into account the greater freedom given by the larger number of branches, which impacts the number of rounds.

$\mathcal{P}$lon$\mathcal{K}$ Optimizations.

One of the more fruitful, but also challenging aspects of $\mathcal{P}$lon$\mathcal{K}$ is its ability to extend the expressive power of the constraints at a reasonable cost. In the analysis, the linear layer cost dominates that of the S-boxes. This is particularly impactful for Poseidon, as the efficiency benefit of its partial rounds is negated. The recent work of Ambrona *et al.* [Amb+22] presents a set of generic and tailored optimizations for $\mathcal{P}$lon$\mathcal{K}$ applicable to Poseidon. Two of the more powerful (but also costly) optimizations involve adding new wires in the constraint system and also including terms of higher degree. For example, it is possible to handle additions of many terms more efficiently by adding a fourth wire.

While an exhaustive comparison of optimization options is beyond the scope of this manuscript, we propose to discuss the efficiency of the different primitives while leaving all the details of the computations in our paper [Bou+23]. We will compare: Poseidon as optimized by Ambrona *et al.*, Griffin, `Reinforced Concrete` which was built with $\mathcal{P}$lon$\mathcal{K}$ optimizations in mind, and `Anemoi`. As Poseidon, Griffin and `Reinforced Concrete` are sponge-based we use $s = 128, d = 5$ and $m = 3$ to represent popular deployment choices, while we set $m = 2$ for `Anemoi`, using the `Jive`$_2$ mode. For a fair comparison we also extrapolate a `Jive`$_2$ version of Poseidon with the optimizations of [Amb+22], and `Reinforced Concrete`, while it is not possible for Griffin which is not defined for $m = 2$.

We summarize our findings in Table 3.5. We extrapolate the $m = 2$ costs for Poseidon and `Reinforced Concrete` by assuming a `Jive`$_2$ mode of operation is feasible at no additional overhead or increase in rounds. Against the next-best proposed system, Poseidon for $m = 3$ as optimized by [Amb+22] we achieve a 21% reduction when using 3 wires and 35% when using 4.We note that while the costs between Poseidon, `Anemoi` and Griffin are directly comparable as they use the same features, `Reinforced Concrete` leverages lookup tables [Gra+22a; GW20] instead. Since custom gates also imply some additional cost, we do note that by [Amb+22, Table 2], the additional overhead (compared to standard $\mathcal{P}$lon$\mathcal{K}$) for the custom gates we describe is between 10% and 40%.

We can go further in the optimization given above by extending $\mathcal{P}$lon$\mathcal{K}$ with a custom gate to compute the square of a wire, which adds a negligible overhead to the prover and the verifier time. This quadratic custom gate gives 56 as a total number of constraints for the 3-wire setting.

	m	Constraints
Poseidon	3	110
	2	88
Reinforced Concrete	3	378
	2	236
Griffin	3	125
AnemoiJive	2	**86**

(a) *With 3 wires.*

	m	Constraints
Poseidon	3	98
	2	82
Reinforced Concrete	3	267
	2	174
Griffin	3	111
AnemoiJive	2	**64**

(b) *With 4 wires.*

Table 3.5: *PlonK constraints with an additional custom gate to compute x^5.*

3.4.1.3 AIR

Finally, we also study the performance of Anemoi in the Algebraic Intermediate Representation (AIR) arithmetization used in STARKs [Ben+18]. Here, the relevant quantities are: the width of the computation state w, the number of computation steps T, and the maximum degree of the constraints $d_{\max}$. While there are several ways to estimate the cost of a specific AIR program given the above quantities, we will consider the total cost to be expressed as $w \cdot T \cdot d_{\max}$, following [Aly+20].

For *Rescue–Prime*, Griffin and Anemoi, the parameters are the same, the width of the computation corresponds to the size of the internal state, the number of computation steps is the number of rounds n_r and the maximum degree of the constraints is d. For Poseidon, the only difference is for the number of computation steps which is in that case $T = \mathsf{RF} + \lceil \mathsf{RP}/m \rceil$.

As a consequence, for *Rescue–Prime*, Poseidon, Griffin and Anemoi, the number of AIR constraints is respectively:

$$\begin{aligned} \textit{Rescue–Prime}, \textsc{Griffin}, \texttt{Anemoi}: &\quad m \cdot n_r \cdot d\,, \\ \textsc{Poseidon}: &\quad m \cdot \left(\mathsf{RF} + \left\lceil \frac{\mathsf{RP}}{m} \right\rceil\right) \cdot d\,. \end{aligned}$$

We then compare the total cost for these four schemes in Table 3.4. Anemoi and Griffin are quite similar, and close to *Rescue–Prime*.

3.4.2 Native performance

Outside of proving systems, Anemoi performances can challenge other algebraic hash functions, especially in Merkle trees thanks to its Jive mode. In particular in STARKs settings where we can use smaller cryptographic fields, Anemoi offers the best balance in terms of native evaluation and number of constraints. In Table 3.6, we illustrate the running time of a 2-to-1 compression method with AnemoiJive, *Rescue–Prime*, Poseidon and Griffin over the 64-bit prime field $\mathbb{F}_p$ with $p = 2^{64} - 2^{32} + 1$. Each instantiation has a 4-field-element (32 bytes) digest size to ensure 128-bit security.[4] *Rescue–Prime*, Poseidon and Griffin have been evaluated with two instantiations: a regular of width 12 with rate 8, capable of compressing two digests with one permutation using the

[4] We refer here to original instantiations, in opposition to a common practice in the industry to tweak parameters (typically the MDS matrix layer). All instantiations here are original paper versions for fair comparison.

sponge construction, and an instantiation of width 8 with rate 4 using `Jive` as compression mode. All experiments were implemented in Rust and performed on an *Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz*. We present average times in microseconds of each experiment running for 5 seconds.

Rescue-P-12	*Rescue-P*-8	Poseidon-12	Poseidon-8	Griffin-12	Griffin-8	`Anemoi-8`
15.67μs	9.13μs	5.87μs	2.69μs	2.87μs	**2.59μs**	4.21μs

Table 3.6: *Native performance of 2-to-1 compression functions for $\mathbb{F}_p$ with $p = 2^{64} - 2^{32} + 1$.*

In Table 3.7, we compare the native performance with *Rescue–Prime*, Poseidon and Griffin with a state size useful for applications like Merkle tree over the scalar field of BLS12-381.

For small state size, the dominant computation for `Anemoi` (like *Rescue–Prime* and Griffin) is $x^{1/d}$ and can be implemented using an appropriate addition chain. Griffin is instantiated with a state size of 3 and `Anemoi`, *Rescue–Prime* and Poseidon with a state size of 2. All experiments were implemented in C and performed on an *Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz*. We present average times in microseconds of each experiment running for 2 seconds.

Rescue–Prime	Poseidon	Griffin	`Anemoi`
206μs	**9.2μs**	74.18μs	128.29μs

Table 3.7: *Native performance of a permutation for the scalar field of BLS12-381.*

It is worth noting that Poseidon, which is a "type 1" primitive, as defined in Chapter 1, is much faster because of the low degree round function. Among the four primitives, Poseidon is indeed the only one that does not involve exponentiations $x^{1/d}$.

Conclusion

Our main contribution in this chapter is of course `Anemoi`, a family of permutations that are efficient across various arithmetization methods, using a previously unknown link between CCZ-equivalence and Arithmetization-Orientation. We must also mention that `Anemoi` has its own logo, described in Figure 3.7. The two butterflies, one with open wings and one with closed wings, are referring to the open and closed `Flystel`. The two variants are known to be CCZ-equivalent which is symbolized by a mirror, more precisely it is a sun-shaped mirror, highlighting that the closed `Flystel` is what makes the strength of `Anemoi`. A cloud also reminds that `Anemoi` represents Gods of wind.

This yields gains from 10% up to more than 50% depending on the context, over existing designs. More precisely, `Anemoi` has about a factor of 2 improvement over Poseidon and *Rescue* in terms of R1CS constraints, a 21%-35% $\mathcal{P}\mathfrak{lon}\mathcal{K}$ constraint reduction over a highly optimized Poseidon implementation, as well as competitive native performances, running between two and three times faster than *Rescue–Prime*, depending on the field size.

Finally, we provided a new simple mode, $\texttt{Jive}_b$, which adds to the growing list of permutation-based modes of operation providing a b-to-1 compression function, of particular relevance in Merkle trees. It allows us to further improve upon the state-of-the-art, so that `Anemoi` `Jive` requires only 56 $\mathcal{P}\mathfrak{lon}\mathcal{K}$ constraints in total (when 3 wires and 2 custom gates are used), compared to the best sponge-based instance of Poseidon which requires 98 constraints with 4 wires (or 110 with

Figure 3.7: `Anemoi` *logo.*

3) and 1 custom gate. With only one custom gate, `AnemoiJive` requires 64 constraints for 4 wires (or 86 with 3).

Interestingly recent work by Liu *et al.* [Liu+22] has already demonstrated the potential for further optimizations leveraging our design: by using four custom gates they are able to reduce the cost of a 3-to-1 `Jive` instance to just over one constraint per round (16 constraints for 14 rounds).

Chapter 4 Algebraic attacks against some Arithmetization-Oriented primitives

Algebraic attacks are often the ones chosen by designers to determine the number of rounds of Arithmetization-Oriented primitives. In this chapter we investigate the security of various primitives against such attacks. More particularly, in this chapter we focus on solving the Constrained Input Constrained Output (CICO) problem for reduced versions of these new symmetric primitives defined over large finite fields. Since Arithmetization-Oriented primitives mostly rely on low-degree polynomial implementations, it is important to study the resistance against algebraic attacks of such primitives. Most of the results presented in this chapter are inspired by some cryptanalysis challenges that were proposed by the Ethereum Foundation in November 2021 [Fou21].

In Section 4.1 we will first explain the difference between solving univariate and multivariate systems, focusing on the CICO problem. We will also see a simple application with the example of Feistel–MiMC. Then, we will explain how to bypass rounds for SPN constructions, in Section 4.2, to decrease the complexity of solving the polynomial system, taking the examples of Poseidon and *Rescue–Prime*. We will also briefly discuss some possible tricks for other primitives. Finally, in Section 4.3 we will see the importance of the choice of the modeling with the examples of Ciminion and Anemoi.

The work presented in this chapter, on Feistel–MiMC, Poseidon and *Rescue–Prime*, which started thanks to cryptanalysis challenges proposed by the Ethereum foundation, as well as the results obtained on Ciminion, have been obtained with Augustin Bariant, Gaëtan Leurent, and Léo Perrin, and published in the journal *IACR Transactions on Symmetric Cryptology* in 2022 [Bar+22].

Contents

4.1 Systems solving

The CICO (Constrained Input Constrained Output) problem [Ber+11] has been identified as a major problem in several attacks against symmetric primitives. Solving this problem must be difficult to ensure that attackers cannot obtain sensitive information by manipulating the inputs and outputs of the system. The CICO problem can be defined as finding the solution of a polynomial system. In this section we discuss the different strategies to solve polynomial systems.

4.1.1 Univariate and multivariate solving

Let us consider a system $(\mathcal{S})$ composed of n polynomial equations on n variables $X_1 \dots X_n$ in $\mathbb{F}_q$ (for simplicity we choose the same number of equations as variables):

$$(\mathcal{S}) : \begin{cases} P_1(X_1, \dots X_n) = 0 \\ P_2(X_1, \dots X_n) = 0 \\ \qquad\qquad\vdots \\ P_n(X_1, \dots X_n) = 0 \end{cases}$$

We assume that the system is non-trivial and that there exists a solution (in $\mathbb{F}_q^n$) of this system that gives sufficient information to break the cryptosystem.

4.1.1.1 Complexity of univariate systems

In the univariate case, the system is composed of a single equation in a single variable X so that we have:

$$P(X) = 0\,.$$

Solving such a system consists in finding the roots of the polynomial $P \in \mathbb{F}_q[X]$. Let d be the degree of P. We proceed as follows.

1. We first compute $Q = X^q - X \mod P$, that requires $\mathcal{O}(d \log(q) \log(d) \log(\log(d)))$ field operations using a double-and-add algorithm.

2. Then, we compute $R = \gcd(P, Q) = \gcd(P, X^q - X)$, so that R has the same roots as P in the field $\mathbb{F}_q$, but its degree is much lower. This step requires $\mathcal{O}(d \log^2(d) \log(\log(d)))$ field operations.

3. Finally, we factor R. The complexity of this step is negligible. Indeed, R is usually of degree one or two since P only has a few roots in the field.

Summing the complexity of the first two steps yields

$$\mathcal{O}\big(d \log(d) \big(\log(d) + \log(q)\big) \log(\log(d))\big)\,, \tag{4.1}$$

implying that the complexity is quasi-linear in the degree of the polynomial.

4.1.1.2 Complexity of multivariate systems

In the multivariate case, we usually have a system with n polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$. The notion of regularity plays a crucial role in the solving of multivariate systems.

Definition 4.1. A system is said to be *regular* if for all i, $gP_i \in \langle P_1, \ldots, P_{i-1} \rangle$ implies that $g \in \langle P_1, \ldots, P_{i-1} \rangle$.

A thorough analysis of specific non-regular systems is very complex for designers. Therefore, a common practice is to estimate the complexity of the Gröbner basis attack for an equivalent regular system, and to add a few rounds as a security margin to take into account the non-regularity of the system.

Let us denote d_i the degree of the polynomial P_i, d the degree of the ideal $\mathcal{I} = \langle P_1, \ldots, P_n \rangle$, and D_{reg} the degree of regularity of $\mathcal{I}$, as defined by Dubois *et al.* in [DG10]. We have

$$D_{\text{reg}} \leqslant 1 + \sum_{i=1}^{n} (d_i - 1) \qquad\qquad d \leqslant \prod_{i=1}^{n} d_i \, .$$

Let us remark that the bounds are reached when the system is regular but the upper bound does not require the system to be regular.

The main technique to solve the multivariate polynomial systems is to compute a Gröbner basis [Buc76] of the ideal $\mathcal{I}$. A Gröbner basis G of $\mathcal{I}$, with respect to a total ordering on the set of monomials, is a particular generating set of $\mathcal{I}$. Gröbner bases become very interesting under the *lexicographic* order since they take the form

$$\{g_1(X_1), g_{2,1}(X_1, X_2), \ldots g_{2,h_2}(X_1, X_2), \ldots g_{n,1}(X_1, \ldots, X_n), \ldots g_{n,h_n}(X_1, \ldots, X_n)\} \, .$$

Indeed, the solutions of this system are easy to recover iteratively by first computing the roots of g_1 in $\mathbb{F}_q$, then substituting X_1 in polynomials $g_{2,i}$, then computing the roots of $g_{2,i}$, ... until g_{n,h_n}.

Directly computing a Gröbner basis in the *lexicographic* order is expensive. Therefore, Faugère *et al.* [Fau+93] proposed to first compute the Gröbner basis in another order. The overall approach to solve a multivariate system of equations is given by the following steps, where the complexity depends on the number of variables n, the degree of the ideal d and the degree of regularity D_{reg}.

1. We first compute a Gröbner basis under the *grevlex* order, using the F5 algorithm. If the polynomial system is regular, then the complexity of this algorithm is bounded by

   $$\mathcal{O}\left(nD_{\text{reg}} \times \binom{n + D_{\text{reg}} - 1}{D_{\text{reg}}}^{\omega}\right) ,$$

   where $\omega \in [2, 3]$ is the matrix multiplication exponent [BFS15]. Let us notice that in the security analysis of some Arithmetization-Oriented primitives like Ciminion [Dob+21], Poseidon [Gra+21], or *Rescue* [Aly+20], another correct upper bound from [BFS04] is used:

   $$\mathcal{O}\left(\binom{n + D_{\text{reg}}}{D_{\text{reg}}}^{\omega}\right) .$$

2. We then change the order by converting this basis into a *lexicographic-ordered* Gröbner basis using the FGLM algorithm. While, the original algorithm [Fau+93] has a complexity of $\mathcal{O}(nd^3)$, more recent variants reach better complexities with probabilistic methods, achieving:

   $$\mathcal{O}(nd^{\omega}) \, , \text{ in [Fau+14]} \qquad \text{or} \qquad \mathcal{O}\left(\sqrt{n}d^{2+\frac{n-1}{n}}\right) \, , \text{ in [FM17].}$$

3. Finally, we have to find the roots in $\mathbb{F}_q^n$ of the Gröbner basis polynomials using univariate system resolution, as previously described, and substitution. This step is of complexity roughly $\mathcal{O}(d \log^2(d))$.

Overall, the univariate solving tends to be much more efficient than the multivariate solving. However, it cannot be applied to all algorithms as there are efficient methods to prevent its applicability, as was done by the designers of *Rescue–Prime* for example, or as we did in `Anemoi` (see Chapter 3).

4.1.2 CICO problem

4.1.2.1 Definition

In this chapter, we assess the security of several algorithms against algebraic attacks, and more precisely we study the security of primitives against attacks solving the CICO problem.

Let $t < m$ be an integer, and let $\mathcal{Z}_t$ be the vector space spanned by the canonical basis $\{e_0, ..., e_{m-t-1}\}$. In other words, $\mathcal{Z}_t$ is the set of all the elements of $\mathbb{F}_q^m$ whose last t coordinates are equal to 0.

Definition 4.2 (CICO Problem)**.** Let $F : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be a function, and let $t < m$ be an integer. The CICO *problem* consists in finding $x \in \mathbb{F}_q^m$ such that

$$x \in \mathcal{Z}_t \text{ and } F(x) \in \mathcal{Z}_t .$$

A brute-force approach would solve this problem with a time complexity of about q^t calls to the permutation: the idea would simply be to try random values x of $\mathcal{Z}_t$ until one of them satisfies $F(x) \in \mathcal{Z}_t$. The ability to solve this problem more efficiently than this brute-force search would potentially allow an attacker to find preimages for a given digest in a sponge mode, or could help with finding collisions, hence its relevance.

4.1.2.2 Ethereum challenges

The main part of the analysis presented in this chapter started with some cryptanalysis challenges proposed by the Ethereum Foundation in November 2021 [Fou21]. Those challenges are explicitly about solving the CICO problem for the permutations used by several AO hash functions, namely Feistel–MiMC, Poseidon, *Rescue–Prime* and `Reinforced Concrete`.

We then manage to get practical attacks for three of the primitives: Feistel–MiMC, Poseidon and *Rescue–Prime*. It is worth noting that the complexity of some of our attacks matches the designers' claims. However, we have found that, in practice, the exact claimed security level for a given number of rounds is not always straightforward. Furthermore, by breaking challenges in practice we give a more concrete understanding of the security of reduced versions. Besides, in the designer's analysis some optimistic complexity assumptions are made regarding the capacity for an attacker to solve polynomial systems, as for example ignoring log factors, or taking a small ω for the matrix multiplication exponent. However, in this chapter we propose a more accurate analysis, focusing on upper bounds rather than lower bounds.

4.1.3 A first example: Feistel–MiMC

We recall that Feistel–MiMC is a Feistel network, based on the simple structure of MiMC, introduced by Albrecht *et al.* [Alb+16]. It operates on $\mathbb{F}_p^2$ ($m = 2$), in this case, using a basic

r-round Feistel structure with the i-th round function being $x \mapsto (x + c_i)^d$, so that $x \mapsto x^d$ is a permutation. In this chapter, we will take $d = 3$, as fixed by the authors of the Ethereum's challenges.

In order to build a polynomial system representing the CICO problem, we consider an input state $(\mathcal{P}_0, \mathcal{Q}_0) = (\mathbf{X}, 0)$. Then we evaluate the round function iteratively, as polynomials in $\mathbb{F}_p[\mathbf{X}]$:

$$\begin{cases} \mathcal{P}_i &= \mathcal{Q}_{i-1} + (\mathcal{P}_{i-1} + c_i)^3 \\ \mathcal{Q}_i &= \mathcal{P}_{i-1} \,. \end{cases}$$

In Figure 4.1, we show how we generate the equations.

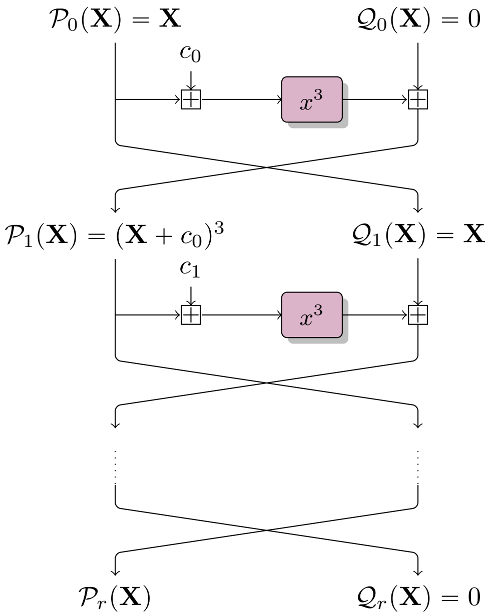

$\mathcal{P}_0(\mathbf{X}) = \mathbf{X}$
$\mathcal{Q}_0(\mathbf{X}) = 0$
c_0
x^3
$\mathcal{P}_1(\mathbf{X}) = (\mathbf{X} + c_0)^3$
$\mathcal{Q}_1(\mathbf{X}) = \mathbf{X}$
c_1
x^3
$\mathcal{P}_r(\mathbf{X})$
$\mathcal{Q}_r(\mathbf{X}) = 0$

Figure 4.1: Generating equation for Feistel–MiMC.

The CICO problem then consists in solving $\mathcal{Q}_r = 0$, i.e. we just have to find the roots of $\mathcal{Q}_r = \mathcal{P}_{r-1}$. Since the round function has degree 3, we obtain a univariate polynomial $\mathcal{P}_{r-1}$ of degree $\deg^u = 3^{r-1}$ after $r - 1$ rounds. As this is a univariate system, we can estimate the complexity of finding the roots by using Equation (4.1):

$$3^{r-1} \times (r-1) \times 1.58 \times 64 \times \log_2(r-1).$$

We give explicit values for the proposed challenges in Table 4.1, where complexity figures in bold correspond to attacks that we have implemented in practice. Parameters have changed while we were working on it, then “original” (Table 4.1a) and “new parameters” (Table 4.1b) are two sets of parameters proposed by the Ethereum Foundation, the first ones being less secure than the latter ones.

We observe that the security claims from the Ethereum Foundation are close to 3^{2r}. This likely corresponds to an estimation of the complexity of a Gröbner base attack using r equations of degree 3 in r variables: the corresponding complexity would be $3^{\omega r} \geqslant 3^{2r}$.

r	Authors claims		Ethereum claims	$\deg^u$		Our complexity
	Lagrange	*GCD*				
6	2^{16}	2^{5}	2^{18}	3^{5}	$\approx 2^{7.9}$	$\mathbf{2^{19}}$
10	2^{30}	2^{9}	2^{30}	3^{9}	$\approx 2^{14.3}$	$\mathbf{2^{26}}$
14	2^{43}	2^{13}	2^{44}	3^{13}	$\approx 2^{20.6}$	$\mathbf{2^{33}}$
18	2^{56}	2^{17}	2^{56}	3^{17}	$\approx 2^{26.9}$	$\mathbf{2^{40}}$
22	2^{69}	2^{21}	2^{68}	3^{21}	$\approx 2^{33.3}$	2^{47}

(a) Original parameters.

r	Authors claims		Ethereum claims	$\deg^u$		Our complexity
	Lagrange	*GCD*				
22	2^{69}	2^{21}	2^{36}	3^{21}	$\approx 2^{33.3}$	2^{47}
25	2^{79}	2^{24}	2^{40}	3^{24}	$\approx 2^{38.0}$	2^{52}
30	2^{95}	2^{28}	2^{48}	3^{29}	$\approx 2^{46.0}$	2^{60}
35	2^{111}	2^{33}	2^{56}	3^{34}	$\approx 2^{53.9}$	2^{69}
40	2^{127}	2^{37}	2^{64}	3^{39}	$\approx 2^{61.8}$	2^{77}

(b) New parameters.

Table 4.1: *Complexity of our attack against Feistel–MiMC, compared with the security claims given by the authors and by the challenges.*

Besides, the original specification of Feistel–MiMC states that Lagrange interpolation attacks are expected to have a complexity of $r \cdot 3^{2r-3}$, while GCDs attacks are expected to have a complexity of $r^2 \cdot 3^{r/2-3}$. As the latter leaves more freedom to the attacker, it does not apply in our context. However, we have decided to put both in Table 4.1 for a fairer comparison.

4.2 Bypassing rounds

In this section, we see that some tricks can allow the attacker to bypass some rounds or at least simplify the polynomial system.

4.2.1 Trick for SPN

We first propose a trick to bypass rounds for SPN construction where the S-box is a monomial function. We will in particular see some applications for Poseidon and *Rescue–Prime*.

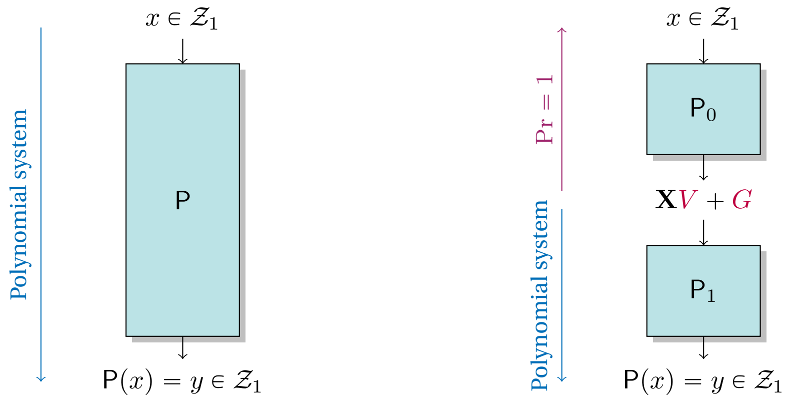
4.2.1.1 General idea

First, let us introduce the general idea. Solving the CICO problem for a permutation P with R rounds normally means solving a polynomial system for the entire permutation, so for R rounds. Here we propose to split the permutation into two permutations such that we only need to construct a polynomial system for one of the small permutations.

Let $\mathsf{P} = \mathsf{P}_0 \circ \mathsf{P}_1$ be a permutation of $\mathbb{F}_p^m$. We suppose that there exist two vectors V and G in $\mathbb{F}_p^m$ such that for all $\mathbf{X} \in \mathbb{F}_p$ we have:

$$\mathsf{P}_0^{-1}(\mathbf{X}V + G) \in \mathcal{Z}_1 \,.$$

In this case, we write all the intermediate variables of P_1 as polynomials in $\mathbf{X}$, starting from the state $\mathbf{X}V + G$, and evaluating round operations one by one as polynomials. Then we can find r such that $\mathsf{P}_1(rV + G) \in \mathcal{Z}_1$ by finding a root r of the polynomial corresponding to the last coordinate of the output. Finally, setting $x = (x_0, x_1, \ldots x_{m-1}) = \mathsf{P}_0^{-1}(rV + G)$ will yield a solution to the CICO problem, while the solver has to handle a polynomial based on P_1 rather than the full P. This approach is summarized in Figure 4.2, and we used it against both Poseidon (see Section 4.2.1.2) and *Rescue–Prime* (see Section 4.2.1.3).



(a) *R-round system.* **(b)** *$(R-2)$-round system.*

Figure 4.2: *A 2-staged trick.*

Let us describe this trick in more detail. First, for the sake of consistency, we will use *steps* when referring to the composition of constant addition, the S-box, and the linear part. Then one *round* of Poseidon consists of one step, and one round of *Rescue–Prime* of two steps: one using S as S-box, the other using S^{-1}.

We consider P_0 to be two steps of an SPN construction without the final linear layer: addition of round constants, S-box layer S_1, linear layer consisting of a multiplication by an MDS matrix, and S-box layer S_2, i.e. we have:

$$\mathsf{P}_0(x) = (S_2 \circ M \circ S_1 \circ \mathsf{Add})(x) \,.$$

We require the S-boxes to be monomial functions, so that $S(A\mathbf{X}) = S(A)S(\mathbf{X})$. We let c_i^r be the i-th round constant used in step r and M_m be the linear layer such that:

$$M_m^{-1} = \begin{bmatrix} \alpha_{0,0} & \alpha_{1,0} & \cdots & \alpha_{m-1,0} \\ \alpha_{0,1} & \alpha_{1,1} & \cdots & \alpha_{m-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{0,m-1} & \alpha_{1,m-1} & \cdots & \alpha_{m-1,m-1} \end{bmatrix} .$$

Trick when $m = 3$

Let us start with the special case $m = 3$. We denote the state after P_0 with variables $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$. Figure 4.3 illustrates how to bypass P_0.

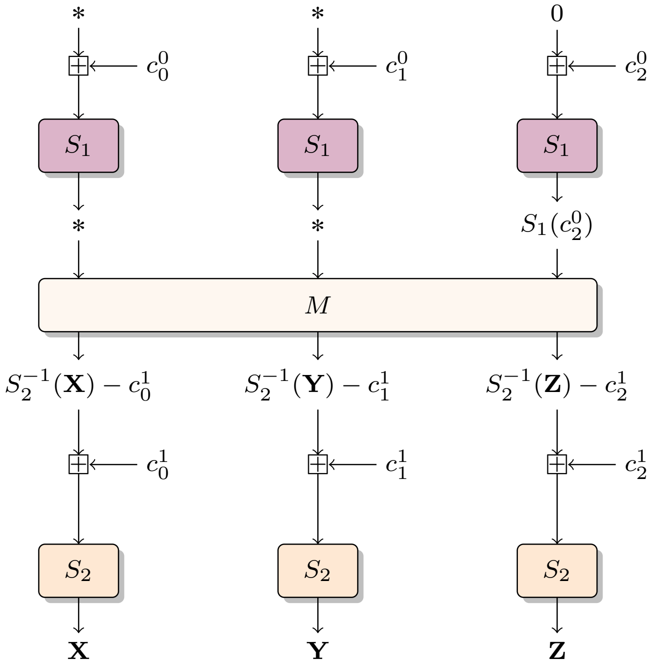


Figure 4.3: *Bypassing two SPN steps ($m = 3$).*

In particular, we see that the condition $\mathsf{P}_0^{-1}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{Z}_1$ is satisfied if and only if

$$\begin{pmatrix} * \\ * \\ S_1(c_2^0) \end{pmatrix} = M^{-1} \times \begin{pmatrix} S_2^{-1}(\mathbf{X}) - c_0^1 \\ S_2^{-1}(\mathbf{Y}) - c_1^1 \\ S_2^{-1}(\mathbf{Z}) - c_2^1 \end{pmatrix} .$$

So the last element of the vector, $S_1(c_2^0)$, must satisfy:

$$\begin{aligned} S_1(c_2^0) &= \alpha_{0,2}(S_2^{-1}(\mathbf{X}) - c_0^1) + \alpha_{1,2}(S_2^{-1}(\mathbf{Y}) - c_1^1) + \alpha_{2,2}(S_2^{-1}(\mathbf{Z}) - c_2^1) \\ &= \alpha_{0,2}S_2^{-1}(\mathbf{X}) + \alpha_{1,2}S_2^{-1}(\mathbf{Y}) + \alpha_{2,2}S_2^{-1}(\mathbf{Z}) - (\alpha_{0,2}c_0^1 + \alpha_{1,2}c_1^1 + \alpha_{2,2}c_2^1) . \end{aligned}$$

In order to simplify the equation, we fix $\mathbf{Z}$ to a constant value g with:

$$g = S_2\big(\alpha_{2,2}^{-1}(\alpha_{0,2}c_0^1 + \alpha_{1,2}c_1^1 + \alpha_{2,2}c_2^1 + S_1(c_2^0))\big) .$$

We obtain

$$\begin{aligned} S_1(c_2^0) &= \alpha_{0,2}S_2^{-1}(\mathbf{X}) + \alpha_{1,2}S_2^{-1}(\mathbf{Y}) + \alpha_{2,2}S_2^{-1}(g) - (\alpha_{0,2}c_0^1 + \alpha_{1,2}c_1^1 + \alpha_{2,2}c_2^1) \\ &= \alpha_{0,2}S_2^{-1}(\mathbf{X}) + \alpha_{1,2}S_2^{-1}(\mathbf{Y}) + S_1(c_2^0) . \end{aligned}$$

It follows that

$$\begin{aligned}
\mathsf{P}_0^{-1}(\mathbf{X}, \mathbf{Y}, g) \in \mathcal{Z}_1 &\iff -\alpha_{1,2}(S_2^{-1}(\mathbf{Y})) = \alpha_{0,2}(S_2^{-1}(\mathbf{X})) \\
&\iff S_2(-\alpha_{1,2})\mathbf{Y} = S_2(\alpha_{0,2})\mathbf{X} \\
&\iff \mathbf{Y} = S_2(\alpha_{0,2})/S_2(-\alpha_{1,2})\mathbf{X}
\end{aligned}$$

Therefore, we obtain an affine space with $\mathsf{P}_1(\mathbf{X}V + G) \in \mathcal{Z}_1$ by choosing:

$$V = (1,\ S_2(\alpha_{0,2})/S_2(-\alpha_{1,2}),\ 0) \text{ and } G = (0, 0, g)\,.$$

General case $(m \geqslant 3)$

In general, we take vectors V and G such that $V = (S_2(A_0), \ldots, S_2(A_{m-2}), 0)$ and $G = (0, \ldots, 0, g)$. Therefore, we can consider an input state after the S-box layer of the second step of the form $(S_2(A_0)\mathbf{X}, \ldots, S_2(A_{m-2})\mathbf{X}, g)$, and study the first two steps as shown in Figure 4.4.

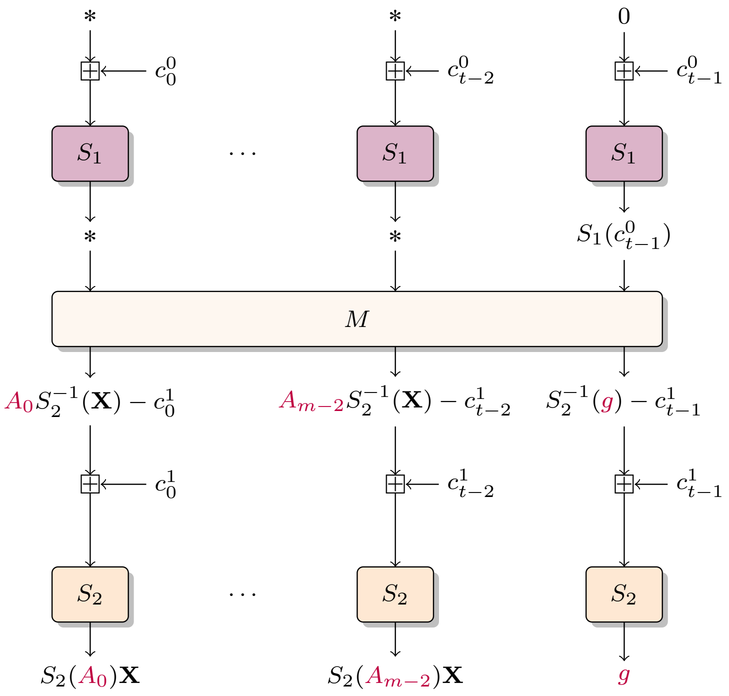


Figure 4.4: *Bypassing two SPN steps (general case).*

Following Figure 4.4, the value $S_1(c_{m-1}^0)$ must satisfy

$$\begin{aligned}
S_1(c_{t-1}^0) &= \sum_{j=0}^{t-2} \alpha_{j,2}(A_j S_2^{-1}(\mathbf{X}) - c_j^1) + \alpha_{m-1,2}(S_2^{-1}(g) - c_{m-1}^1) \\
&= S_2^{-1}(\mathbf{X}) \left(\sum_{j=0}^{m-2} \alpha_{j,2} A_j \right) + \alpha_{m-1,2} S_2^{-1}(g) - \sum_{j=0}^{t-1} \alpha_{j,2} c_j^1\,.
\end{aligned}$$

It is the case provided for instance that:

$$\begin{cases} A_{m-2} & = -\sum_{j=0}^{m-3} \frac{\alpha_{j,2}}{\alpha_{m-2,2}} A_j \\ g & = S_2\left(\frac{1}{\alpha_{m-1,2}} \sum_{j=0}^{m-1} \alpha_{j,2} c_j^1 + S_1(c_{m-1}^0) \right) . \end{cases} \tag{4.2}$$

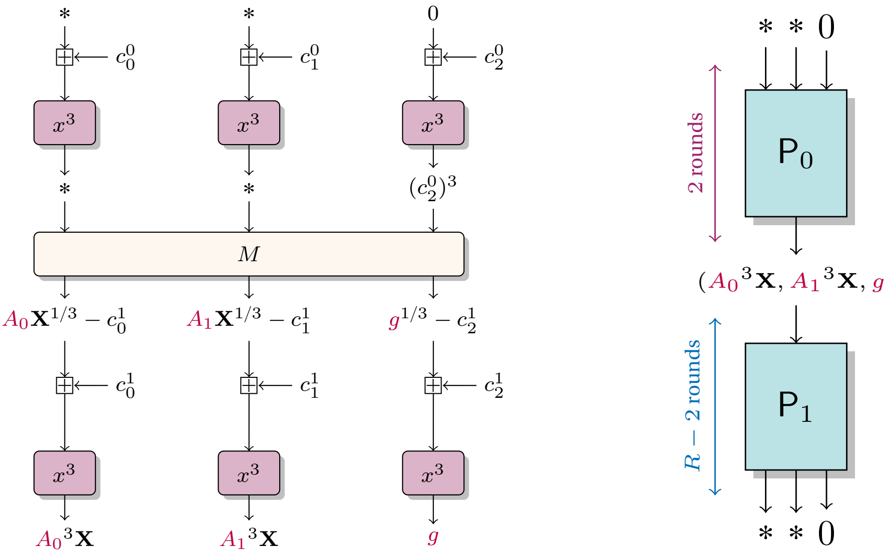
As a consequence, if we find a value $\mathbf{X}$ such that the image of $(S_2(A_0)\mathbf{X}, \ldots, S_2(A_{m-2})\mathbf{X}, g)$ through $R-2$ steps of the primitive is equal to $(*, \ldots, *, 0)$, then we will always be able to deduce an input $(x_0, x_1, \ldots, x_{m-2}, 0)$ for R steps of the primitive that is mapped to $\mathcal{Z}_1$.

4.2.1.2 Application to Round-Reduced Poseidon

We recall that Poseidon [Gra+21], introduced in Chapter 1, is composed of $R = \mathsf{RF} + \mathsf{RP}$ rounds of two different types: full rounds have m S-box functions, and partial rounds have only one S-box and $m-1$ identity functions. The challenges from the Ethereum Foundation use $m = 3$, the S-box is $x \mapsto x^3$ and $\mathsf{RF} = 8$ is fixed, while RP varies according to the security level required.

A basic encoding of Poseidon into equations can be solved quickly for a small number of rounds. However, targeting more rounds requires to use the technique described in Section 4.2.1.1. The idea is to decrease the degree and the complexity of the polynomial system by more carefully choosing its variables.

Let $m = 3$, and S_1, S_2 such that $S_1(x) = S_2(x) = x^3$. Then, applying our trick for SPN rounds, we consider an input state after the S-box layer of the second round of the form $({A_0}^3\mathbf{X}, {A_1}^3\mathbf{X}, g)$ i.e. we use $V = ({A_0}^3, {A_1}^3, 0)$ and $G = (0, 0, g)$. We describe how we bypass two rounds of Poseidon in Figure 4.5.



(a) First two rounds.

(b) Overview.

Figure 4.5: How to bypass the first two rounds of Poseidon.

We obtain

$$\begin{cases} A_1 &= -\frac{\alpha_{0,2}}{\alpha_{1,2}} A_0 \\ g &= \left(\frac{1}{\alpha_{2,2}}\left(\alpha_{0,2}c_0^1 + \alpha_{1,2}c_1^1\right) + c_2^1 + (c_2^0)^3\right)^3 . \end{cases} \tag{4.3}$$

As previously mentioned, if we find a value $\mathbf{X}$ such that the image of $({A_0}^3\mathbf{X}, {A_1}^3\mathbf{X}, g)$ through $R-2$ rounds of Poseidon (and a linear layer) is equal to $(*,*,0)$, then we will always be able to deduce an input $(x,y,0)$ for R-round of Poseidon that is mapped to $\mathcal{Z}_1$.

Therefore, we evaluate the permutation as polynomials in $\mathbb{F}_p[\mathbf{X}]$ starting from the state $({A_0}^3\mathbf{X}, {A_1}^3\mathbf{X}, g)$ with A_0, A_1, g satisfying System (4.3), and solving the CICO problem is equivalent to finding the root of the polynomial corresponding to the rightmost branch of the output.

4.2.1.3 Application to Round-Reduced *Rescue–Prime*

We recall that each round of *Rescue–Prime*, consists of two steps: while the first one involves an S-box S, an MDS matrix M, and the addition of the round constants, the second one is quite similar but replaces S with its inverse S^{-1}. For our study, we will use the specifications of *Rescue–Prime* [SAD20], which means in particular that in each round, we first apply $S: x \mapsto x^3$ and then S^{-1} (rather than the contrary as described in the original paper [Aly+20]).

The challenges from the Ethereum Foundation use $m = 3$ or $m = 2$, and the S-boxes are $x \mapsto x^3$ and its inverse $x \mapsto x^{1/3}$.

Let us repeat the idea described in the previous section and apply it to *Rescue–Prime*. Let $m = 3$, and S_1, S_2 such that $S_1(x) = x^3$, and $S_2(x) = S_1^{-1}(x) = x^{1/3}$. We consider an input state after the S-box layer of the second step of the form $({A_0}^{1/3}\mathbf{X}, {A_1}^{1/3}\mathbf{X}, g)$ i.e. we use $V = ({A_0}^{1/3}, {A_1}^{1/3}, 0)$ and $G = (0, 0, g)$.

We first notice that we can switch the order of the multiplication by the MDS matrix and the addition of the constants. Let

$$\begin{pmatrix} C_0^0 \\ C_1^0 \\ C_2^0 \end{pmatrix} = M^{-1} \begin{pmatrix} c_0^0 \\ c_1^0 \\ c_2^0 \end{pmatrix} .$$

In particular, we have:

$$C_2^0 = \alpha_{0,2}c_0^0 + \alpha_{1,2}c_1^0 + \alpha_{2,2}c_2^0 .$$

As a consequence, using the same notation as above, the value C_2^0, in Figure 4.6, must satisfy

$$\begin{aligned} C_2^0 &= \alpha_{0,2}A_0\mathbf{X}^3 + \alpha_{1,2}A_1\mathbf{X}^3 + \alpha_{2,2}g^3 \\ &= \mathbf{X}^3\left(\alpha_{0,2}A_0 + \alpha_{1,2}A_1\right) + \alpha_{2,2}g^3 . \end{aligned}$$

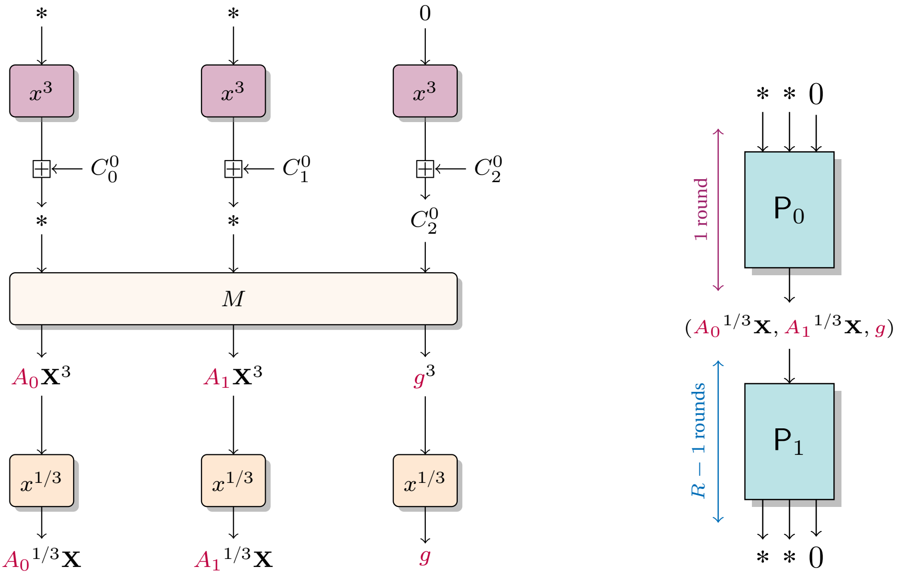
It is the case for instance when:

$$\begin{cases} A_1 &= -\frac{\alpha_{0,2}}{\alpha_{1,2}} A_0 \\ g &= \left(\frac{1}{\alpha_{2,2}}\left(\alpha_{0,2}c_0^0 + \alpha_{1,2}c_1^0\right) + c_2^0\right)^{1/3} . \end{cases}$$

It follows that, if we find a value $\mathbf{X}$ such that the image of $({A_0}^{1/3}\mathbf{X}, {A_1}^{1/3}\mathbf{X}, g)$ through $R-1$ rounds of *Rescue–Prime* (and a linear layer) is equal to $(*,*,0)$, then we will always be able to deduce an input $(x,y,0)$ for R-round *Rescue–Prime* that is mapped to $\mathcal{Z}_1$.

Then, for the remaining $R-1$ rounds, Figure 4.7 shows how we generate the following polynomial equations to avoid the inverse S-box.

$$\forall j \in \{0,1,2\},\ \mathcal{P}_{i,j}(X_i, Y_i, Z_i) - \mathcal{Q}_{i,j}(X_{i+1}, Y_{i+1}, Z_{i+1}) = 0 .$$



(a) *First round.*

(b) *Overview.*

Figure 4.6: *How to bypass the first round (i.e. the first two steps) of Rescue–Prime.*

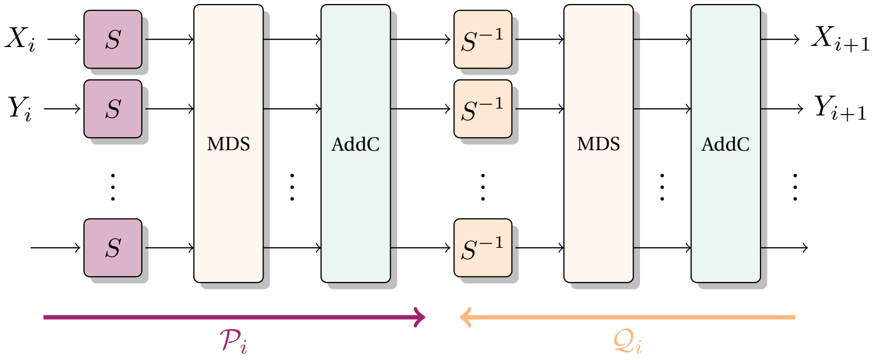


Figure 4.7: *Round i of Rescue–Prime.*

Finally, this results in the following system of polynomial equations:

$$\begin{cases} \forall\, 1 \leqslant i \leqslant N-1, \forall\, j \in \{0,1,2\}, \\ \mathcal{P}_{i,j}(X_i, Y_i, Z_i) - \mathcal{Q}_{i,j}(X_{i+1}, Y_{i+1}, Z_{i+1}) = 0\,, \end{cases}$$

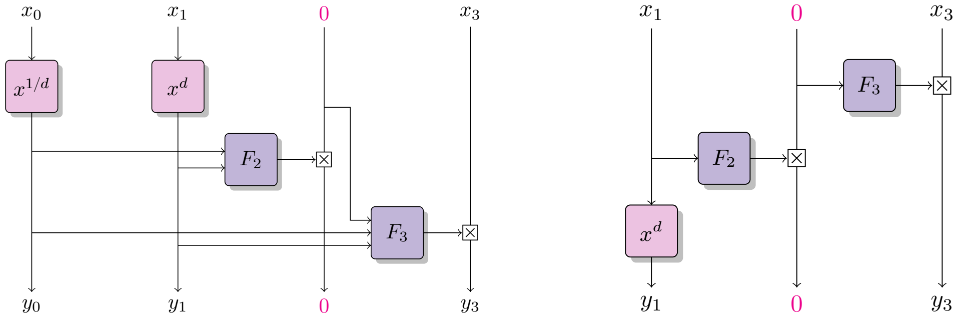
where $Z_R = 0$ and

$$\begin{pmatrix} X_1 \\ Y_1 \\ Z_1 \end{pmatrix} = M \begin{pmatrix} {A_0}^{1/3}\mathbf{X} \\ {A_1}^{1/3}\mathbf{X} \\ g \end{pmatrix} + \begin{pmatrix} c_0^1 \\ c_1^1 \\ c_2^1 \end{pmatrix}.$$

This system has $m(R-1)$ variables and $m(R-1)$ equations.

4.2.2 Trick for other primitives

What is interesting is to detect the existence of particular spaces when iterating rounds. Then let us see if we can observe a similar property for other primitives. Let us take the examples of Griffin and Reinforced Concrete since the non-linear layer used in both designs is using similar ideas, i.e. multiplications between branches. Those constructions are not based on classical SPN, using one S-box per branch, however, because of the multiplication we can still observe some propagation of subspaces. In Figure 4.8a and Figure 4.8b, we show for Griffin and Reinforced Concrete, respectively, that having a 0 in input branch x_i implies a 0 in the corresponding output branch y_i. Such a property is independent of the form of the functions F_i used in the figures (see Chapter 1 for the precise form of the F_i for both Griffin and Reinforced Concrete).



(a) For Griffin. *(b) For Reinforced Concrete.*

Figure 4.8: Propagation of subspaces.

It is worth mentioning that such a property cannot be observed for example for Anemoi thanks to the construction of its non-linear layer based on a 3-round Feistel network (see Chapter 2). The Flystel is an S-box that operates on $\mathbb{F}_q^2$ such that any element of the form $(x, 0)$ or of the form $(0, x)$ is not necessarily sent to $(x, 0)$ or $(0, x)$ respectively (except for the particular case $x = 0$).

In the case of Reinforced Concrete, the linear layer Concrete is the circulant matrix $(2, 1, 1)$. Then, we also notice that spaces of the following form are preserved by the linear layer:

$$\begin{pmatrix} x \\ -x \\ 0 \end{pmatrix}, \quad \begin{pmatrix} x \\ 0 \\ -x \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 \\ x \\ -x \end{pmatrix}.$$

However these observations should not threaten the complexity of solving polynomial systems because the resistance of Reinforced Concrete to algebraic attacks relies on its middle layer Bar for its resistance to algebraic attacks.

In the case of Griffin, the use of both $x^{1/d}$ and x^d at the same step would complicate the application of the trick presented in Section 4.2.1.1.

4.2.3 Impact on the solving complexity

4.2.3.1 Poseidon

Poseidon has $R = \text{RF} + \text{RP}$ rounds in total, but we skip the first two rounds using the trick of Section 4.2.1.1. Therefore, we obtain a univariate polynomial of degree $\deg^u = 3^{R-2}$, and since the system is univariate, we can estimate the complexity of finding the roots using Equation (4.1) leading to:

$$3^{R-2} \times (R-2) \times 1.58 \times 64 \times \log_2(R-2)\,.$$

We give explicit values for the proposed challenges in Table 4.2, along with the corresponding security claims. Complexity figures in bold correspond to attacks that we have implemented in practice, breaking some challenges issued by the Ethereum foundation.

RP	Authors claims	Ethereum claims	$\deg^u$	Our complexity
3	2^{17}	2^{45}	$3^{9} \approx 2^{14.3}$	$\mathbf{2^{26}}$
8	2^{25}	2^{53}	$3^{14} \approx 2^{22.2}$	$\mathbf{2^{35}}$
13	2^{33}	2^{61}	$3^{19} \approx 2^{30.1}$	$\mathbf{2^{44}}$
19	2^{42}	2^{69}	$3^{25} \approx 2^{39.6}$	2^{54}
24	2^{50}	2^{77}	$3^{30} \approx 2^{47.5}$	2^{62}

Table 4.2: *Complexity of our attack against POSEIDON, compared with the security claims given with the challenges.*

The original specification of POSEIDON states that interpolation attacks are expected to have a complexity similar to the one of our attacks, namely about $3^{\mathsf{RP}+\mathsf{RF}}$ as given in Equation (3) in [Gra+21]. However, the challenges of the Ethereum Foundation appear to claim a higher security level. Indeed, for these challenges, the claim was that an attack would require at least 2^{37+s} steps, where s is a security level specified in bits, and is equal to $8, 16, 34, 32$ and 40 when RP is equal to $3, 8, 13, 19$ and 24 respectively. While it is unclear which attack it corresponds to, we actually observe that this claim is close to $3^{3\mathsf{RF}+\mathsf{RP}}$. Overall, our practical attacks show that the authors claims are slightly cautious, ignoring some log factors.

In practice, we use `SageMath` [Sag22] to generate the polynomial, and we compute the roots either directly from `SageMath`, or with an external program using NTL [Sho].

4.2.3.2 *Rescue–Prime*

Rescue–Prime cannot be efficiently written as a univariate polynomial system, because it uses both the S-boxes $x \mapsto x^3$ and $x \mapsto x^{1/3}$. Each S-box has a low univariate degree in one direction, but a high degree in the other direction. Therefore, as previously explained, we add intermediate variables so that each S-box can be described with a low-degree equation, and we build a multivariate system.

More precisely, let us consider *Rescue–Prime* with a m-element state ($m=2$ or $m=3$) and R rounds. We use variables $(X_0, Y_0, \dots)$ to represent the input and $(X_i, Y_i, \dots)$ to represent the internal state after the i-th round ($m(R+1)$ variables in total). As shown in Figure 4.7, we can write m equations linking the m variables at the input and output of round i, using only the direct S-box $x \mapsto x^3$. Therefore, we have degree-3 equations:

$$\forall j \in \{0, \dots, m-1\},\ \mathcal{P}_{i,j}(X_i, Y_i, \dots) - \mathcal{Q}_{i,j}(X_{i+1}, Y_{i+1}, \dots) = 0\,.$$

If we add equations $X_0 = 0$ and $X_N = 0$, we obtain a system of polynomial equations representing the CICO problem. Using the trick of Section 4.2.1.1, we observe that the input variables can be removed, because we can directly write a degree-3 polynomial of $X_1, Y_1, \dots$ that must be equal to $S(X_0) = 0$. We can also remove X_N because it is fixed to zero, and we obtain a system of $m(R-1)+1$ equations and $mR-1$ variables.

With $m = 2$, we have the same number of equations and variables. However, with $m \geqslant 3$ we have more variables than equations, and we can use our trick to obtain a smaller system corresponding to a subset of the solutions with one solution on average. More precisely, with $m = 3$ branches and R rounds, we obtain a system of $3(R-1)$ degree-3 equations with the same number of variables. In our experiments, the system behaves like a generic system and has $\deg^u = 3^{3(R-1)}$ solutions in the algebraic closure of the field. Therefore, the complexity of solving the system is approximately:

$$\left(3^{3(R-1)}\right)^{\omega} \leqslant \left(3^{3(R-1)}\right)^{3} = 3^{9(R-1)} \,.$$

With $m = 2$ branches and R rounds, we obtain a system of $2R-1$ degree-3 equations with the same number of variables. Therefore, $\deg^u = 3^{2R-1}$ and the complexity of solving the system is approximately:

$$\left(3^{2R-1}\right)^{\omega} \leqslant \left(3^{2R-1}\right)^{3} = 3^{6R-3} \,.$$

We give explicit values for the proposed challenges in Table 4.3, where complexity figures in bold correspond to attacks that we have implemented in practice. As before, we used `SageMath` to generate our system of equations. However, we used `Magma` [BCP97] to find the solutions of the corresponding multivariate system.

R	m	Authors claims	Ethereum claims	$\deg^u$	Our complexity
4	3	2^{36}	$2^{37.5}$	$3^{9} \approx 2^{14.3}$	**2^{43}**
6	2	2^{40}	$2^{37.5}$	$3^{11} \approx 2^{17.4}$	2^{53}
7	2	2^{48}	$2^{43.5}$	$3^{13} \approx 2^{20.6}$	2^{62}
5	3	2^{48}	2^{45}	$3^{12} \approx 2^{19.0}$	2^{57}
8	2	2^{56}	$2^{49.5}$	$3^{15} \approx 2^{23.8}$	2^{72}

Table 4.3: *Complexity of our attack against Rescue–Prime, compared with the security claims given with the challenges.*

Note that in the original paper of *Rescue–Prime* [SAD20] the authors state that Gröbner basis attacks are expected to have the following complexity

$$\binom{(0.5(d-1)+1)m(R-1)+3}{m(R-1)+1}^{2} .$$

This complexity corresponds to the cost of F5 algorithm with a small value of $\omega = 2$ for the matrix multiplication exponent, while the complexity of our practical attacks is given by the cost of FGLM. Overall, our analysis shows that for the specific case of *Rescue–Prime* the FGLM step dominates F5 in time complexity, implying that the authors claims are also slightly cautious.

4.3 Importance of the choice of the modeling

In this section we emphasize the importance of the choice of the modeling when building the polynomial system. We present two distinct cases: Ciminion and `Anemoi`.

While we previously saw practical algebraic attacks, we now move to the designer's point of view. More precisely, we show that Ciminion has a much smaller security margin than anticipated by the designers, and the analysis we bring for `Anemoi` is the one allowing us to determine the number of rounds for the permutation in Chapter 3.

4.3.1 Ciminion

Ciminion [Dob+21] is an encryption scheme which uses a key of length k to encrypt a given plaintext. In this case, we are not investigating the complexity of the CICO problem, the goal is simply to recover the key (or some subkeys) with a time complexity lower than 2^k.

In the original paper, Dobraunig *et al.* proposed to study Gröbner basis attacks on a modified version of Ciminion, that they conjectured to be weaker than the real Ciminion by putting the key addition after the permutation p_E (see Figure 4.9). In the modified Ciminion, they came up with a system of 6 equations of degrees $\{2^{r-1}, 2^r, 2^r, 2^{r+1}, 2^{r+1}, 2^{r+2}\}$ over 6 variables, where r is the number of rounds of p_E.

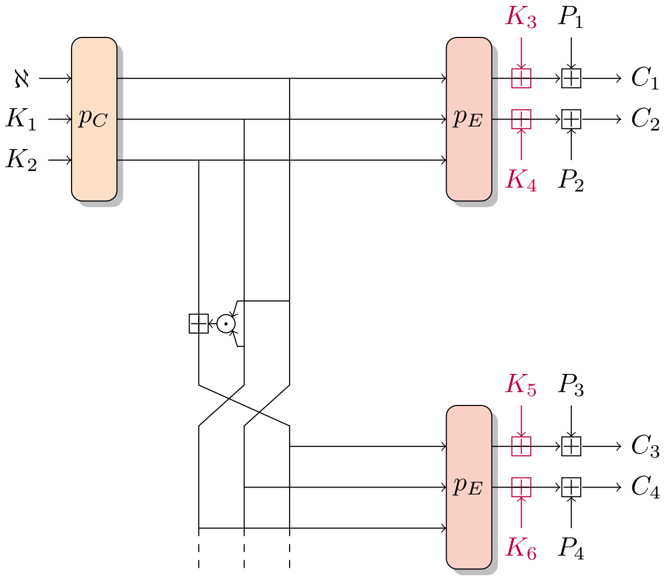


Figure 4.9: *Weaker version of Ciminion analyzed in [Dob+21].*

The value of r was chosen so that this attack has complexity at least 2^s. More precisely, the authors estimated the complexity of the F5 algorithm with parameters

$$n = 6\,,\ \text{and} \qquad D_{\text{reg}} = 21 \cdot 2^{r-1} - 5 \approx 2^{r+3.4}\,.$$

Following [BFS04], they estimated the complexity as

$$\binom{n + D_{\text{reg}}}{D_{\text{reg}}}^{\omega} \leqslant \left(\frac{(D_{\text{reg}} + n)^n}{n!}\right)^{\omega} \approx 2^{(6r+10.9)\omega}\,.$$

This estimation is actually an upper bound, and a sharper upper bound of

$$\mathcal{O}\left(nD_{\text{reg}} \times \binom{n + D_{\text{reg}} - 1}{D_{\text{reg}}}^{\omega}\right)$$

is given in [BFS15, Proposition 1] as mentioned in Section 4.1.1.2.

The designers took $\omega = 2$ as a lower bound, obtaining a minimum number of rounds $r \geqslant \lceil \frac{s-21.8}{12} \rceil$, and added 5 rounds as a security margin.

4.3.1.1 Our new modeling

Instead of looking at a system of equations resulting from a presumed weaker scheme, we study the original scheme and propose a better way to set up a system of equations. For a given nonce $\aleph$, we consider the first two output blocks. We denote $\alpha_i = C_i - P_i$ and $\alpha'_i = C'_i - P'_i$, for $i = 1 \dots 4$, and introduce two variables $X, Y \in \mathbb{F}_q$ for the missing output words (not given as part of the ciphertext) after the first and second permutations p_E, as depicted in Figure 4.10.

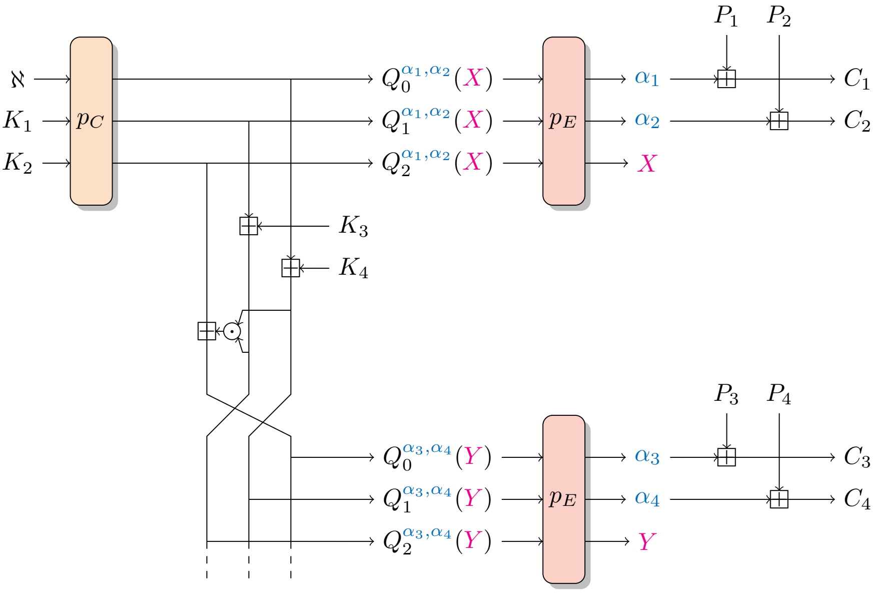

$\aleph$
K_1
K_2
p_C
$Q_0^{\alpha_1,\alpha_2}(X)$
$Q_1^{\alpha_1,\alpha_2}(X)$
$Q_2^{\alpha_1,\alpha_2}(X)$
p_E
α_1
α_2
X
P_1
P_2
C_1
C_2
K_3
K_4
$Q_0^{\alpha_3,\alpha_4}(Y)$
$Q_1^{\alpha_3,\alpha_4}(Y)$
$Q_2^{\alpha_3,\alpha_4}(Y)$
α_3
α_4
Y
P_3
P_4
C_3
C_4

Figure 4.10: *How to generate equations for Ciminion.*

The output of the first permutation p_E is (α_1, α_2, X), therefore, we can write the input as polynomials in X:

$$(Q_0^{\alpha_1,\alpha_2}(X), Q_1^{\alpha_1,\alpha_2}(X), Q_2^{\alpha_1,\alpha_2}(X)) = p_E^{-1}(\alpha_1, \alpha_2, X)\,.$$

Similarly, the output of the second permutation p_E is (α_3, α_4, Y), and we can write the corresponding input as polynomials in Y:

$$(Q_0^{\alpha_3,\alpha_4}(Y), Q_1^{\alpha_3,\alpha_4}(Y), Q_2^{\alpha_3,\alpha_4}(Y)) = p_E^{-1}(\alpha_3, \alpha_4, Y)\,.$$

Then, we write equations linking the input of the first two p_E through the rol function:

$$\begin{cases} Q_0^{\alpha_1,\alpha_2}(X) &= Q_1^{\alpha_3,\alpha_4}(Y) - K_4 \\ Q_1^{\alpha_1,\alpha_2}(X) &= Q_2^{\alpha_3,\alpha_4}(Y) - K_3 \\ Q_2^{\alpha_1,\alpha_2}(X) &= Q_0^{\alpha_3,\alpha_4}(Y) - Q_1^{\alpha_3,\alpha_4}(Y) \odot Q_2^{\alpha_3,\alpha_4}(Y) \end{cases}$$

Finally, we consider two ciphertexts, obtained from two different nonces, ℵ and ℵ′. We can then eliminate the keys K_3, K_4 and obtain a system of four equations in the four variables (X, Y, X', Y'), using two blocks of ciphertexts from each nonce:

$$\begin{cases} Q_0^{\alpha_1,\alpha_2}(X) - Q_0^{\alpha_1',\alpha_2'}(X') & = Q_1^{\alpha_3,\alpha_4}(Y) - Q_1^{\alpha_3',\alpha_4'}(Y') \\ Q_1^{\alpha_1,\alpha_2}(X) - Q_1^{\alpha_1',\alpha_2'}(X') & = Q_2^{\alpha_3,\alpha_4}(Y) - Q_2^{\alpha_3',\alpha_4'}(Y') \\ Q_2^{\alpha_1,\alpha_2}(X) & = Q_0^{\alpha_3,\alpha_4}(Y) - Q_1^{\alpha_3,\alpha_4}(Y)Q_2^{\alpha_3,\alpha_4}(Y) \\ Q_2^{\alpha_1',\alpha_2'}(X') & = Q_0^{\alpha_3',\alpha_4'}(Y') - Q_1^{\alpha_3',\alpha_4'}(Y')Q_2^{\alpha_3',\alpha_4'}(Y') \,. \end{cases} \tag{4.4}$$

Solving this system allows to recover the full internal state, and to deduce the keys K_1, K_2, K_3, K_4. In order to solve the system, we use the approach explained in Section 4.1.1.2.

4.3.1.2 Solving complexity.

Let us denote $\mathcal{P}_i$ the polynomial corresponding to the i-th row of the system, such that we have for all $i = 1 \dots 4$, $\mathcal{P}_i(X, X', Y, Y') = 0$, i.e. we have

$$\begin{cases} \mathcal{P}_1 & = Q_0^{\alpha_1,\alpha_2}(X) - Q_0^{\alpha_1',\alpha_2'}(X') - Q_1^{\alpha_3,\alpha_4}(Y) + Q_1^{\alpha_3',\alpha_4'}(Y') \\ \mathcal{P}_2 & = Q_1^{\alpha_1,\alpha_2}(X) - Q_1^{\alpha_1',\alpha_2'}(X') - Q_2^{\alpha_3,\alpha_4}(Y) + Q_2^{\alpha_3',\alpha_4'}(Y') \\ \mathcal{P}_3 & = Q_2^{\alpha_1,\alpha_2}(X) - Q_0^{\alpha_3,\alpha_4}(Y) + Q_1^{\alpha_3,\alpha_4}(Y)Q_2^{\alpha_3,\alpha_4}(Y) \\ \mathcal{P}_4 & = Q_2^{\alpha_1',\alpha_2'}(X') - Q_0^{\alpha_3',\alpha_4'}(Y') + Q_1^{\alpha_3',\alpha_4'}(Y')Q_2^{\alpha_3',\alpha_4'}(Y') \,. \end{cases}$$

We notice that $\mathcal{P}_i$ is a sum of univariate polynomials so that:

$$\mathcal{P}_i(X, X', Y, Y') = \mathcal{P}_i^X(X) + \mathcal{P}_i^{X'}(X') + \mathcal{P}_i^Y(Y) + \mathcal{P}_i^{Y'}(Y') \,.$$

Then, it is sufficient to determine $\max_j \deg^u(\mathcal{P}_i^j)$ for each $\mathcal{P}_i$. Given that

$$\begin{cases} \deg_X^u\left(Q_0^{\alpha_1,\alpha_2}\right) & = \deg_{X'}^u\left(Q_0^{\alpha_1',\alpha_2'}\right) = \deg_Y^u\left(Q_0^{\alpha_3,\alpha_4}\right) = \deg_{Y'}^u\left(Q_0^{\alpha_3',\alpha_4'}\right) = 2^{r-1} \\ \deg_X^u\left(Q_1^{\alpha_1,\alpha_2}\right) & = \deg_{X'}^u\left(Q_1^{\alpha_1',\alpha_2'}\right) = \deg_Y^u\left(Q_1^{\alpha_3,\alpha_4}\right) = \deg_{Y'}^u\left(Q_1^{\alpha_3',\alpha_4'}\right) = 2^{r-1} \\ \deg_X^u\left(Q_2^{\alpha_1,\alpha_2}\right) & = \deg_{X'}^u\left(Q_2^{\alpha_1',\alpha_2'}\right) = \deg_Y^u\left(Q_2^{\alpha_3,\alpha_4}\right) = \deg_{Y'}^u\left(Q_2^{\alpha_3',\alpha_4'}\right) = 2^r \,, \end{cases}$$

the degree of the polynomials $\mathcal{P}_i$ in X, X', Y and Y' are given in Table 4.4.

	X	X'	Y	Y'
$\mathcal{P}_1$	2^{r-1}	2^{r-1}	2^{r-1}	2^{r-1}
$\mathcal{P}_2$	2^{r-1}	2^{r-1}	2^r	2^r
$\mathcal{P}_3$	2^r	0	$3 \cdot 2^{r-1}$	0
$\mathcal{P}_4$	0	2^r	0	$3 \cdot 2^{r-1}$

Table 4.4: *Degree of polynomials $\mathcal{P}_i$.*

In particular, System (4.4) has two equations of degree $3 \cdot 2^{r-1}$, one of degree 2^r, and one of degree 2^{r-1}. Therefore, we have the following parameters:

$$\begin{cases} n & = 4 \\ D_{\text{reg}} & \leqslant 1 + \displaystyle\sum_{i=1}^{n}(d_i - 1) = 9 \cdot 2^{r-1} - 3 \leqslant 9 \cdot 2^{r-1} \approx 2^{r+2.2} \\ d & \leqslant \displaystyle\prod_{i=1}^{n} d_i = 9 \cdot 2^{4r-3} \approx 2^{4r+0.2} \,. \end{cases}$$

We can deduce upper bounds on the cost of the steps required to solve the system.

Computing a Gröbner basis with respect to the *grevlex* order using Faugère's F5 algorithm has asymptotic complexity

$$\begin{aligned} nD_{\text{reg}} \times \binom{n + D_{\text{reg}} - 1}{D_{\text{reg}}}^{\omega} &= 4 \times 2^{r+2.2} \times \binom{2^{r+2.2} + 3}{2^{r+2.2}}^{\omega} \\ &\leqslant 2^{r+4.2} \left(\frac{(2^{r+2.2} + 3)^3}{3!} \right)^{\omega} \\ &\approx 2^{r+4.2+(3r+4)\omega} \,. \end{aligned}$$

On the other hand, performing the change of order with a fast variant of FGLM has asymptotic complexity

$$d^{\omega} \approx 2^{(4r+0.2)\omega} \,.$$

FGLM is therefore the bottleneck.

From an attacker's point of view, we assume that linear algebra is implemented with Strassen's algorithm, resulting in $\omega = 2.807$. Taking the designer's recommended number of rounds $r = \lceil \frac{s+37}{12} \rceil$, this attack is slightly faster than 2^s for large values of s, with a time complexity

$$2^{(4r+0.2)\omega} = 2^{\left(4\lceil \frac{s+37}{12} \rceil + 0.2\right)\omega} \approx 2^{\frac{4\omega}{12}s+35.2} \approx 2^{0.94s+35.2} \,.$$

For practical values of s, the attack is not faster than 2^s. However, it shows that the design has a much smaller security margin than expected by the designers. In particular, using an optimistic value of $\omega = 2$ as in the designers' security analysis, we obtain an attack complexity of about $2^{112.4}$ for the designers' recommended 128-bit security with 14 rounds.

4.3.2 Anemoi

The aim of this section is to study the complexity of algebraic attacks to determine the number of rounds of Anemoi, introduced in Chapter 3. As we are investigating such attacks from a designer's point of view, we are mainly interested in a minimal condition on the number of rounds to reach a security of 2^s bits so that we allow ourselves to underestimate complexity of the attack in several places. In what follows we will focus on the following version of the CICO problem, stated for $\ell = 1$, where ℓ is the number of columns in the Anemoi internal state.

Definition 4.3 (Variant of Definition 4.2). Let $\mathsf{P} : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ be a permutation. The CICO problem consists in finding $(y_{\text{in}}, y_{\text{out}}) \in \mathbb{F}_q^2$ such that $\mathsf{P}(0, y_{\text{in}}) = (0, y_{\text{out}})$.

Let us note that in this section, we restrict ourselves to the case $\ell = 1$ to ease experiments. When $\ell > 1$, the number of equations and variables is expected to be naturally multiplied by ℓ.

In this thesis, we propose to discuss the results obtained for the complexity of algebraic attacks, and we leave the details of the proofs and the experiments in our paper [Bou+23].

4.3.2.1 Characteristic 2

In even characteristic, we derive the number of rounds from the following estimate.

Estimate 4.1. We estimate the cost of solving the CICO problem in even characteristic by one of the FGLM steps, which has complexity

$$\mathcal{O}(\ell n_r \cdot 9^{\omega \ell n_r}) \,,$$

where ω is the linear algebra exponent from the FGLM algorithm.

This estimate comes from the fact that, in such a case, the cost of the Gröbner basis computation is mostly independent from the number of rounds and that the cost of FGLM can be approximated by the one on a generic system containing $2\ell n_r$ cubic equations.

4.3.2.2 Odd characteristic.

In this section we will argue that the CICO problem behaves differently in odd characteristic, and more importantly that considering two types of modeling leads to different results.

First Modelling

The first modeling consists in introducing two equations and two variables at each round. Let $\mathbf{X_i}$ and $\mathbf{Y_i}$ be the input variables in each round i. As $\ell = 1$, we first add the constants and apply the PHT so that we have:

$$(X'_i, Y'_i) = \mathcal{P}(\mathbf{X_i} + c_i, \mathbf{Y_i} + d_i) \,.$$

Then the output variables are given after applying the open `Flystel` $\mathcal{H}$ as follows:

$$(\mathbf{X_{i+1}}, \mathbf{Y_{i+1}}) = \mathcal{H}(X'_i, Y'_i) \,.$$

Since the open and closed `Flystel` are CCZ-equivalent, this equality can also be written as

$$(X'_i, \mathbf{X_{i+1}}) = \mathcal{V}(Y'_i, \mathbf{Y_{i+1}}) \,,$$

where $\mathcal{V}$ is the closed `Flystel` which only relies on low degree functions. This implies that

$$\begin{cases} X'_i & = (Y'_i - \mathbf{Y_{i+1}})^d + Q_\gamma(Y'_i) \\ \mathbf{X_{i+1}} & = (Y'_i - \mathbf{Y_{i+1}})^d + Q_\delta(\mathbf{Y_{i+1}}) \,. \end{cases}$$

We depict on Figure 4.11a the way we build equations in each round.

Then, let us consider the following system:

$$(\mathcal{S}_1) : \begin{cases} \forall\, i,\ 0 \leqslant i \leqslant n_r - 1 \\ \mathscr{F}_i = (Y'_i - \mathbf{Y_{i+1}})^d + Q_\gamma(Y'_i) - X'_i = 0 \\ \mathscr{G}_i = (Y'_i - \mathbf{Y_{i+1}})^d + Q_\delta(\mathbf{Y_{i+1}}) - \mathbf{X_{i+1}} = 0 \end{cases}$$

The CICO system is then described by $(\mathcal{S}_1)$ by fixing the variables $X_0 = 0$ and $X_{n_r} = 0$. Let us notice that this system contains $2n_r$ equations in the $2n_r$ variables $X_0, \ldots, Y_{n_r}, Y_0, \ldots Y_{n_r}$ when $\ell = 1$ and $2\ell n_r$ in the general case.

Second Modelling

Let us now describe a second modeling.[1] As in the first modeling we let

$$(X_i', Y_i') = \mathcal{P}(X_i + c_i, Y_i + d_i)\ .$$

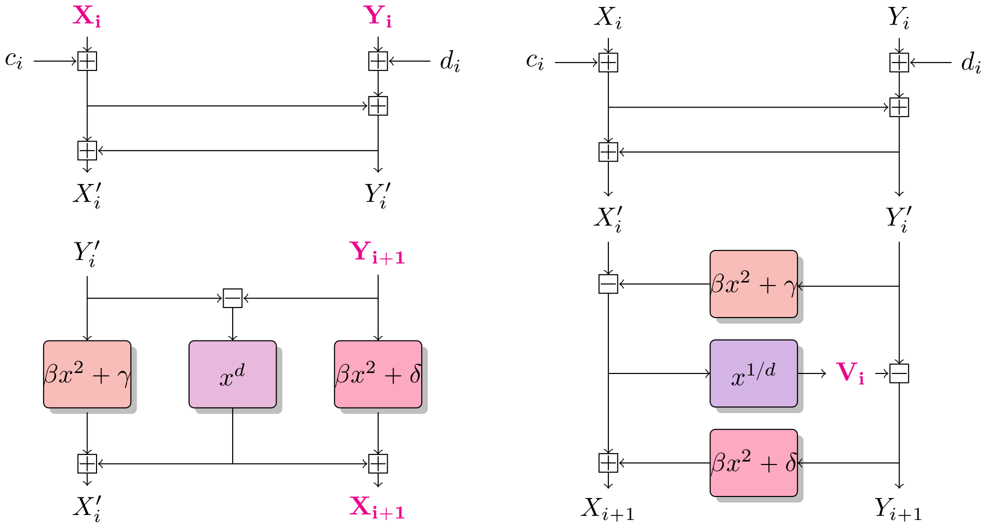
Then, we introduce a new variable $\mathbf{V_i}$ such that

$$\mathbf{V_i} = Y_i' - Y_{i+1}\ ,$$

the idea being to have only one variable and only one equation per round. It also holds that

$$X_{i+1} = X_i' - \beta Y_i'^2 - \gamma + \beta Y_{i+1}^2 + \delta\ .$$

This modeling is described in Figure 4.11b.



(a) *First modeling.*

(b) *Second Modeling.*

Figure 4.11: *Modeling of one round of* Anemoi *when* $\ell = 1$.

Let us consider the following system:

$$(\mathcal{S}_2) : \begin{cases} \forall\, i,\ 0 \leqslant i \leqslant n_r - 1 \\ \mathscr{P}_i = \mathbf{V_i}^d - (X_i' - (\beta Y_i'^2 + \gamma)) = 0\ . \end{cases}$$

We note that the system contains n_r equations in the $n_r + 2$ variables $X_0, Y_0, V_0, \ldots, V_{n_r-1}$. The CICO system is then obtained from $(\mathcal{S}_2)$ by fixing the variable $X_0 = 0$ and by adding the equation in $X_0, Y_0, V_0, \ldots, V_{n_r-1}$ which corresponds to the constraint $X_{n_r} = 0$ and which is not a linear equation anymore. This second modeling then contains half as much equations and variables than the first one.

More importantly, while we could expect the degree of the $\mathscr{P}_i$'s to increase exponentially, it only increases linearly with the number of rounds. In Figure 4.12 we show the time complexity for

[1] This modeling was originally found by a reviewer for Eurocrypt 2023.

solving the CICO problem on reduced versions of `Anemoi` for $d \in \{3, 5, 7\}$ and for prime field of size p, where p is around 16 bits. We observe that the second modeling is indeed faster to solve. The graph also highlights that the higher the exponent d is, the hardest it is to run experiments and then to deduce bounds for the complexity of solving the CICO problem for `Anemoi`.

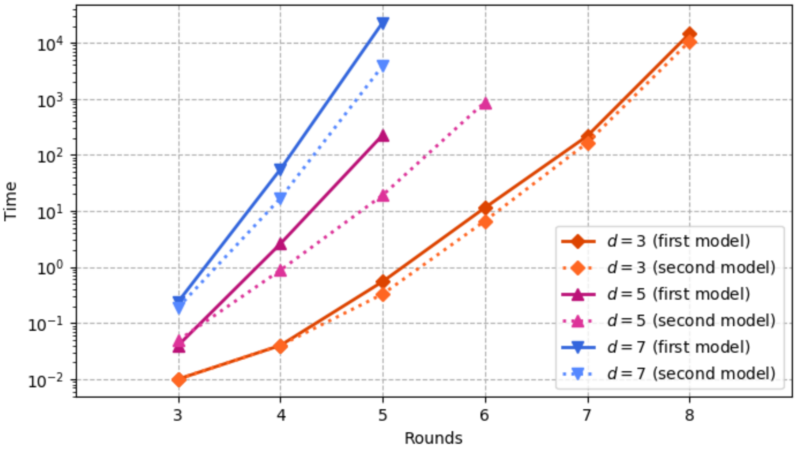


Figure 4.12: Comparison of both modeling for different instances of `Anemoi`.

4.3.2.3 Choosing the number of rounds

In odd characteristic, the dominant cost corresponds to the Gröbner basis computation. Let d_{exp} be the experimental solving degree of solving the CICO problem with the first modeling. In the following conjecture, we derive d_{exp} from experiments for $\ell = 1$.

Conjecture 4.1. *We have*

$$d_{exp} \geqslant 2n_r + \kappa_d \ ,$$

where κ_d is a constant depending only on d. We found $\kappa_3 = 1$, $\kappa_5 = 2$, $\kappa_7 = 4$, $\kappa_9 = 7$ and $\kappa_d = 9$ for $d = 11$.

We would expect the value of κ_d to keep increasing with d but the computations needed to estimate it become too costly as d increases. We then derive the number of rounds for `Anemoi` from the following estimate. Note that we did not consider the cost of FGLM since it appears to be negligible compared to this estimate.

Estimate 4.2. In odd characteristic, we estimate the cost of solving the CICO problem with the first modeling for $\ell = 1$ by

$$\mathcal{O}\left(\binom{d_{\text{exp}} + 2n_r}{2n_r}^{\omega}\right) \ ,$$

where d_{exp} is given in Conjecture 4.1 and where ω is the matrix multiplication exponent, as defined in Section 4.1.1.2.

The second modeling seems to take advantage of the special features of our design, but does not seem to improve the time complexity of the first one, at least asymptotically. Nevertheless, we add 2 extra rounds to Estimate 4.2 to ensure that these equations will not compromise security if exploited in a more sophisticated way.

We also generalize Conjecture 4.1 and Estimate 4.2 to $\ell > 1$ by replacing $2n_r$ by $2\ell n_r$ everywhere.

Conclusion

In this chapter we have investigated the security of some Arithmetization-Oriented primitives against algebraic attacks. Such attacks are often used to determine the number of rounds of these new primitives because of their low-degree polynomial modelisation, hence the need to better understand them. The analysis we proposed was first motivated by the challenges proposed by the Ethereum Foundation. Although we have not broken the claims of the authors of Feistel–MiMC, Poseidon or *Rescue–Prime*, our practical attacks contribute to a better understanding of the behaviour of algebraic systems.

Beyond our exploration of algebraic attacks, we also present valuable suggestions for future designs. First, we emphasized the need to build univariate models instead of multivariate models whenever it is possible, since they are easier to solve. We also propose tricks to bypass rounds for SPN constructions and others. For Poseidon we can indeed save two rounds when building the polynomial system to solve the CICO problem, while we save one round for *Rescue–Prime*.

Finally, we have also highlighted the importance of careful modeling choices, trying as many variants of encoding as possible when designing a primitive. In particular, by considering a different modeling than the one proposed by the designer of Ciminion, we have shown that the primitive has a much smaller security margin than expected by the designers. Moreover, when investigating the number of rounds needed to build a secure `Anemoi` permutation, we have also shown the importance of studying different modelings.

Chapter 5

Univariate polynomial representation and algebraic degree of MiMC

In this chapter we study univariate polynomial representations when iterating power functions. In particular, we focus on the MiMC block cipher [Alb+16], which consists of many iterations of a simple round function: the addition of a key and round constants, and a low-degree power permutation of $\mathbb{F}_{2^n}$, where $n \approx 129$. This analysis also leads to an upper bound on the algebraic degree of the cipher. In the next chapter, we will study the security of MiMC against higher-order differential attacks, for which the complexity increases with the algebraic degree. Therefore, we need to better understand how quantity behaves while iterating a round function.

In Section 5.1 we first fix some definitions and notation to explain how to quantify the algebraic degree using univariate polynomials. In Section 5.2 we show that when iterating power functions, some exponents are missing in the univariate polynomial. Such an analysis allows us to define upper bounds on the algebraic degree of the encryption for various instances of MiMC in Section 5.3. Finally, in Section 5.4, we investigate the algebraic degree of the inverse transformation.

The results presented in this chapter and in Chapter 6 on the algebraic degree of MiMC_3 and MiMC_3^{-1} have been obtained with Anne Canteaut and Léo Perrin, and published in the journal *Designs, Codes and Cryptography* in 2023 [BCP23]. The generalization of the results to other instances of MiMC_d has been presented at the conference *Finite Fields and their Applications* in June 2023 [Bou23] and a paper is currently in progress.

Contents

5.1 Quantifying the algebraic degree

While the most common studied case of MiMC is the instance using the cube as a round function, which is also the one we study in [BCP23], in this chapter our aim is to generalize the study to other instances of MiMC. The main propositions of this chapter for the bounds on the algebraic degree are summarized in Table 5.1.

d	Corresponding proposition	Approach used
$2^j + 1, j > 1$	Proposition 5.8	Missing exponents (Proposition 5.5)
$2^j - 1, j > 1$	Proposition 5.11	Missing exponents (Proposition 5.7)
3^{-1}	Corollary 5.5	Influence of the encryption degree

Table 5.1: *Corresponding proposition for the bound on the degree, for various instances of* MiMC_d.

In this section, we first propose an inductive procedure to determine the set of all exponents that can appear in the univariate form of the polynomial describing r rounds of MiMC_d. This process is summarized in Proposition 5.1, and we then describe some direct consequences for the algebraic degree.

5.1.1 Generating exponents

We recall that MiMC corresponds to the composition $F_{r-1} \circ \ldots \circ F_0$ where

$$\forall i,\ 0 \leqslant i < r,\ \ F_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ x \mapsto x^d \oplus c_{i+1}\ ,$$

with d coprime with $(2^n - 1)$ and the $c_{i+1} \in \mathbb{F}_{2^n}$ are arbitrary constants. It is worth noting that the key is omitted in this description: indeed, as far as the algebraic degree is concerned, it can be considered to be part of the round constants. As a consequence, the round function of a MiMC instance is fully specified by the exponent d and by the sequence c of all round constants, and we denote such a MiMC instance $\mathsf{MiMC}_{d,c}[r]$.

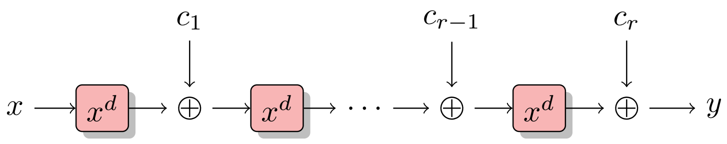


Figure 5.1: $\mathsf{MiMC}_{d,c}$ *with* r *rounds.*

We will also denote by $(B_d^r)_{r\geqslant 1}$ the sequence of the maximal algebraic degrees of r rounds of MiMC_d, i.e., for any $r \geqslant 1$, B_d^r is the degree of $\mathsf{MiMC}_{d,c}[r]$ for at least one sequence $c = (c_1, \ldots, c_r)$ of constants:

$$B_d^r := \max_c \deg^a \mathsf{MiMC}_{d,c}[r]\ .$$

Note that, without loss of generality, we can assume that $c_r = 0$. Our goal is then to find the exact value of B_d^r. Indeed, a (very expensive) attack on MiMC_3 has been exhibited in [Eic+20], exploiting the fact that the number of rounds proposed by the designers is not sufficient to achieve a maximal algebraic degree. However, this weakness is based on a simple upper-bound on B_d^r and any gap between this bound and the exact value of the degree would decrease the complexity of the attack (or increase the number of rounds covered for a given complexity). Our aim is therefore to determine the exact value of B_d^r, or equivalently the minimal complexity of any attack based on higher-order differentials such as those in [Eic+20].

We first introduce some definitions and notations that will be extensively used in this chapter.

Definition 5.1 (Covering)**.** Let x and y be two elements in $\mathbb{F}_2^n$. Then, we say that y *is covered by* x and we write $y \preceq x$ if $y_i \leqslant x_i$ for all i.

Similarly, if i and j are two integers, then $j \preceq i$ means that the 2-adic expansion of j is covered by the 2-adic expansion of i.

We will denote by $\mathcal{E}_{d,r}$ the set of exponents of the monomials appearing in the univariate polynomial $\mathsf{MiMC}_{d,c}[r]$ over $\mathbb{F}_{2^n}$ for at least one sequence c.

Proposition 5.1. *Let n and $d < 2^n - 1$ be two integers such that $\gcd(d, 2^n - 1) = 1$. Then, we have:*

$$\mathcal{E}_{d,r} = \{dj \bmod (2^n - 1) \textit{ where } j \preceq i,\ i \in \mathcal{E}_{d,r-1}\} .$$

Proof. Let $c = (c_2, \ldots, c_r)$ be a sequence of constants and suppose that the univariate form of $\mathsf{MiMC}_{d,c}[r-1]$ is given by

$$\mathcal{P}_{r-1}(x) = \sum_{i \in \mathcal{E}_{d,r-1}} \alpha_i x^i .$$

Then, if $\hat{c} = (c_1, c_2 \ldots, c_r)$, the univariate form of $\mathsf{MiMC}_{d,\hat{c}}[r]$ is

$$\mathcal{P}_r(x) = \mathcal{P}_{r-1}(x^d + c_1) = \sum_{i \in \mathcal{E}_{d,r-1}} \alpha_i (x^d + c_1)^i .$$

Let I_i denote the support of the 2-adic expansion of some exponent i: $I_i = Supp(i)$. Then, we have

$$(x^d + c_1)^i = \prod_{\ell \in I_i} (x^d + c_1)^{2^\ell} = \prod_{\ell \in I_i} (x^{d2^\ell} + c_1^{2^\ell}) .$$

It follows that after expansion of the product, the terms appearing in the polynomial $\mathcal{P}_r$ have the following form:

$$\alpha_i \left(c_1^{\sum_{\ell \in I_i \setminus J_i} 2^\ell} \right) \left(x^{d \sum_{\ell \in J_i} 2^\ell} \right) \quad \text{where} \quad J_i \subseteq I_i .$$

As a consequence, the monomials that may appear in $\mathcal{P}_r$ are of the form $x^{dj \bmod (2^n-1)}$ with $j \preceq i$. The coefficient of such a monomial is then equal to

$$p_j = \sum_{i \in E_j} \alpha_i c_1^{j \oplus i} \text{ where } E_j = \{i \in \mathcal{E}_{d,r-1} : j \preceq i\} .$$

By definition of the set $\mathcal{E}_{d,r-1}$, there exists at least one sequence of constants c such that $\alpha_i \neq 0$ for some exponent i in E_j. Then, p_j is a nonzero polynomial in c_1 and cannot vanish for all $c_1 \in \mathbb{F}_{2^n}$. This implies that $x^{dj \bmod (2^n-1)}$ appears in $\mathcal{P}_r$ for at least one sequence of constants $\hat{c} = (c_1, c)$. It directly follows that the set of all exponents appearing in the univariate polynomial $\mathsf{MiMC}_{d,c}[r]$ is:

$$\mathcal{E}_{d,r} = \{(dj) \bmod (2^n - 1) \text{ where } j \preceq i, i \in \mathcal{E}_{d,r-1}\} .$$

□

Recalling that the algebraic degree of a transformation is given by the maximum of the Hamming weights of the exponents appearing in the univariate polynomial describing the transformation, we deduce that the maximum algebraic degree after r rounds, B_d^r, is the maximal weight of the elements in $\mathcal{E}_{d,r}$.

5.1.2 Algorithmic point of view

In this section, we propose another vision of Proposition 5.1 based on an algorithmic procedure. First, let us notice that after one round of encryption, we always have $\mathcal{E}_{d,1} = \{0, d\}$. Then, we can apply recursively Proposition 5.1 to construct $\mathcal{E}_{d,r}$ from $\mathcal{E}_{d,r-1}$. In practice, this process relies on two operations defined for any set of integers.

Mult$_d$ multiplies each element of the input set by d modulo $(2^n - 1)$:

$$\mathsf{Mult}_d : \begin{cases} \mathbb{N}^{\mathbb{N}} & \to \mathbb{N}^{\mathbb{N}} \\ \{j_0, \ldots, j_{\ell-1}\} & \mapsto \{(dj_0) \bmod (2^n-1), \ldots, (dj_{\ell-1}) \bmod (2^n-1)\} \end{cases},$$

Cover returns the set of all elements covered by elements in the input:

$$\mathsf{Cover} : \begin{cases} \mathbb{N}^{\mathbb{N}} & \to \mathbb{N}^{\mathbb{N}} \\ \{j_0, \ldots, j_{\ell-1}\} & \mapsto \{k \preceq j_i, i \in \{0, \ldots, \ell-1\}\} \end{cases}.$$

Using these two operations, we can re-write Proposition 5.1 as follows:

Corollary 5.1. *Let n and $d < 2^n - 1$ be two integers such that $\gcd(d, 2^n - 1) = 1$. We have*

$$\mathcal{E}_{d,r} = \mathsf{Mult}_d\big(\mathsf{Cover}(\mathcal{E}_{d,r-1})\big).$$

We observe that only Mult$_d$ depends on the exponent of the round function, and that the cardinality of its output is the same as the cardinality of the input, whereas for Cover, the cardinality of the output is usually higher than the cardinality of the input. This process can be seen as a tree, summarized in Figure 5.2, where each element in $\mathcal{E}_{d,r}$ can be seen like a child of an element $j \in \mathcal{E}_{d,r-1}$ after applying Mult$_d \circ$ Cover. We note that while each element in $\mathcal{E}_{d,r}$ has at least one parent in $\mathcal{E}_{d,r-1}$, this parent might not be unique.

Lemma 5.1. *Let $\mathcal{E}$ be any set of integers*

(i) *For any integers d_1, d_2*

$$\mathsf{Mult}_{d_2}\left(\mathsf{Mult}_{d_1}(\mathcal{E})\right) = \mathsf{Mult}_{d_1}\left(\mathsf{Mult}_{d_2}(\mathcal{E})\right) = \mathsf{Mult}_{d_1 d_2}(\mathcal{E}).$$

(ii) *The input of the* Cover *operation is contained in its output:*

$$\mathcal{E} \subseteq \mathsf{Cover}(\mathcal{E}).$$

(iii) *For any $\ell \geqslant 1$*

$$\mathsf{Mult}_{d^\ell}(\mathcal{E}_{d,r-\ell}) \subseteq \mathcal{E}_{d,r}.$$

(iv) *The operations* Mult$_2$ *and* Cover *commute:*

$$\mathsf{Mult}_2\left(\mathsf{Cover}(\mathcal{E})\right) = \mathsf{Cover}\left(\mathsf{Mult}_2(\mathcal{E})\right).$$

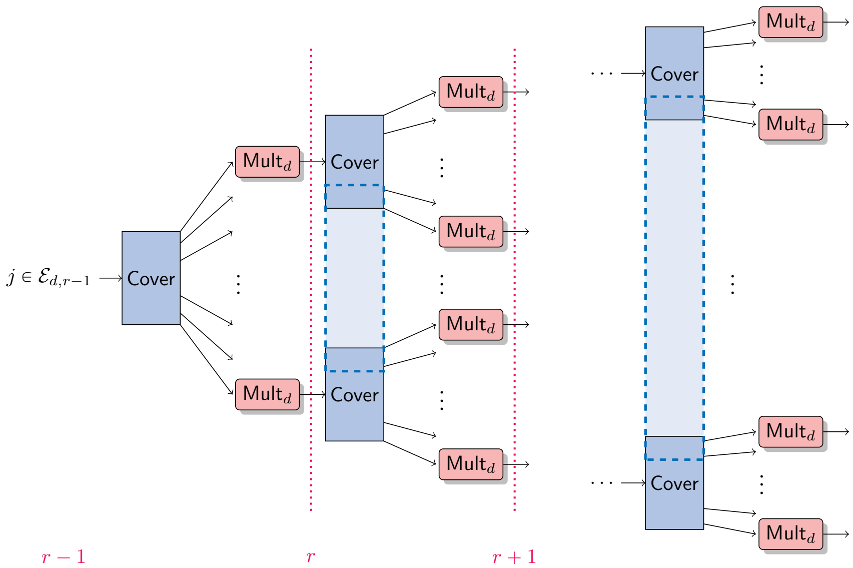


Figure 5.2: Getting next-round exponents.

Proof. We let $\mathcal{E} = \{e_i\}_{i \geqslant 0}$.

(i) The result trivially comes from the commutativity of the multiplication. We have

$$\mathsf{Mult}_{d_2}\left(\mathsf{Mult}_{d_1}(\mathcal{E})\right) = \mathsf{Mult}_{d_2}\left(\{d_1 e_i \bmod (2^n-1)\}\right) = \{d_2 d_1 e_i \bmod (2^n-1)\},$$

implying that

$$\mathsf{Mult}_{d_2}\left(\mathsf{Mult}_{d_1}(\mathcal{E})\right) = \mathsf{Mult}_{d_2 d_1}(\mathcal{E}) = \mathsf{Mult}_{d_1 d_2}(\mathcal{E}) = \mathsf{Mult}_{d_1}\left(\mathsf{Mult}_{d_2}(\mathcal{E})\right).$$

(ii) First let us observe that any integer is covered by itself, i.e.for any e_i, we have $e_i \preceq e_i$. It then directly follows that

$$\mathcal{E} = \{e_i\}_{i\geqslant 0} \subseteq \{k, k \preceq e_i\}_{i \geqslant 0} = \mathsf{Cover}(\mathcal{E}).$$

(iii) We show this by induction on ℓ. First, the property is satisfied for $\ell = 1$ since $\mathcal{E}_{d,r-1} \subseteq \mathsf{Cover}(\mathcal{E}_{d,r-1})$ from **(ii)**, then using Corollary 5.1 we have:

$$\mathsf{Mult}_d(\mathcal{E}_{d,r-1}) \subseteq \mathsf{Mult}_d\left(\mathsf{Cover}(\mathcal{E}_{d,r-1})\right) = \mathcal{E}_{d,r}.$$

Now, let us now assume that the property holds for ℓ, then we have:

$$\begin{aligned}
\mathsf{Mult}_{d^{\ell+1}}(\mathcal{E}_{d,r-\ell-1}) &= \mathsf{Mult}_{d^\ell}(\mathsf{Mult}_d(\mathcal{E}_{d,r-\ell-1})) && \text{by (i)},\\
&\subseteq \mathsf{Mult}_{d^\ell}(\mathsf{Mult}_d(\mathsf{Cover}(\mathcal{E}_{d,r-\ell-1}))) && \text{by (ii)},\\
&\subseteq \mathsf{Mult}_{d^\ell}(\mathcal{E}_{d,r-\ell}) && \text{by Corollary 5.1},\\
&\subseteq \mathcal{E}_{d,r} && \text{by induction hypothesis},
\end{aligned}$$

(iv) Let us notice that

$$\mathsf{Cover}(\mathcal{E}) = \{k, k \preceq e_i\}_{i \geqslant 0} = \left\{ k, k = \sum_{\ell \in \mathsf{Supp}(e_i)} 2^{\ell} \right\} ,$$

and that

$$\left\{ 2k, k = \sum_{\ell \in \mathsf{Supp}(e_i)} 2^{\ell} \right\} = \left\{ k, k = \sum_{\ell \in \mathsf{Supp}(e_i)} 2^{\ell+1} \right\} = \left\{ k, k = \sum_{\ell \in \mathsf{Supp}(2e_i)} 2^{\ell} \right\} .$$

As a consequence

$$\mathsf{Mult}_2 \left(\mathsf{Cover}(\mathcal{E})\right) = \mathsf{Cover}\left(\mathsf{Mult}_2(\mathcal{E})\right) .$$

□

From Corollary 5.1 and Lemma 5.1 we can then deduce that the maximal algebraic degree never decreases when the number of rounds increases.

Proposition 5.2. *For any integer d, $(B_d^r)_{r \geqslant 1}$ is a non-decreasing sequence:*

$$B_d^r \geqslant B_d^{r-1}, \ \forall r \geqslant 2 .$$

Moreover, when d is odd, we have

$$\mathcal{E}_{d,r-1} \subseteq \mathcal{E}_{d,r}, \ \forall r \geqslant 1 .$$

Proof. Let $d = \sum_{i=0}^{\mathrm{wt}(d)-1} 2^{\ell_i}$, be the binary expansion of d with $0 \leqslant \ell_0 < \ldots < \ell_{\mathrm{wt}(d)-1}$. We will first prove by induction on r, that $\mathsf{Mult}_{2^{\ell_0}}(\mathcal{E}_{d,r-1}) \subseteq \mathcal{E}_{d,r}$.

- **For $r = 2$:** it holds since $\mathcal{E}_{d,1} = \{0, d\}$, so $\mathsf{Mult}_{2^{\ell_0}}(\mathcal{E}_{d,1}) = \{0, 2^{\ell_0} d\}$. In particular, $2^{\ell_0} \in \mathsf{Cover}(\mathcal{E}_{d,1})$ so that:

$$\mathsf{Mult}_{2^{\ell_0}}(\mathcal{E}_{d,1}) = \mathsf{Mult}_d(\mathsf{Cover}(\{0, 2^{\ell_0}\})) \subseteq \mathsf{Mult}_d(\mathsf{Cover}(\mathcal{E}_{d,1})) = \mathcal{E}_{d,2} .$$

- **Induction step.** Let us assume that the property holds for $\mathcal{E}_{d,r}$.

$$\begin{aligned}
\mathsf{Mult}_{2^{\ell_0}}(\mathcal{E}_{d,r}) &= \mathsf{Mult}_{2^{\ell_0}}(\mathsf{Mult}_d(\mathsf{Cover}(\mathcal{E}_{d,r-1}))) && \text{by Corollary 5.1,}\\
&\subseteq \mathsf{Mult}_d(\mathsf{Mult}_{2^{\ell_0}}(\mathsf{Cover}(\mathcal{E}_{d,r-1}))) && \text{by Lemma 5.1 (i),}\\
&\subseteq \mathsf{Mult}_d(\mathsf{Cover}(\mathsf{Mult}_{2^{\ell_0}}(\mathcal{E}_{d,r-1}))) && \text{by Lemma 5.1 (iv),}\\
&\subseteq \mathsf{Mult}_d(\mathsf{Cover}(\mathcal{E}_{d,r})) && \text{by induction hypothesis,}\\
&= \mathcal{E}_{d,r+1} && \text{by Corollary 5.1.}
\end{aligned}$$

Finally, the result follows by observing that

$$\mathrm{wt}(2^{\ell_0} i \bmod (2^n - 1)) = \mathrm{wt}(i) .$$

Indeed we have

$$\begin{aligned}
B_d^r &= \max\{\mathrm{wt}(i), i \in \mathcal{E}_{d,r}\}\\
&\geqslant \max\{\mathrm{wt}(i), i \in \mathsf{Mult}_{2^{\ell_0}}(\mathcal{E}_{d,r-1})\}\\
&\geqslant \max\{\mathrm{wt}(i), i \in \mathcal{E}_{d,r-1}\}\\
&\geqslant B_d^{r-1} .
\end{aligned}$$

In particular, if d is odd, $\ell_0 = 0$, which implies that $\mathcal{E}_{d,r-1} = \mathsf{Mult}_{2^{\ell_0}}(\mathcal{E}_{d,r-1}) \subseteq \mathcal{E}_{d,r}$. □

Our main goal is then to estimate the algebraic degree of multiple iterations of MiMC_d. As a consequence, our focus is on the Hamming weight of the exponents. Because of Lemma 5.1 **(iv)**, we can reduce the size of $\mathcal{E}_{d,r}$ at each iteration by keeping only one representative per cyclotomic class. In other words, if $2^i x$ appears in $\mathcal{E}_{d,r}$, we can replace it by x without loosing information about the algebraic degree of the block cipher. More interestingly, if x is already in $\mathcal{E}_{d,r}$, it means that we can simply remove $2^i x$ from it. In practice, this significantly simplifies the computations.

5.1.3 Some Simple Applications

In this section, we propose some simple applications of the properties we have seen so far. A pattern of particular interest is what we call a *plateau*. To understand what it corresponds to, let us first consider a simple example with the cube as the iterated power function. For any input x, the output of the composition of the first two rounds is

$$(x^3 + c_1)^3 + c_2 = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3 + c_2 \,. \tag{5.1}$$

Note that it is also possible to use Proposition 5.1 for $d = 3$ to determine the exponents in the univariate representation of two rounds of MiMC. Using that $\mathcal{E}_{3,1} = \{0, 3\}$, we have:

$$\mathcal{E}_{3,2} \;=\; \mathsf{Mult}_3\left(\mathsf{Cover}(\{0,3\})\right) \;=\; \mathsf{Mult}_3\left(\{0,1,2,3\}\right) \;=\; \{0,3,6,9\}\,.$$

We deduce that the composition of these two rounds is quadratic as its algebraic degree is equal to $\max\{\mathrm{wt}(i),\ i \in \{0,3,6,9\}\}$, which is equal to 2. It is counter-intuitive: we would expect the algebraic degree to increase when a non-affine function is iterated. The algebraic degree that stays constant between two rounds is precisely what we call a *plateau*. It may happen that a plateau covers more than two rounds, as for the last rounds of the inverse transformation (see Section 5.4).

Definition 5.2 (Plateau)**.** We say that there is a *plateau* for the algebraic degree of MiMC_d between rounds r and $r + i$ whenever:

$$B_d^{r+i'} = B_d^r,\ \forall\, i' = 1, \ldots, i\,.$$

Since $(B_d^r)_{r\geqslant 1}$ is a non-decreasing sequence, the existence and the frequency of plateaus are the most relevant elements when estimating the degree of MiMC_d after a large number of rounds.

First of all, we can prove that there will always be such a plateau between the first and second rounds for all d of the form $d = 2^k - 1$ for some k.

Proposition 5.3. *Let $F : x \mapsto x^d$ be a permutation of $\mathbb{F}_{2^n}$ where $d = 2^k - 1$, and $\gcd(k, n) = 1$. Then, if $d^2 < 2^n - 1$, we have:*

$$\deg^a(F(F(x) + c)) = \deg^a(F)\,,$$

where c is an arbitrary constant.

Proof. Since $d = 2^k - 1$, it holds that $\mathsf{Cover}(\{d\}) = \{0, 1, \ldots, d\}$. It follows that

$$\mathcal{E}_{d,2} = \mathsf{Mult}_d(\mathsf{Cover}(\mathcal{E}_{d,1})) = \mathsf{Mult}_d(\mathsf{Cover}(\{0,d\})) = \mathsf{Mult}_d(\{0,1,\ldots,d\})\,,$$

so that we get

$$\deg^a((x^d + c)^d) = \max\{\mathrm{wt}(e), e \in \mathcal{E}_{d,2}\} = \max\{\mathrm{wt}(dj), j \in \{0,1,\ldots,d\}\}\,.$$

In order to prove that $\deg^a((x^d+c)^d) = \deg^a(F)$, it is then sufficient to show that $\mathrm{wt}(dj) = \mathrm{wt}(d) = k$ for any integer $1 \leqslant j \leqslant d$. Suppose that $j \in \{0, ..., d\}$ is such that $j = \sum_{\ell=0}^{k-1} \varepsilon_\ell 2^\ell$, where $\varepsilon_\ell \in \{0,1\}$ for all ℓ. We can thus write:

$$dj = (2^k - 1)\sum_{\ell=0}^{k-1} \varepsilon_\ell 2^\ell = \sum_{\ell=0}^{k-1} \varepsilon_\ell 2^{k+\ell} - \sum_{\ell=0}^{k-1} \varepsilon_\ell 2^\ell .$$

Using that $d = \sum_{\ell=0}^{k-1} 2^\ell$, we can write

$$d - \sum_{\ell=0}^{k-1} \varepsilon_\ell 2^\ell = \sum_{\ell=0}^{k-1} (1-\varepsilon_\ell) 2^\ell .$$

Let $j' = j+1$. Then we have:

$$j'd = (j+1)d = \sum_{\ell=0}^{k-1} \varepsilon_\ell 2^{k+\ell} + d - \sum_{\ell=0}^{k-1} \varepsilon_\ell 2^\ell = \sum_{\ell=0}^{k-1} \varepsilon_\ell 2^{k+\ell} + \sum_{\ell=0}^{k-1} (1-\varepsilon_\ell) 2^\ell ,$$

where

$$\mathrm{wt}\left(\sum_{\ell=0}^{k-1} \varepsilon_\ell 2^{k+\ell}\right) = \mathrm{wt}\left(\sum_{\ell=0}^{k-1} \varepsilon_\ell 2^{\ell}\right) = \mathrm{wt}(j) \quad \text{and} \quad \mathrm{wt}\left(\sum_{\ell=0}^{k-1} (1-\varepsilon_\ell) 2^{\ell}\right) = k - \mathrm{wt}(j) .$$

As a consequence, the Hamming weight of dj' for any $j' \in \{1, ..., d\}$ is equal to k.

□

Let us come back to the particular case $d = 3$. We can observe another plateau during the first four rounds of MiMC$_3$. Indeed, by using Proposition 5.1 again, we can easily construct the sets $\mathcal{E}_{3,3}$ and $\mathcal{E}_{3,4}$ to determine the degree at rounds 3 and 4 of MiMC$_3$. First, let us observe that:

$$\begin{aligned}\mathcal{E}_{3,3} &= \mathsf{Mult}_3\left(\mathsf{Cover}(\mathcal{E}_{3,2})\right)\\ &= \{0,3,6,9,12,18,24,27\} ,\end{aligned}$$

implying that the algebraic degree at the third round is $\mathrm{wt}(27) = 4$. Then, using that

$$\mathcal{E}_{3,4} = \mathsf{Mult}_3\left(\mathsf{Cover}(\mathcal{E}_{3,3})\right) ,$$

we deduce that the maximum-weight exponents in $\mathcal{E}_{3,4}$ are

$$\{27,30,51,54,57,75,78\} ,$$

so that the algebraic degree is also 4 after the fourth round.

Therefore, there are two plateaus in the growth of the degree during the first four rounds of MiMC$_3$. So a natural question is then whether there are other plateaus in the following rounds, and if so, how often they appear. Thanks to Proposition 5.1 we can construct the exponents appearing at each round using those of the previous round. A simple C implementation of this procedure allowed us to determine the algebraic degree as depicted on Figure 5.3. We will refer to it as the *observed degree* or *exact degree*. In the remaining part of this chapter and Chapter 6 we will understand more precisely when these plateaus appear. We will also study other instances of MiMC. In particular, we will see that for $d = 2^k - 1$ there are also other plateaus but their frequency decreases as k increases.

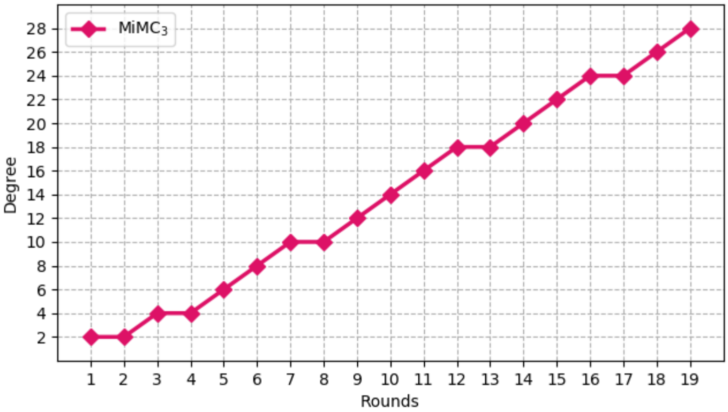


Figure 5.3: *Observed algebraic degree of* MiMC$_3$ *(for* $n \geqslant 31$*).*

5.2 Sparse univariate polynomials

As we have already seen, the algebraic degree can be easily derived from the univariate form of the polynomial describing the transformation. Then, if we could determine the form of the univariate polynomial by describing more precisely the set $\mathcal{E}_{d,r}$ of exponents of monomials with non-zero coefficients, this would give us a more precise bound on the algebraic degree. So, in this section our aim is to show that some families of exponents never appear in the univariate form of the polynomial describing MiMC$_d$.

To better describe the pattern followed by missing exponents we have chosen to represent them with an array of active and non-active squares. We explain the representation in Figure 5.4.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

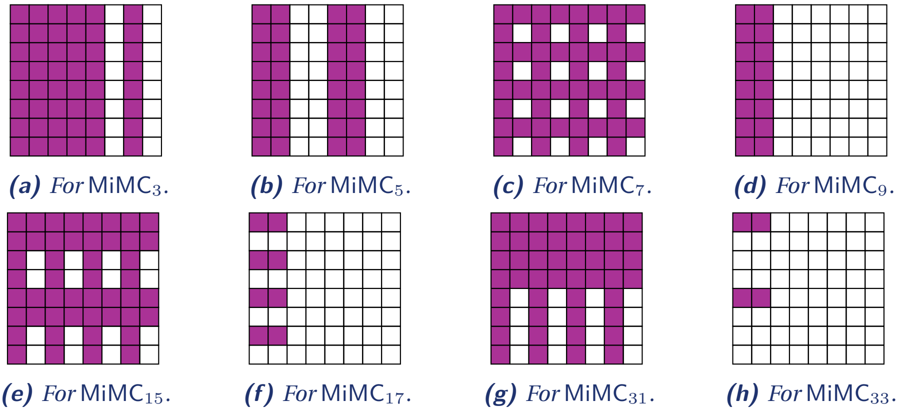
(a) *Representation modulo* 16.

		■	
	■		

(b) *Active exponents modulo* 16.

Figure 5.4: *Representation of the exponents of* $x^2 + x^9 + x^{18} + x^{25}$.

Then in Figure 5.5 we show the exponents that might appear in the univariate form of MiMC$_d[r]$. Exponents are represented modulo 64, and each non active square means that the corresponding exponents are missing. This indicates that some polynomials have a very sparse representation. In the following we will explain why such exponents can not appear in the univariate polynomial representation of MiMC$_d[r]$. In Section 5.2.1 we will focus on the case where $d \equiv 1 \bmod 2^j$ and $j > 1$, and in Section 5.2.2 we will study the case where $d \equiv 2^j - 1 \bmod 2^{j+1}$.



(a) *For* MiMC$_3$. *(b)* *For* MiMC$_5$. *(c)* *For* MiMC$_7$. *(d)* *For* MiMC$_9$.

(e) *For* MiMC$_{15}$. *(f)* *For* MiMC$_{17}$. *(g)* *For* MiMC$_{31}$. *(h)* *For* MiMC$_{33}$.

Figure 5.5: *Representation of exponents modulo* 64 *for some instances of* MiMC$_d$.

5.2.1 Missing exponents for MiMC$_d$, with $d \equiv 1 \bmod 2^j$ and $j > 1$

The mappings x^3 is a specific case of Gold functions [Gol68], i.e. of x^d, with d of the form $2^j + 1$. Let us investigate the general case for such permutations.

Proposition 5.4. *[McE87] The mapping x^d with $d = 2^j + 1$ is a permutation in $\mathbb{F}_{2^n}$ if and only if $n/\gcd(j, n)$ is odd.*

Proposition 5.5. *Let $\mathcal{E}_{d,r}$ be the set of exponents in the univariate form of* MiMC$_d[r]$*, where $d = 2^j + 1$ with $j > 1$. Then, any $i \in \mathcal{E}_{d,r}$ satisfies*

$$i \bmod 2^j \in \{0, 1\} .$$

Proof. We prove it by induction on r. First, it holds at round 2, since

$$\mathcal{E}_{d,2} = \{0, 2^j + 1, 2^{2j} + 2^j, 2^{2j} + 2^{j+1} + 1\} .$$

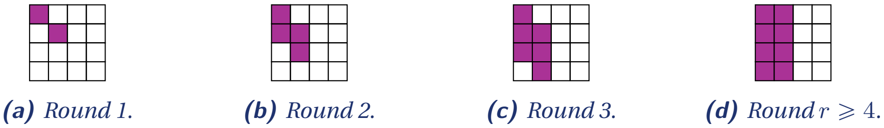
Then, let us assume that the property holds for $\mathcal{E}_{d,r}$, i.e., any $i \in \mathcal{E}_{d,r}$ can be written $i = a2^j + \varepsilon$ with $\varepsilon \in \{0, 1\}$. Let $i' \preceq i$. Then, $i' = a'2^j + \varepsilon'$ with $a' \preceq a$ and $\varepsilon' \leqslant \varepsilon$. Moreover,

$$\begin{aligned} di' &= (2^j + 1)(a'2^j + \varepsilon') = 2^j(a'2^j + \varepsilon' + a') + \varepsilon' \\ &\equiv \varepsilon' \bmod 2^j . \end{aligned}$$

Then, it follows that any $\ell = di' \in \mathcal{E}_{d,r+1}$ is such that $\ell \bmod 2^j \in \{0, 1\}$. □

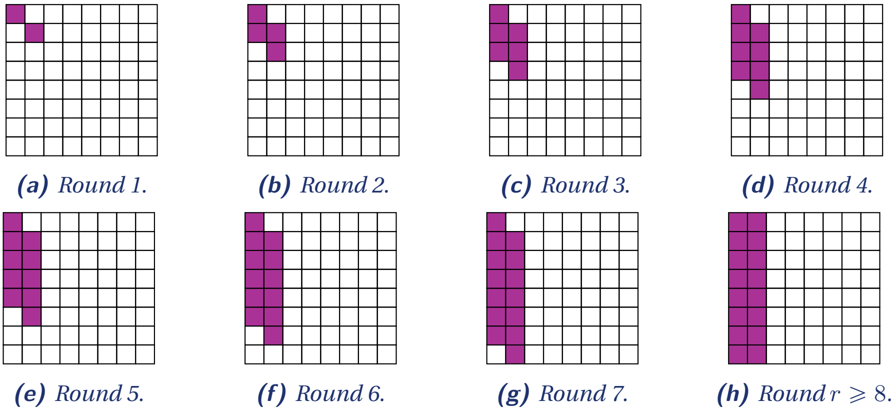
Proposition 5.5 implies that, for any d such that $d = 1 \bmod 2^j$ and $j > 1$, all exponents in the univariate form of MiMC$_d[r]$ are necessarily equal to 0 or 1 modulo 2^j. It also shows that the univariate polynomial describing MiMC$_d$ gets more and more sparse when j increases.

In particular, in the first rounds more missing exponents can be observed as illustrated in Figures 5.6 and 5.7 for MiMC$_5$ and MiMC$_9$ respectively. Indeed, in Corollary 5.2, we prove that for all rounds $r \leqslant 2^j$, the polynomials representing MiMC$_d$ are more sparse than predicted by Proposition 5.5.



(a) *Round 1.* *(b)* *Round 2.* *(c)* *Round 3.* *(d)* *Round $r \geqslant 4$.*

Figure 5.6: *Representation of exponents modulo 16 for MiMC_5.*



(a) *Round 1.* *(b)* *Round 2.* *(c)* *Round 3.* *(d)* *Round 4.*

(e) *Round 5.* *(f)* *Round 6.* *(g)* *Round 7.* *(h)* *Round $r \geqslant 8$.*

Figure 5.7: *Representation of exponents modulo 64 for MiMC_9.*

Corollary 5.2. *Let $\mathcal{E}_{d,r}$ be the set of exponents in the univariate form of $\mathsf{MiMC}_d[r]$, where $d = 2^j + 1$. Then, any $i \in \mathcal{E}_{d,r}$ satisfies*

$$\begin{cases} i \bmod 2^{2j} \in \left\{\gamma 2^j, (\gamma+1)2^j + 1, \text{ with } 0 \leqslant \gamma \leqslant r-1\right\} & \text{if } r \leqslant 2^j\,, \\ i \bmod 2^j \in \{0, 1\} & \text{if } r \geqslant 2^j\,. \end{cases}$$

Proof. Suppose that $r \leqslant 2^j$. We prove the result by induction on r. It holds at round 1, since

$$\mathcal{E}_{d,1} = \{0, 2^j + 1\} = \left\{\gamma 2^j, (\gamma+1)2^j + 1,\ \gamma = 0\right\} .$$

Let us now assume that the property holds for $\mathcal{E}_{d,r}$, i.e., any $i \in \mathcal{E}_{d,r}$ satisfies

$$i \bmod 2^{2j} \in \left\{\gamma 2^j, (\gamma+1)2^j + 1,\ \gamma = 0, \dots r-1\right\} .$$

First we notice that

$$\mathsf{Cover}(\{\gamma 2^j, \gamma = 0, \dots r-1\}) = \{\gamma 2^j, \gamma = 0, \dots r-1\} ,$$

and

$$\mathsf{Cover}(\{(\gamma+1)2^j + 1, \gamma = 0, \dots r-1\}) = \left\{1, (\gamma+1)2^j, (\gamma+1)2^j + 1, \gamma = 0, \dots r-1\right\} ,$$

implying that $i' \in \mathcal{E}_{d,r+1}$ satisfies

$$i' \in \left\{(2^j+1)(\gamma 2^j), (2^j+1)(\gamma 2^j + 1), \gamma = 0, \dots r\right\} ,$$

that is

$$i' \bmod 2^{2j} \in \left\{\gamma 2^j, (\gamma+1)2^j + 1,\ \gamma = 0, \dots r\right\} .$$

If $r = 2^j$ we have

$$\{i \bmod 2^{2j} \in \{\gamma 2^j, (\gamma+1)2^j + 1,\ \gamma = 0, \dots r-1\}\} = \{i \bmod 2^j \in \{0,1\}\} .$$

Finally, if $r > 2^j$, the result corresponds to Proposition 5.5. □

5.2.2 Missing exponents for MiMC_d, with $d \equiv 2^j - 1 \bmod 2^{j+1}$

Let us now investigate other instances of MiMC. While the cube is one example of Gold functions, the polynomials representing MiMC_3 do not behave as previously described. Indeed applying Proposition 5.5 would mean that the exponents that might appear in the polynomials are equal to 0 or 1 modulo 2. Although such an observation is true, this does not give any clue on the possible sparsity of the polynomials. In this section we see that the polynomials representing MiMC_3, and more generally the polynomials representing MiMC_d where $d \equiv 2^j - 1 \bmod 2^{j+1}$, also have missing exponents.

5.2.2.1 A first example with MiMC_3

Proposition 5.6. *Let $\mathcal{E}_{3,r}$ be the set of exponents in the univariate form of* $\mathsf{MiMC}_3[r]$*, as defined in Proposition 5.1. Then, any $i \in \mathcal{E}_{3,r}$ satisfies*

$$i \not\equiv 5, 7 \bmod 8 .$$

Proof. We prove the result by induction on r.

- **For $r = 3$:** the property is satisfied since

$$\mathcal{E}_{3,3} = \{0, 3, 6, 9, 12, 18, 24, 27\} .$$

  So $15, 21 \notin \mathcal{E}_{3,3}$ meaning that each element of $\mathcal{E}_{3,3}$ is different from 5 and 7 modulo 8.

- **Induction step:** Let us now assume that the property holds for $\mathcal{E}_{3,r}$, i.e., for any integer $i \in \mathcal{E}_{3,r}$ we have $i \not\equiv 5, 7 \bmod 8$. It follows that, for any $j \in \mathsf{Cover}(\mathcal{E}_{3,r})$, we have $j \not\equiv 5, 7 \bmod 8$. Indeed, let us recall that

$$\mathcal{E}_{3,r+1} = \{3j, \text{ such that } j \in \mathsf{Cover}(\mathcal{E}_{3,r})\} .$$

  But, if $j \bmod 8 \in \{0,1,2,3,4,6\}$, then we necessarily have $3j \bmod 8 \in \{0,1,2,3,4,6\}$. As a consequence, any $i \in \mathcal{E}_{3,r+1}$ is such that $i \not\equiv 5, 7 \bmod 8$.

□

This proposition implies that the degree of $\mathsf{MiMC}_3[r]$ cannot exceed

$$k_{3,r} := \lfloor r \log_2 3 \rfloor$$

since $\mathcal{E}_{3,r} \subseteq \{i : i \leqslant 3^r\} \subseteq \{i : i < 2^{k_{3,r}+1}\}$. Indeed, the only integer $i < 2^{k_{3,r}+1}$ of weight strictly greater than $k_{3,r}$ is $2^{k_{3,r}+1} - 1$, which does not belong to $\mathcal{E}_{3,r}$ since it satisfies $2^{k_{3,r}+1} - 1 \equiv 7 \bmod 8$.

5.2.2.2 Generalization

The mappings x^3 is another specific case of functions x^d with $d = 2^j - 1$. In this section we generalize Proposition 5.6 to MiMC_d, where d is any integer such that $d \equiv 2^j - 1 \bmod 2^{j+1}$ $(j \neq 0)$.

Proposition 5.7. *Let $\mathcal{E}_{d,r}$ be the set of exponents in the univariate form of $\mathsf{MiMC}_d[r]$, where $d = 2^j - 1$. Then, any $i \in \mathcal{E}_{d,r}$ satisfies*

$$i \bmod 2^{j+1} \in \{0, 1, \dots 2^j\} \cup \{2^j + 2\gamma \textit{ such that } \gamma = 1, 2, \dots 2^{j-1} - 1\} .$$

Proof. We prove the result by induction on r. It holds at round 2. First, let us recall that

$$\mathcal{E}_{d,2} = \{dk, k \in \{0, \dots, d\}\} .$$

If $k = 1 + 2k'$ is odd we have

$$dk \bmod 2^{j+1} \equiv (2^j - 1)(1 + 2k') = 2^j - (1 + 2k') ,$$

with $k \in \{0, 1, \dots 2^{j-1} - 1\}$. Therefore, we have

$$dk \bmod 2^{j+1} \in \{2\gamma + 1 \text{ with } \gamma = 0, 1, \dots 2^{j-1} - 1\} .$$

If $k = 2k'$ is even we have

$$dk \bmod 2^{j+1} \equiv (2^j - 1)2k' = 2^j + 2(2^{j-1} - k') ,$$

with $k \in \{0, 1, \dots 2^{j-1} - 1\}$. Therefore, we have

$$dk \bmod 2^{j+1} \in \{0\} \cup \{2^j + 2\gamma \text{ with } \gamma = 1, 2, \dots 2^{j-1} - 1\} .$$

In particular, this implies that any $i \in \mathcal{E}_{d,2}$ satisfies

$$i \bmod 2^{j+1} \in \{0, 1, \dots 2^j\} \cup \{2^j + 2\gamma \text{ with } \gamma = 1, 2, \dots 2^{j-1} - 1\} .$$

Let us now assume that the property holds for $\mathcal{E}_{d,r}$, i.e., any $i \in \mathcal{E}_{d,r}$ satisfies

$$i \bmod 2^{j+1} \in \{0, 1, \dots 2^j\} \cup \{2^j + 2\gamma \text{ with } \gamma = 1, 2, \dots 2^{j-1} - 1\} .$$

It follows that, for any $k \in \mathsf{Cover}(\mathcal{E}_{d,r})$, we have

$$k \bmod 2^{j+1} \notin \{2^j + 2\gamma + 1 \text{ with } \gamma = 1, 2, \dots 2^{j-1} - 1\} .$$

Any element i in $\mathcal{E}_{d,r+1}$ is given by $i = dk$ with $k \in \mathsf{Cover}(\mathcal{E}_{d,r})$. But, if k is such that

$$k \bmod 2^{j+1} \in \{0, 1, \dots 2^j\} \cup \{2^j + 2\gamma \text{ with } \dots \gamma = 1, 2, 2^{j-1} - 1\} ,$$

then we necessarily have

$$dk \bmod 2^{j+1} \in \{0, 1, \dots 2^j\} \cup \{2^j + 2\gamma \text{ with } \gamma = 1, 2, \dots 2^{j-1} - 1\} .$$

Indeed, as we have seen previously if $k \in \{0, \dots, d\}$ then

$$dk \in \{0\} \cup \{2\gamma + 1 \text{ with } \gamma = 0, 1, \dots 2^{j-1} - 1\} \cup \{2^j + 2\gamma \text{ with } \gamma = 1, 2, \dots 2^{j-1} - 1\} .$$

Power of the iterated function	Form of missing exponents	Rate of missing exponents
$3, 11, 19, 27, 35, 43, 51, 59$	$e \bmod 8 \in \{5, 7\}$	$\geqslant 25\%$
$5, 13, 21, 29, 37, 45, 53, 61$	$e \bmod 4 \in \{2, 3\}$	$\geqslant 50\%$
$7, 23, 39, 55$	$e \bmod 16 \in \{9, 11, 13, 15\}$	$\geqslant 25\%$
$9, 25, 41, 57$	$e \bmod 8 \in \{2, 3, 4, 5, 6, 7\}$	$\geqslant 75\%$
$15, 47$	$e \bmod 32 \in \{17, 19, 21 \ldots 31\}$	$\geqslant 25\%$
$17, 49$	$e \bmod 16 \in \{2, 3, 4, 5 \ldots 15\}$	$\geqslant 87.5\%$
31	$e \bmod 64 \in \{33, 35, 37 \ldots 63\}$	$\geqslant 25\%$
33	$e \bmod 32 \in \{2, 3, 4, 5 \ldots 31\}$	$\geqslant 93.75\%$

Table 5.2: *Missing exponents for* $\mathsf{MiMC}_d, d \leqslant 61$.

Then, let $k = 2^j + 2\gamma$ where $\gamma \in \{0, 1, \ldots 2^{j-1} - 1\}$. We have

$$dk \bmod 2^{j+1} \equiv (2^j - 1)(2^j + 2\gamma) = 2^j + 2\gamma(2^j - 1)\,,$$

implying that

$$dk \bmod 2^{j+1} \in \{2\gamma \text{ such that } \gamma = 1, \ldots 2^{j-1}\}\,.$$

It follows that any $i \in \mathcal{E}_{d,r+1}$ is such that

$$i \bmod 2^{j+1} \notin \{2^j + 2\gamma + 1, \gamma = 1, 2, \ldots 2^{j-1} - 1\}\,.$$

□

This proposition implies that for any d such that $d = 2^j - 1 \bmod 2^{j+1}$, then all exponents modulo 2^{j+1} in the univariate form of $\mathsf{MiMC}_d[r]$ are necessarily equal to an even integer or lower than 2^j .

While most of the primitives use an iterated function defined by a low degree exponent (usually the smallest one), we also aim at giving a comparison between different exponents. We note that for any choice of the exponent d for the iterated power function in MiMC_d, at least one fourth of the exponents never appear.

Although it is not known at this stage how to exploit efficiently sparse univariate polynomial representations to build distinguishers, we would like to point that even if Gold functions are particularly interesting because of their low degree, using them might be risky given the very sparse univariate representation of MiMC in this case.

In this section we have considered polynomials such that the secret key is part of the round constants since this does not change the algebraic degree. We note also that the same is true for the families of exponents that are missing in the univariate form of the polynomials representing MiMC_d.

Remark 5.1. The results of the Proposition 5.5, Corollary 5.2 and Proposition 5.7 are still valid if we add a whitening key before applying MiMC as defined on Figure 5.1. Indeed, if $F(x) = \sum_i \alpha_i x^i$, then we have

$$F(x+k) = \sum_i \alpha_i \prod_{\ell \in I} (x+k)^{2^\ell} = \sum_i \alpha_i \prod_{\ell \in I} (x^{2^\ell} + k^{2^\ell}) = \sum_i \alpha_i \sum_{J \subseteq I} x^{\sum_{\ell \in J} 2^\ell} c^{\sum_{\ell \in I \setminus J} 2^\ell}\,,$$

where $I = \mathsf{Supp}(i)$, and the above properties remain valid for any element i' such that $i' \preceq i$.

Then the only difference in the univariate representation is that when omitting the whitening key we have only multiples of d.

5.3 Bounding the degree

We now mainly focus on the algebraic degree of MiMC_d over $\mathbb{F}_{2^n}$, i.e., on the value of B_d^r. As already mentioned, the algebraic degree can be derived from the univariate representation of MiMC_d. Therefore, the missing exponents exhibited in Section 5.2 will allow us to determine bounds on the algebraic degree of MiMC_d.

First, we notice that a trivial lower bound can be exhibited. Indeed, if the univariate degree d^r is lower than $2^n - 1$, then the monomial x^{d^r} appears in the polynomial and its coefficient is always 1, independently of the choice of the round constants and therefore never vanishes. Then, knowing that B_d^r is a non-decreasing sequence (see Proposition 5.2), this obviously defines a lower bound:

$$B_d^r \geqslant \max\{\mathrm{wt}(d^i), i \leqslant r\} \ . \tag{5.2}$$

Obviously, as long as the degree of the univariate polynomial does not exceed $2^n - 1$, the algebraic degree of r rounds of MiMC_d is upper-bounded by $\lceil \log_2(d^r) \rceil = \lceil r \log_2 d \rceil$. But this bound, used in [Eic+20] to set up integral attacks, can be easily improved by showing that the elements in $\mathcal{E}_{d,r}$ satisfy some particular properties.

More precisely, in this section we aim at better understanding the behaviour of the algebraic degree using the sparse univariate polynomial representation. In particular we show that for some instance of MiMC_d the difference between the observed degree and $k_{d,r} := \lfloor r \log_2 d \rfloor$ is high in the first rounds as illustrated in Figure 5.8. We recall that by observed degree, we mean the degree computed with a C program implementing the procedure of Corollary 5.1. Since computations become more expensive while using higher-degree permutations, we choose to represent instances of MiMC_d until $d = 17$ for $r = 7$ rounds.

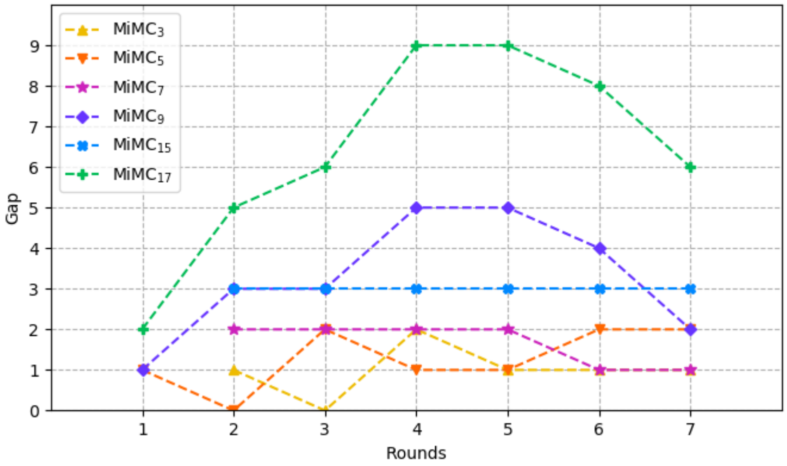


Figure 5.8: *Gap between the observed degree of* MiMC_d *and* $k_{d,r}$.

5.3.1 Bounds for MiMC_d with $d = 2^j + 1$

To bound the algebraic degree, we use the sparsity of univariate polynomials proved in Section 5.2.1 and the divisibility of exponents modulo d. Let e be an integer written as $e = \sum_{i \in \mathsf{Supp}(e)} 2^i$. By first investigating the value of each $2^i \bmod d$, we can then deduce the value of e modulo d, and so can conclude whether e can appear as an exponent in the univariate polynomial representation of MiMC_d.

So let us first consider the powers of 2 modulo d.

Lemma 5.2. *Let $d = 2^j + 1$, then*

$$2^i \bmod d \equiv \begin{cases} 2^{i \bmod 2j} & \text{if } i \equiv 0, \ldots, j \bmod 2j \,, \\ d - 2^{(i \bmod 2j) - j} & \text{if } i \equiv j+1, \ldots, 2j-1 \bmod 2j \,. \end{cases}$$

Proof. We first prove the case for $i < 2j$ and then generalize to any i.

- If $i = 0, \ldots, j$, then $d > 2^i$ so $2^i = 2^i \bmod d$.
- If $i = j+1, \ldots, 2j-1$, then

$$2^i = 2^j \cdot 2^{i-j} = (2^j + 1)2^{i-j} - 2^{i-j} \equiv d - 2^{i-j} \bmod d \,.$$

- Finally let $i' \geqslant 2j$ be such that $i' = i + \ell \cdot 2j$ with $i < 2j$. By observing that $2^{2j} \equiv 1 \bmod d$ since $d \mid (2^{2j} - 1)$, we have

$$2^{i'} = 2^i \cdot (2^{2j})^\ell \equiv 2^i \bmod d \,.$$

□

From Lemma 5.2 we can then deduce some criteria for the divisibility of any integer by d.

Lemma 5.3. *Let $d = 2^j + 1$, such that $j \geqslant 2$, and let $k_{d,r} = \lfloor r \log_2 d \rfloor$. Then $2^{k_{d,r}+1} - 2^\ell - d + 2$, with $\ell \in \{0\} \cup \{2^j, 2^j + 1, \ldots k_{d,r}\}$, is divisible by d if and only if*

$$(k_{d,r} \bmod 2j, \ell \bmod 2j) \in \{(0,2), (j-1,0), (j+1,j+1)\} \,.$$

Proof. First, let us observe that if $(k_{d,r} \bmod 2j) \in \{0, j-1, j+1\}$, then Lemma 5.2 implies that $(k_{d,r} \bmod 2j, \ell \bmod 2j) \in \{(0,2), (j-1,0), (j+1,j+1)\}$ in order to have $d | 2^{k_{d,r}+1} - 2^\ell - d + 2$. Then, we suppose $k_{d,r} = \gamma \bmod 2j \notin \{0, j-1, j+1\}$, and we distinguish 3 cases:

1. $\gamma \bmod 2j \in \{1, \ldots j-2\}$

$$2^{k_{d,r}+1} - 2^\ell - d + 2 = 2^{\gamma+1} - 2^\ell + 2 \bmod d \,,$$

where $(2^{\gamma+1} + 2) \in \{6, 10, \ldots, 2^{j-1} + 2\}$. According to Lemma 5.2, no power of 2 is equal to such a value modulo d.

2. $\gamma \bmod 2j = j$, then

$$2^{k_{d,r}+1} - 2^\ell - d + 2 = 2(2^j + 1) - 2^\ell - d = -2^\ell \bmod d \,,$$

which is never divisible by d.

3. $\gamma \bmod 2j \in \{j+2, \dots 2j-1\}$
$$2^{k_{d,r}+1} - 2^{\ell} - d + 2 = 2^{\gamma+1} - 2^{\ell} + 2 \bmod d\,,$$
where $(2^{\gamma+1}+2) \in \{2^{j+3}+2, \dots, 2^{2j}+2\}$. According to Lemma 5.2, no power of 2 is equal to such a value modulo d.

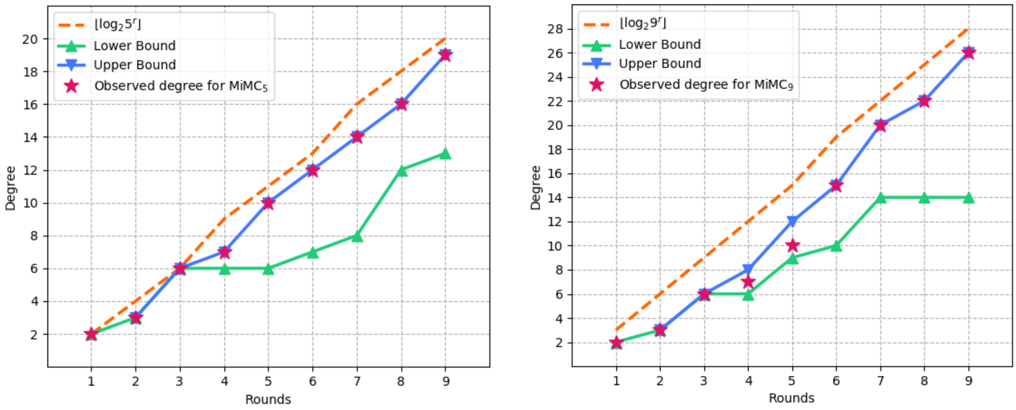
□

Using Lemma 5.3 we can then define an upper bound on the algebraic degree of MiMC_d when $d = 2^j + 1$.

Proposition 5.8. *Let $r > 1$. The maximal algebraic degree of $\mathsf{MiMC}_d[r]$, with $d = 2^j + 1$, satisfies:*
$$B_d^r \leqslant \begin{cases} k_{d,r} - j + 1 & \textit{if}\, k_{d,r} \bmod 2j \in \{0, j-1, j+1\}\,, \\ k_{d,r} - j & \textit{otherwise}\,. \end{cases}$$

Proof. As stated in Proposition 5.5, any exponent $i \in \mathcal{E}_{d,r}$ is such that $i \bmod 2^j \in \{0,1\}$. Then, the only possible exponents ω such that $\mathrm{wt}(\omega) = k_{d,r} - j + 1$ are necessarily of the following form:
$$(2^{k_{d,r}+1} - 2^j + 1) - 2^{\ell} = 2^{k_{d,r}+1} - 2^{\ell} - d + 2\,.$$
Then, using Lemma 5.3 we can directly conclude that such exponents exist only if $k_{d,r} \bmod 2j \in \{0, j-1, j+1\}$. □

This bound can be refined on the first rounds using Corollary 5.2 since we can identify more missing exponents. In Figures 5.9a and 5.9b we compare our upper bound given in Proposition 5.8 and the lower bound given in Equation (5.2) with the observed degree for MiMC_5 and MiMC_9 respectively.



(a) MiMC_5 ***(b)*** MiMC_9

Figure 5.9: *Comparison between our bounds and the exact degree of MiMC_d, $d = 2^j + 1$.*

Let us compare our bound, given in Proposition 5.8 and other bounds obtained, following our work on MiMC_3, in [Liu+23a; Cui+22]. The method from [Liu+23a] relies on a specific representation of exponents called the “coefficient grouping strategy” which allows to efficiently convert the problem of finding the algebraic degree into an optimization problem. We will give more details on such procedure in Chapter 7. In [Cui+22], the authors rely on the division property. By introducing propagation rules of monomials with an efficient modelisation for solvers, their searching tool is able to compute very tight bounds for the algebraic degree. Our approach is different since it does not rely on a solver but on a better understanding of the univariate form of the polynomial describing the transformation. While our approach does not improve or even reach the same precision as other methods, we would like to stress that the analysis we provide is valid for any number of rounds and is not limited by the computational performances of a computer.

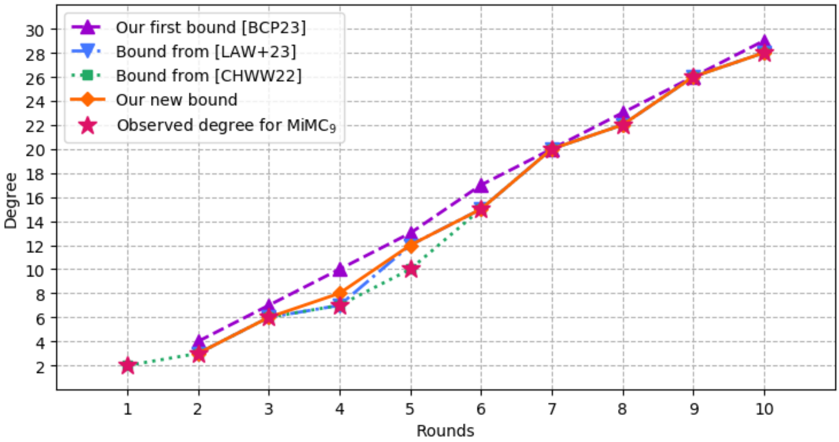


Figure 5.10: Comparison between various bounds on the degree of MiMC_9.

5.3.2 Bounds for MiMC_d with $d = 2^j - 1$

In light of Section 5.3.1, we also investigate bounds for the algebraic degree of MiMC_d using the knowledge of missing exponents (see Proposition 5.7) and the divisibility by d of any integer.

5.3.2.1 First example with MiMC_3

We now exhibit a more accurate upper-bound on the degree of MiMC_3, which makes use of the following result.

Lemma 5.4. *[Her36] The equation* $2^x - 3^y = 5$ *admits only two solutions* $(x, y) = (3, 1)$ *and* $(5, 3)$.

Proposition 5.9. *Let* $k_{3,r} = \lfloor r \log_2 3 \rfloor$. *Then, for all* $r > 4$, *we have*

$$2^{k_{3,r}+1} - 5 > 3^r .$$

Proof. The proof depends on the parity of $k_{3,r}$.

- If $k_{3,r}$ is odd so that $k_{3,r} = 2k + 1$, it is enough to show that

$$3^r \notin \{2^{2k+2} - 5, 2^{2k+2} - 4, 2^{2k+2} - 3, 2^{2k+2} - 2, 2^{2k+2} - 1\} ,$$

since $3^r < 2^{2k+2}$ by definition of $k_{3,r}$. As $2^{2k+2} \equiv 1 \bmod 3$, it follows that

$$2^{2k+2} - 3 \equiv 1 \bmod 3 \quad \text{and} \quad 2^{2k+2} - 5 \equiv 2^{2k+2} - 2 \equiv 2 \bmod 3\,,$$

so that $3^r \notin \{2^{2k+2}-5, 2^{2k+2}-3, 2^{2k+2}-2\}$. Then $2^{2k+2}-4$ and $2^{2k+2}-1$ are both multiple of 3, but $3^r \neq 2^{2k+2} - 4$ since $2^{2k+2} - 4 = 4(2^{2k} - 1)$ and 3^r is not a multiple of 4, and $3^r \neq 2^{2k+2} - 1$ since $2^{2k+2} - 1 \equiv 7 \bmod 8$, and for any power of 3 we have $3^r \bmod 8 \in \{1, 3\}$. We deduce that $3^r < 2^{2k+2} - 5$.

- Similarly, if $k_{3,r}$ is even, so that $k_{3,r} = 2k$, we first prove that

  $$3^r \notin \{2^{2k+1} - 4, 2^{2k+1} - 3, 2^{2k+1} - 2, 2^{2k+1} - 1\}\,.$$

  As $2^{2k+1} \equiv 2 \bmod 3$, it follows that

  $$2^{2k+1} - 3 \equiv 2 \bmod 3 \quad \text{and} \quad 2^{2k+1} - 4 \equiv 2^{2k+1} - 1 \equiv 1 \bmod 3\,,$$

  so that $3^r \notin \{2^{2k+2} - 4, 2^{2k+2} - 3, 2^{2k+2} - 1\}$. Then $2^{2k+1} - 2$ is a multiple of 3, but $3^r \neq 2^{2k+1} - 2$ since $2^{2k+1} - 2 = 2(2^{2k} - 1)$ and 3^r is odd. Finally, according to Lemma 5.4, the equation $3^r = 2^{2k+1} - 5$ has no solution for $r > 4$. We deduce that $3^r < 2^{2k+1} - 5$.

□

Proposition 5.10. *For any $r \geqslant 4$, the algebraic degree after r rounds of* MiMC$_3$ *satisfies*

$$B_3^r \leqslant 2 \times \lceil k_{3,r}/2 - 1 \rceil\,,$$

where $k_{3,r} = \lfloor r \log_2 3 \rfloor$.

Proof. Let us observe that

$$2 \times \lceil k_{3,r}/2 - 1 \rceil = \begin{cases} k_{3,r} - 1 & \text{if } k_{3,r} \equiv 1 \bmod 2 \\ k_{3,r} - 2 & \text{if } k_{3,r} \equiv 0 \bmod 2\,. \end{cases}$$

Then, we first show that the algebraic degree at round r is at most $k_{3,r} - 1$ whatever the parity of $k_{3,r}$.

Assuming the degree is $k_{3,r}$, this would mean that there exists $\omega \in \mathcal{E}_{3,r}$ such that $\mathrm{wt}(\omega) = k_{3,r}$. By definition of $k_{3,r}$, ω should be of the form $2^{k_{3,r}+1} - 2^j - 1$ with $0 \leqslant j \leqslant k_{3,r}$. However such exponents are either non-divisible by 3 or missing. Indeed, we know from Proposition 5.6 that, when $j \notin \{0, 2\}$, exponents $2^{k_{3,r}+1} - 2^j - 1$ are missing since $2^{k_{3,r}+1} - 2^j - 1 \bmod 8 \in \{5, 7\}$. And for $j \in \{0, 2\}$, we derive from Proposition 5.9 that

$$2^{k_{3,r}+1} - 2^j - 1 \geqslant 2^{k_{3,r}+1} - 5 > 3^r\,,$$

implying that these exponents do not belong to $\mathcal{E}_{3,r}$.

Now, let us prove that, when $k_{3,r}$ is even, the degree cannot be $k_{3,r} - 1$. Similarly, the only possible exponents of weight $k_{3,r} - 1$ are of the form

$$\omega = 2^{k_{3,r}+1} - 2^j - 2^i - 1, \text{ with } 0 \leqslant i < j \leqslant k_{3,r}\,.$$

Such exponents are all equal to 5 or 7 modulo 8 except when i or j belongs to $\{0, 2\}$. If i or j is equal to 0, then $\omega = 2^{k_{3,r}+1} - 2^\ell - 2$, and if i or j is equal to 2, then $\omega = 2^{k_{3,r}+1} - 2^\ell - 5$. However when $k_{3,r}$ is even, $2^{k_{3,r}+1} - 2$ and $2^{k_{3,r}+1} - 5$ are both divisible by 3 implying that neither $2^{k_{3,r}+1} - 2^\ell - 2$ nor $2^{k_{3,r}+1} - 2^\ell - 5$ can be divisible by 3. □

From Equation (5.2) page 121 and the previous proposition we deduce that the algebraic degree of MiMC$_3$ satisfies the following relation:

$$\max\{\mathrm{wt}(3^i), i \leqslant r\} \leqslant B_3^r \leqslant 2 \times \lceil k_{3,r}/2 - 1 \rceil\,.$$

5.3.2.2 Generalization

One particular point of interest in this section is to detect the presence of plateaus. In Section 5.1.3 it has been proved that there is always a plateau between the first two rounds of MiMC_d where $d = 2^j - 1$. Moreover, when $d = 3$ such plateaus occur each time that $k_{3,r}$ is odd and $k_{3,r+1}$ is even (the complete proof will be given in Corollary 6.3 after proving that the upper bound given in the previous section is exact). Here, we aim at generalizing this result. Studying an upper bound on B_d^r, we show that we can observe a plateau between round r and $r+1$ when $k_{d,r} \equiv j-1 \bmod j$ and $k_{d,r+1} \equiv 0 \bmod j$. However, unlike for MiMC_3, we are not yet able to prove that our bound is exact.

We start by investigating the divisibility by d of any integer. First let us have a look at powers of 2 modulo d.

Lemma 5.5. *Let $d = 2^j - 1$, then*

$$2^i \bmod d \equiv 2^{i \bmod j} .$$

Proof. We first prove the case for $i < j$ and then generalize to any i.

- If $i = 0, \ldots, j-1$, then $d > 2^i$ so $2^i = 2^i \bmod d$.
- Finally for $i' \geqslant j$, such that $i' = i + \ell \cdot j$ with $i < j$, we have

$$2^{i'} = 2^i \cdot (2^j)^\ell \equiv 2^i \bmod d .$$

□

As a consequence of Lemma 5.5, we deduce some criteria for the divisibility by d of any integer.

Lemma 5.6. *Let $d = 2^j - 1$, such that $j \geqslant 3$. We have*

$$d \mid 2^{k_{d,r}-k} - 1 \text{ if and only if } k_{d,r} = k \bmod j .$$

Let k be an integer such that $0 \leqslant k < j$. For all integers $\lambda \in \{-1, 0, 1, \ldots k-1\}$ we define

$$e_{\lambda,k} = 2^{k_{d,r}-\lambda} - \sum_{\ell=1}^{k-\lambda} 2^{i_\ell} - 1 . \tag{5.3}$$

Then, there exists $\{i_\ell\}_{1 \leqslant \ell \leqslant k-\lambda} \in [\![0, k_{d,r} - \lambda - 1]\!]^{k-\lambda}$ such that $e_{\lambda,k}$ is divisible by d if and only if

$$(k_{d,r} \bmod j) \in \{\lambda + 1, \ldots, k\} .$$

Proof. Let us notice that the first statement is a direct consequence of Lemma 5.5 since $2^{k_{d,r}-k} - 1$ is divisible by d if and only if $k_{d,r} - k$ is divisible by j.

Then, let k and λ be integers such that $0 \leqslant k < j$ and $\lambda \in \{-1, 0, 1, \ldots k-1\}$. Then let $\kappa \equiv k_{d,r} \bmod j$.

- if $\kappa \in [\![\lambda + 1, k]\!]$ then we have

$$e_{\lambda,k} = 2^{k_{d,r}-\lambda} - \sum_{\ell=1}^{k-\lambda} 2^{i_\ell} - 1 = 2^{\kappa-\lambda} - 1 - \sum_{\ell=1}^{k-\lambda} 2^{i_\ell} \bmod d ,$$

  where $(2^{\kappa-\lambda} - 1) \in [\![1, 2^{k-\lambda} - 1]\!]$, such that $\mathrm{wt}(2^{\kappa-\lambda} - 1) = \kappa - \lambda \in [\![1, k-\lambda]\!]$. Such a value can be obtained with a sum of $k - \lambda$ powers of 2 modulo d since, according to Lemma 5.5, $\mathrm{wt}\left(\sum_{\ell=1}^{k-\lambda} 2^{i_\ell} \bmod d\right) \leqslant k - \lambda$.

- if $\kappa \in [\![0, \lambda]\!]$ then we have

$$e_{\lambda,k} = 2^{k_{d,r}-\lambda} - \sum_{\ell=1}^{k-\lambda} 2^{i_\ell} - 1 = 2^{j+\kappa-\lambda} - 1 - \sum_{\ell=1}^{k-\lambda} 2^{i_\ell} \bmod d\,,$$

  where $(2^{j+\kappa-\lambda}-1) \in \{2^{j-\lambda}-1, \ldots, 2^j-1\}$, such that $\mathrm{wt}(2^{j+\kappa-\lambda}-1) = j+\kappa-\lambda \in [\![j-\lambda, j]\!]$. Such a value cannot be obtained with a sum of $k-\lambda$ powers of 2 modulo d since, according to Lemma 5.5, $\mathrm{wt}\left(\sum_{\ell=1}^{k-\lambda} 2^{i_\ell} \bmod d\right) \leqslant k-\lambda < j-\lambda$.

- if $\kappa \in [\![k+1, j-1]\!]$ then we have

$$e_{\lambda,k} = 2^{k_{d,r}-\lambda} - \sum_{\ell=1}^{k-\lambda} 2^{i_\ell} - 1 = 2^{\kappa-\lambda} - 1 - \sum_{\ell=1}^{k-\lambda} 2^{i_\ell} \bmod d\,,$$

  where $(2^{\kappa-\lambda}-1) \in [\![2^{k+1-\lambda}-1, 2^{j-1-\lambda}-1]\!]$, such that $\mathrm{wt}(2^{\kappa-\lambda}-1) = \kappa-\lambda \in [\![k+1-\lambda, j-1-\lambda]\!]$. Such a value cannot be obtained with a sum of $k-\lambda$ powers of 2 modulo d since, according to Lemma 5.5, $\mathrm{wt}\left(\sum_{\ell=1}^{k-\lambda} 2^{i_\ell} \bmod d\right) \leqslant k-\lambda < k+1-\lambda$.

It follows that

$$d \mid e_{\lambda,k} \text{ if and only if } (k_{d,r} \bmod j) \in \{\lambda+1, \ldots, k\}\,.$$

□

Remark 5.2. We notice that we do not require the $\{i_\ell\}_{1\leqslant\ell\leqslant k-\lambda}$ to be distinct since our proof relies on inequalities for the Hamming weight. Moreover, for some cases, the only possibility to have an integer divisible by d is to allow some of the $\{i_\ell\}_{1\leqslant\ell\leqslant k-\lambda}$ to be identical. For example, let $\lambda = -1$, $k = 1$ and $k_{d,r} \equiv 0 \bmod j$. Then we have:

$$e_{-1,1} = 2^{k_{d,r}+1} - \sum_{\ell=1}^{2} 2^{i_\ell} - 1 \equiv 2 - 2^{i_1} - 2^{i_2} - 1 = 1 - 2^{i_1} - 2^{i_2} \bmod d\,,$$

implying that we require that $i_1 = i_2 = j-1$ so that $2^{i_1} + 2^{i_2} = 2^j = 1 \bmod d$.

However, in the following Proposition 5.11, we do care about the precise Hamming weight of exponents so we will only consider integers $e_{\lambda,k}$ such that the $\{i_\ell\}_{1\leqslant\ell\leqslant k-\lambda}$ are distinct. This condition does not change the fact that for $(k_{d,r} \bmod j) \in \{k+1, \ldots, j-1\}$, the integers $e_{\lambda,k}$ are not divisible by d.

Example 5.1. Let us take some examples for $d = 15 = 2^4 - 1$. We have $15 \mid 2^{k_{15,r}-k} - 1$ if and only if $k_{15,r} = k \bmod 4$. For $\lambda = -1$ and $k = 0$ we get that $2^{k_{15,r}+1} - 2^{i_1} - 1$ is divisible by 15 if and only if $k_{15,r} = 0 \bmod 4$. The first index such that $k_{15,r} = 0 \bmod 4$ is $r = 33$, so that $k_{15,33} = 128$. Indeed, for $i_1 = 0 \bmod 4$ we have $15 \mid 2^{129} - 2^{i_1} - 1$ since

$$\begin{aligned} 2^{129} - 2^{4a} - 1 &= 2^{129} - 2^{4a+1} + 2^{4a} - 1 \\ &= 2^{4a+1}(2^{128-4a} - 1) + (2^{4a} - 1) \end{aligned}$$

and both terms are divisible by 15 (we use that $15 \mid 2^u - 1$ if and only if $4 \mid u$).

We also have for instance that $2^{k_{15,r}+1} - 2^{i_1} - 2^{i_2} - 1$ is divisible by 15 if and only if $k_{15,r} \bmod 4 \in \{0, 1\}$. The first index such that $k_{15,r} = 1 \bmod 4$ is $r = 22$, so that $k_{15,22} = 85$. Indeed, for

$i_1 = 0 \bmod 4$ and $i_2 = 1 \bmod 4$, for $i_1 = 1 \bmod 4$ and $i_2 = 0 \bmod 4$ we have $15 \mid 2^{86} - 2^{i_1} - 2^{i_2} - 1$. For instance, we can check that:

$$\begin{aligned}2^{86} - 2^{4a} - 2^{4b+1} - 1 &= 2^{86} - 2^{4a+1} + 2^{4a} - 2^{4b+2} + 2^{4b+1} - 1\\ &= (2^{86} - 2^{4b+2}) + (2^{4b+1} - 2^{4a+1}) + (2^{4a} - 1)\\ &= 2^{4b+2}(2^{84-4b} - 1) + 2^{4a+1}(2^{4b-4a} - 1) + (2^{4a} - 1)\end{aligned}$$

is divisible by 15.

Similarly, if $\lambda = 1$ and $k = 2$, then $2^{k_{15,r}-1} - 2^{i_1} - 1$ is divisible by 15 if and only if $k_{15,r} = 2 \bmod 4$. The first index such that $k_{15,r} = 2 \bmod 4$ is $r = 11$, so that $k_{15,11} = 42$. For $i_1 = 0 \bmod 4$ we have $15 \mid 2^{41} - 2^{i_1} - 1$ since

$$\begin{aligned}2^{41} - 2^{4a} - 1 &= 2^{41} - 2^{4a+1} + 2^{4a} - 1\\ &= 2^{4a}(2^{40-4a} - 1) + (2^{4a} - 1)\end{aligned}$$

is divisible by 15.

Lemma 5.6 then enables us to define an upper bound on the algebraic degree of MiMC_d when $d = 2^j - 1$.

Proposition 5.11. *Let $d = 2^j - 1$, such that $j \geqslant 2$. Then,*

$$B_d^r \leqslant k_{d,r} - (k_{d,r} \bmod j)\,.$$

Proof. Let $k = k_{d,r} \bmod j$. Let us assume that $\mathcal{E}_{d,r}$ contains some exponent e of Hamming weight $k_{d,r} - k'$ for some $k' < k$. Then, any such exponent e satisfies $\log_2 e \leqslant k_{d,r}$. It is then necessarily of the form $2^{k_{d,r}-k'} - 1$ or of the form of Equation (5.3) with distinct $\{i_\ell\}_{1\leqslant\ell\leqslant k-\lambda}$. In Lemma 5.6, we have shown that such an integer is divisible by d if and only if $(k_{d,r} \bmod j) \in \{\lambda+1, \dots k'\}$. As $k > k'$, those integers cannot belong to $\mathcal{E}_{d,r}$ meaning that all exponents are necessary of Hamming weight $\omega \leqslant k_{d,r} - k$. It directly follows that the degree of MiMC_d after r rounds satisfies $B_d^r \leqslant k_{d,r} - (k_{d,r} \bmod j)$. □

From Lemma 5.4, we deduce that the equation $2^k = 3^r + 5$ has no solution for $r \geqslant 4$. Then in Lemma 5.7 we generalize this result.

Lemma 5.7. *Let $d = 2^j - 1$ be such that $3 \leqslant j \leqslant 7$. If $k_{d,r} = 0 \bmod j$, then the equation:*

$$2^k = d^r + 2^j + 1$$

has no solution (k, j, r) for $r > 1$.

Proof. First let us notice that $2^k = d^r + 2^j + 1$ has a solution for $r = 1$ and $k = j + 1$. So $d^r = -2^j - 1 \bmod 2^{j+1}$. Let us suppose that $r > 1$, then we have $k > j + 1$. In the proof we will look at each case separately. The general idea is to study congruences modulo powers of 2 to obtain a contradiction.

If $j = 3$, we need $7^r = -9 \bmod 2^4$.

- First let us consider congruences modulo 2^4. As $7^1 = 2^4 - 9 = -9 \bmod 2^4$ and the order of 7 in $\mathbb{Z}/2^4\mathbb{Z}$ is 2, then $r = 1 + 2r_1$.

- Let us take congruences modulo 2^5. As $7^1 \neq -9 \bmod 2^5$ and the order of 7 in $\mathbb{Z}/2^5\mathbb{Z}$ is 4, then $r = 1 + 2r_1 = 1 + 2(1 + 2r_2) = 3 + 4r_2$.

- Let us consider congruences modulo 2^6. As $7^1 \neq -9 \bmod 2^6$ and the order of 7 in $\mathbb{Z}/2^6\mathbb{Z}$ is 8, then $r = 3 + 4r_2 = 3 + 2(1 + 2r_3) = 7 + 8r_3$.

- Let us take congruences modulo 2^7. As $7^1 \neq -9 \bmod 2^7$ and the order of 7 in $\mathbb{Z}/2^7\mathbb{Z}$ is 16, then $r = 7 + 8r_3 = 7 + 8(1 + 2r_4) = 15 + 16r_4$.

- Finally let us consider congruences modulo 17. Using that $7^{16} = 1 \bmod 17$, we have

  $$2^k = 7^r + 9 = 7^{15+16r_4} + 9 = 7^{15} + 9 = 5 + 9 = 14 \bmod 17\,.$$

  However, no power of 2 is equal to 14 modulo 17 (see Lemma 5.2).

If $j = 4$, we have $15^r = -17 \bmod 2^5$. We use the same procedure as for $j = 3$.

- First we have $15^1 \neq -17 \bmod 2^i$ for $i = 6, 7, 8, 9, 10, 11, 12$.

- In $\mathbb{Z}/2^i\mathbb{Z}$, for $i = 5, 6, 7, 8, 9, 10, 11, 12$, the order of 15 is respectively $2, 4, 8, 16, 32, 64, 128, 256$ implying that $r = 255 + 256r'$.

- Then, using that $15^{256} = 1 \bmod 257$, we have

  $$2^k = 15^r + 17 = 15^{255+256r'} + 17 = 15^{255} + 17 = 120 + 17 = 137 \bmod 257\,.$$

  However, no power of 2 is equal to 137 modulo 257 (see Lemma 5.2).

If $j = 5$, we have $31^r = -33 \bmod 2^6$. We use the same procedure as for $j = 3$.

- First we have $31^1 \neq -33 \bmod 2^i$ for $i = 7, 8, 9, 10, 11$.

- In $\mathbb{Z}/2^i\mathbb{Z}$, for $i = 6, 7, 8, 9, 10, 11$, the order of 31 is respectively $2, 4, 8, 16, 32, 64$ implying that $r = 63 + 64r'$.

- Then, using that $31^{64} = 1 \bmod 65$, we have

  $$2^k = 31^r + 33 = 31^{63+64r'} + 33 = 31^{63} + 33 = 21 + 33 = 54 \bmod 65\,.$$

  However, no power of 2 is equal to 54 modulo 65 (see Lemma 5.2).

If $j = 6$, we have $63^r = -65 \bmod 2^7$. We use the same procedure as for $j = 3$.

- First we have $63^1 \neq -65 \bmod 2^i$ for $i = 8, 9, 10, 11, 12, 13, 14$.

- In $\mathbb{Z}/2^i\mathbb{Z}$, for $i = 7, 8, 9, 10, 11, 12, 13, 14$, the order of 63 is respectively $2, 4, 8, 16, 32, 64, 128, 256$ implying that $r = 255 + 256r'$.

- Then, using that $63^{256} = 1 \bmod 257$, we have

  $$2^k = 63^r + 65 = 63^{255+256r'} + 65 = 63^{255} + 65 = 102 + 65 = 167 \bmod 257\,.$$

  However, no power of 2 is equal to 167 modulo 257 (see Lemma 5.2).

If $j = 7$, we have $127^r = -129 \bmod 2^8$. We use the same procedure as for $j = 3$.

- First we have $127^1 \neq -129 \bmod 2^i$ for $i = 9, 10, 11, 12, 13, 14, 15$.

- In $\mathbb{Z}/2^i\mathbb{Z}$, for $i = 8, 9, 10, 11, 12, 13, 14, 15$, the order of 127 is respectively $2, 4, 8, 16, 32, 64, 128, 256$ implying that $r = 255 + 256r'$.
- Then, using that $127^{256} = 1 \bmod 257$, we have

$$2^k = 127^r + 129 = 127^{255+256r'} + 129 = 127^{255} + 129 = 85 + 129 = 214 \bmod 257\,.$$

However, no power of 2 is equal to 214 modulo 257 (see Lemma 5.2).

□

Proposition 5.12. *Let $d = 2^j - 1$, such that $2 \leqslant j \leqslant 7$. Then if $k_{d,r} = 0 \bmod j$, we have:*

$$2^{k_{d,r}+1} - 2^j - 1 > d^r\,,$$

where $r > 4$ if $d = 3$ and $r > 1$ otherwise.

Proof. Proposition 5.9 shows that the results holds for $j = 2$ i.e. $d = 3$. Then for $j \geqslant 3$, let us notice that it is sufficient to show that d^r is neither equal to $2^{k_{d,r}+1} - 2^j - 1$ nor to $2^{k_{d,r}+1} - 2$, since any integer $2^{k_{d,r}+1} - 2^i - 1$, where $i \not\equiv 0 \bmod j$ is not divisible by d. Then $2^{k_{d,r}+1} - 2$ is even, while d^r is odd, implying that d^r is not equal to $2^{k_{d,r}+1} - 2$. Finally, Lemma 5.7 shows that the equation $2^{k_{d,r}+1} - 2^j - 1 > d^r$ has no solution for $r > 1$. □

Corollary 5.3. *Let $d = 2^j - 1$, such that $2 \leqslant j \leqslant 7$. Then, we have*

$$B_d^r \leqslant \begin{cases} k_{d,r} - j & \textit{if } b_{7,r} = 0\,, \\ k_{d,r} - (k_{d,r} \bmod j) & \textit{otherwise}\,. \end{cases}$$

Proof. If $k_{d,r} \neq 0 \bmod j$ then we have Proposition 5.11. Now let us assume that $k_{d,r} = 0 \bmod j$. Our aim is to prove that no exponent of Hamming weight $\omega \geqslant k_{d,r} - j'$ where $j' < j$ can appear at round r when $k_{d,r} = 0 \bmod j$. Let

$$e = 2^{k_{d,r}+1} - \sum_{\ell=1}^{j'} 2^{i_\ell} - 1\,.$$

First if $j' = 1$, then we know that if $i_1 \leqslant j$ then $e = 2^{k_{d,r}+1} - 2^{i_1} - 1 > d^r$ so it does not belong to $\mathcal{E}_{d,r}$. And if $i_1 \geqslant j + 1$, then $e \equiv 2^{j+1} - 1 \bmod 2^{j+1}$ that does not belong to $\mathcal{E}_{d,r}$ according to Proposition 5.7.

Then let us take $j' \geqslant 2$ and let

$$e = 2^{k_{d,r}+1} - \sum_{\lambda \in J_1} 2^\lambda - \sum_{\lambda \in J_2} 2^\lambda - 1\,,$$

where J_1 and J_2 are sets such that

$$J_1 = \{i_\ell, 1 \leqslant \ell \leqslant j', i_\ell \leqslant j\} \quad \text{and} \quad J_2 = \{i_\ell, 1 \leqslant \ell \leqslant j', i_\ell \geqslant j + 1\}\,.$$

First let us observe that if J_1 is empty then $e \equiv 2^{j+1} - 1 \bmod 2^{j+1}$ so $e \notin \mathcal{E}_{d,r}$. More precisely, J_1 needs to contain at least 0 or j, otherwise e is a missing exponent. Indeed, if both 0 and j are missing, and since

$$e \equiv 2^{k_{d,r}+1} - \sum_{\lambda \in J_1} 2^\lambda - \sum_{\lambda \in J_2} 2^\lambda - 1 \equiv 2^{j+1} - \sum_{\lambda \in J_1} 2^\lambda - 1 \mod 2^{j+1}\,,$$

then we have

$$e \bmod 2^{j+1} \equiv 2^j + \sum_{i=1}^{j-1} \varepsilon_i 2^i, +1 \ \text{ where } \varepsilon_i = 0\,,\ \text{if } i \in J_1\,,\ \text{and } \varepsilon_i = 1\,,\ \text{if } i \notin J_1\,,$$

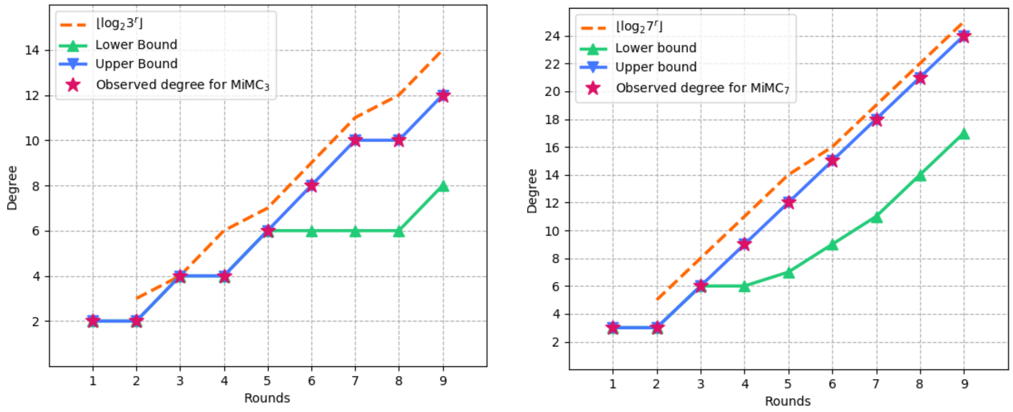
which exactly corresponds to missing exponents according to Proposition 5.7 i.e. exponents of the form $2^j + 2\gamma + 1$ for $\gamma \in \{1, \ldots, 2^{j-1} - 1\}$.

As a consequence, we have

$$e = 2^{k_{d,r}+1} - \sum_{\lambda \in (J_1 \cup J_2) \setminus \{0 \text{ or } j\}} 2^\lambda - 2 \equiv - \sum_{\lambda \in (J_1 \cup J_2) \setminus \{0 \text{ or } j\}} 2^\lambda \bmod (2^j - 1)\,.$$

Then e has a sum of $j' - 1$ powers of 2, distinct from each other, meaning that we cannot get a multiple of $2^j - 1$: $\mathrm{wt}\left(\sum_{\lambda \in (J_1 \cup J_2) \setminus \{0 \text{ or } j\}} 2^\lambda \bmod 2^j - 1\right) = j' - 1 < j$. □

In Figure 5.11a for MiMC$_3$ and in Figure 5.11b for MiMC$_7$ we can see that the bound from Corollary 5.3 exactly corresponds to the observed degree for small instances of MiMC$_d$ with $d = 2^j - 1$.



(a) MiMC$_3$. ***(b)*** MiMC$_7$.

Figure 5.11: *Comparison between our bounds and the exact degree of* MiMC$_d$, $d = 2^j - 1$.

5.4 On the Algebraic Degree of MiMC$_3^{-1}$

In Section 5.3 we derived bounds on the algebraic degree of some instances of MiMC$_d$ thanks to the specific univariate representation of the transformation. We are now interested in the algebraic degree of the inverse transformation. MiMC$_3^{-1}$ is obtained by reversing the order of the round constants and by replacing the round function by $F^{-1}(x) = x^s$ where

$$s = \frac{2^{n+1} - 1}{3} = \sum_{i=0}^{(n-1)/2} 2^{2i}$$

(see e.g. [Nyb94, Prop. 5]).

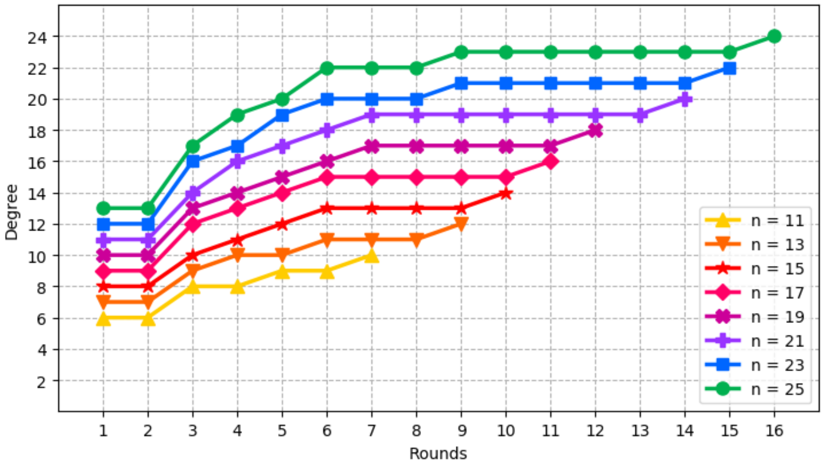


Figure 5.12: *Observed algebraic degree of* MiMC_3^{-1}.

In Figure 5.12, that has also been derived from a C implementation of Corollary 5.1 for various instances of MiMC_3^{-1}, we observe two significant facts, on which we will focus:

1. Whatever the extension degree is, there is a plateau between the first two rounds (see Section 5.4.1).

2. The degree grows rapidly up to $n-2$ and then there is a large plateau that increases with the size of the field on the last rounds (see Section 5.4.2).

5.4.1 A Plateau Between Rounds 1 and 2

Given that the algebraic degree of the round function of MiMC_3^{-1} is already high in the first round, we would a priori expect an explosion of the degree in the second round rather than a plateau. In this subsection, we will see that this event is due to the particular shape of the exponent $s = (2^{n+1}-1)/3$ which has active bits only in even position.

Our aim is to prove Proposition 5.13 that gives bounds on the Hamming weight of integers js, depending in the Hamming weight of j. Interestingly, our approach is closely related to Jacobsthal numbers, i.e. the sequence $\{J_n\}_{n\geqslant 0}$ satisfying the following property:

$$J_0 = 0, \;\; J_{n+1} = 2^n - J_n \;, \;\; \text{implying that } J_n = \frac{2^n - (-1)^n}{3} \;.$$

Although the link with Jacobsthal numbers is worth mentioning, we have chosen not to use it in the following since we did not feel that it simplified the computations.

Let us introduce some notation. If i and k are even integers such that $i \leqslant k$, then

$$\mathcal{E}_i^k \text{ is the sum of Even powers of 2, so that } \quad \mathcal{E}_i^k = \sum_{\ell=i/2}^{k/2} 2^{2\ell}\,.$$

$$\mathcal{O}_i^k \text{ is the sum of Odd powers of 2, so that } \quad \mathcal{O}_i^k = \sum_{\ell=i/2}^{k/2} 2^{2\ell+1}\,.$$

$$\mathcal{A}_i^k \text{ is the sum of All powers of 2, so that } \quad \mathcal{A}_i^k = \sum_{\ell=i}^{k} 2^{\ell}\,.$$

The sums $\mathcal{E}_i^k$, $\mathcal{O}_i^k$ and $\mathcal{A}_i^k$ satisfy some interesting properties.

Lemma 5.8. *Let i be an integer, and s the inverse of 3 modulo $2^n - 1$, then we have*

$$2^i s \bmod (2^n-1) \equiv \begin{cases} \mathcal{O}_0^{i-2} + \mathcal{E}_i^{n-1} & \textit{if } i = 0 \bmod 2\,, \\ \mathcal{E}_0^{i-1} + \mathcal{O}_{i-1}^{n-3} & \textit{if } i = 1 \bmod 2\,. \end{cases}$$

Proof. First let us notice that

$$s = \sum_{\ell=0}^{(n-1)/2} 2^{2\ell} = \mathcal{E}_0^{n-1}\,.$$

This implies that if i is even, then

$$2^i \times s = \sum_{\ell=0}^{(n-1)/2} 2^{2\ell+i} \equiv \sum_{\ell=0}^{(i-2)/2} 2^{2\ell+1} + \sum_{\ell=i/2}^{(n-1)/2} 2^{2\ell} \bmod (2^n-1)\,,$$

and if i is odd then

$$2^i \times s = \sum_{\ell=0}^{(n-1)/2} 2^{2\ell+i} \equiv \sum_{\ell=0}^{(i-1)/2} 2^{2\ell} + \sum_{\ell=(i-1)/2}^{(n-3)/2} 2^{2\ell+1} \bmod (2^n-1)\,.$$

□

Lemma 5.9. *Let i, k, m be even integers such that $i \leqslant k \leqslant m$, then we have the following relations*

(i) $2\mathcal{E}_i^k = \mathcal{O}_i^k$,

(ii) $2\mathcal{O}_i^k = \mathcal{E}_{i+2}^{k+2}$,

(iii) $\mathcal{A}_i^{k+1} = \mathcal{E}_i^k + \mathcal{O}_i^k$ *and* $\mathcal{A}_i^k = \mathcal{E}_i^k + \mathcal{O}_i^{k-2}$,

(iv) $2^i + \mathcal{A}_i^k = 2^{k+1}$,

(v) $2^i + \mathcal{E}_i^{k-2} + \mathcal{O}_i^m = 2^k + \mathcal{O}_k^m$,

(vi) $2^{i-1} + \mathcal{O}_{i-2}^{k-2} + \mathcal{E}_i^m = 2^{k+1} + \mathcal{E}_{k+2}^m$.

Proof. **(i)** and **(ii)** directly follow from the definition of $\mathcal{E}$ and $\mathcal{O}$:

$$2\mathcal{E}_i^k = 2\sum_{\ell=i/2}^{k/2} 2^{2\ell} = \sum_{\ell=i/2}^{k/2} 2^{2\ell+1} = \mathcal{O}_i^k$$
$$2\mathcal{O}_i^k = 2\sum_{\ell=i/2}^{k/2} 2^{2\ell+1} = \sum_{\ell=(i+2)/2}^{(k+2)/2} 2^{2\ell} = \mathcal{E}_{i+2}^{k+2}\,.$$

Then, as $\mathcal{E}_i^k$ covers only even powers with last element 2^k, and $\mathcal{O}_i^k$ odd powers with last element 2^{k+1}, we get **(iii)**:

$$\begin{aligned}\mathcal{A}_i^{k+1} &= \mathcal{E}_i^k + \mathcal{O}_i^k \\ \mathcal{A}_i^k &= \mathcal{A}_i^{k+1} - 2^{k+1} = \mathcal{E}_i^k + \mathcal{O}_i^{k-2}\,.\end{aligned}$$

(iv) also comes from the definition of $\mathcal{A}_i^k$, since a carry starting on the first column of an all-one vector propagates until the end.

$$2^i + \mathcal{A}_i^k = 2^{k+1}\,.$$

As a consequence we obtain **(v)**:

$$\begin{aligned}2^i + \mathcal{E}_i^{k-2} + \mathcal{O}_i^m &= 2^i + \mathcal{E}_i^{k-2} + \mathcal{O}_i^{k-2} + \mathcal{O}_k^m \\ &= 2^i + \mathcal{A}_i^{k-1} + \mathcal{O}_k^m && \text{by (iii)} \\ &= 2^k + \mathcal{O}_k^m && \text{by (iv)},\end{aligned}$$

and **(vi)**:

$$\begin{aligned}2^{i-1} + \mathcal{O}_{i-2}^{k-2} + \mathcal{E}_i^m &= 2^{i-1} + 2^{i-1} + \mathcal{O}_i^{k-2} + \mathcal{E}_i^k + \mathcal{E}_{k+2}^m \\ &= 2^i + \mathcal{A}_i^k + \mathcal{E}_{k+2}^m && \text{by (iii)} \\ &= 2^{k+1} + \mathcal{E}_{k+2}^m && \text{by (iv)}.\end{aligned}$$

□

Lemma 5.10. *Let i and k be even integers, then we have*

$$\mathrm{wt}\left(\mathcal{E}_i^k\right) = \mathrm{wt}\left(\mathcal{O}_i^k\right) = (k-i+2)/2\,.$$

Proof. $\mathcal{E}_i^k$ covers the interval between i and k with exactly one bit over two being 1, so

$$\mathrm{wt}\left(\mathcal{E}_i^k\right) = (k-i)/2 + 1 = (k-i+2)/2\,.$$

Then it follows that

$$\mathrm{wt}\left(\mathcal{O}_i^k\right) = \mathrm{wt}\left(2\cdot\mathcal{E}_i^k\right) = \mathrm{wt}\left(\mathcal{E}_i^k\right) = (k-i+2)/2\,.$$

□

In the following we will see that the Hamming weight of sj depends on the value of j modulo 3. Then to build an inductive proof we will rely on the following remark that gives the representation of sj modulo $2^n - 1$ when j is of Hamming weight 3.

Remark 5.3. Let us observe that for any triple of even integers $0 \leqslant i_0 < i_1 < i_2 < n$:

$$\mathcal{S}_3 = 2^{i_0} + \mathcal{O}_{i_0}^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} \equiv s(2^{i_0} + 2^{i_1} + 2^{i_2}) \bmod (2^n - 1) \ .$$

Indeed we can check that

$$\begin{aligned} 3 \times \mathcal{S}_3 &= 3 \times \left(2^{i_0} + \mathcal{O}_{i_0}^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2}\right) \\ &= 2^{i_0} + 2^{i_0+1} + \mathcal{O}_{i_0}^{i_1-2} + \mathcal{E}_{i_0+2}^{i_1} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{O}_{i_1}^{i_2-2} \\ &= 2^{i_0} + 2^{i_0+1} + \mathcal{A}_{i_0+1}^{i_1-1} + 2^{i_1} + \mathcal{A}_{i_1}^{i_2-1} \\ &= 2^{i_0} + 2^{i_0+1} + \mathcal{A}_{i_0+1}^{i_1-1} + 2^{i_2} \\ &= 2^{i_0} + 2^{i_0+1} + (2^{i_1} - 2^{i_0+1}) + 2^{i_2} \\ &= 2^{i_0} + 2^{i_1} + 2^{i_2} \ . \end{aligned}$$

Proposition 5.13. *Let $j \preceq s$. Then for all j such that $\mathrm{wt}(j) \geqslant 2$, we have:*

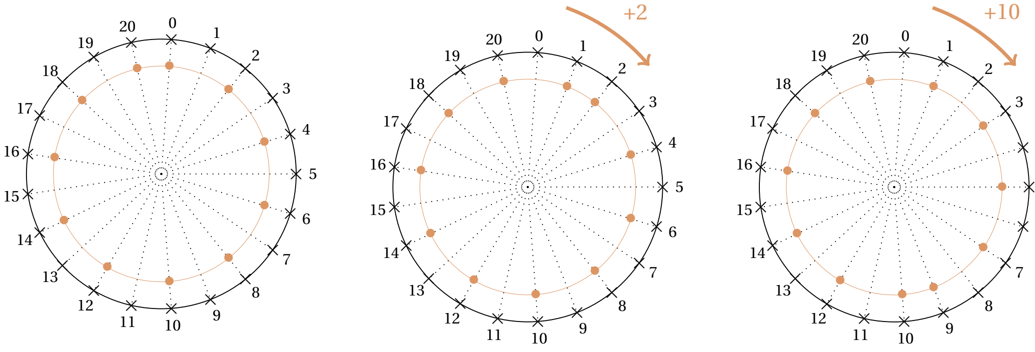
$$\mathrm{wt}(js \bmod 2^n - 1) \in \begin{cases} \llbracket \mathrm{wt}(j) - 1, (n-1)/2 \rrbracket \ \textit{if} \ \mathrm{wt}(j) \equiv 2 \bmod 3 \ , \\ \llbracket \mathrm{wt}(j), (n+1)/2 \rrbracket \ \textit{if} \ \mathrm{wt}(j) \equiv 0, 1 \bmod 3 \ . \end{cases}$$

Let us consider some examples before giving the proof. We propose one example for each value of $\mathrm{wt}(j)$ modulo 3.

Example 5.2 ($\mathrm{wt}(j) \equiv 2 \bmod 3$). Let $n = 21$, we have

$$s = (2^{n+1} - 1)/3 = \sum_{\ell=0}^{10} 2^{2\ell} = \mathcal{E}_0^{20} = 1398101 \ .$$

Let $j = 2^2 + 2^{10} = 1028$, we have $\mathrm{wt}(j) = 2$. We will construct $sj \bmod (2^n - 1)$ step by step and illustrate the construction with figures. Indeed, this computation can also be seen with circles to visualize the mechanics behind it. Multiplying s by a power of 2 means rotating the active powers of 2 around a circle representing all the powers of 2 up to $2^n - 1$, as shown on Figure 5.13.



(a) s

(b) $2^2 s$

(c) $2^{10} s$

Figure 5.13: *Bit representation of s and rotation.*

Then on Figure 5.13b the circle is shifted by two nodes to represent $2^2 s$ and on Figure 5.13c it is shifted by ten nodes to represent $2^{10} s$. We will show the different steps to build $sj \bmod (2^n - 1)$

on Figure 5.14, where we construct the result of the sum of $2^2 s$ and $2^{10} s$ in the central circle. We have

$$\begin{aligned} sj &= 2^2 \mathcal{E}_0^{20} + 2^{10} \mathcal{E}_0^{20} \\ &= 2 + \mathcal{E}_2^{20} + \mathcal{O}_0^{8} + \mathcal{E}_{10}^{20} \,. \end{aligned}$$

This is the first step in Figure 5.14, where we have one circle for $2 + \mathcal{E}_2^{20}$, one for $\mathcal{O}_0^8 + \mathcal{E}_{10}^{20}$. Then, we have

$$\begin{aligned} sj &= 2 + \mathcal{E}_2^{8} + \mathcal{O}_0^{8} + 2 \cdot \mathcal{E}_{10}^{20} \\ &= 2 + \mathcal{E}_2^{8} + \mathcal{O}_0^{8} + \mathcal{O}_{10}^{20} \\ &= 1 + 2 + \mathcal{E}_2^{8} + \mathcal{O}_0^{8} + \mathcal{O}_{10}^{18} \,. \end{aligned}$$

This is the second step in Figure 5.14, where the central circle stores the value $1 + \mathcal{O}_{10}^{18}$. We let the other values on their initial circles to better see the evolution. Finally, we have

$$\begin{aligned} sj &= 1 + 2 + \mathcal{A}_1^{9} + \mathcal{O}_{10}^{18} \\ &= 1 + 2^{10} + \mathcal{O}_{10}^{18} \,. \end{aligned}$$

This is the third step in Figure 5.14. It follows that

$$sj = 1 + 2^{10} + \sum_{\ell=5}^{9} 2^{2\ell+1} = 699393 \bmod 2^{21} - 1 \,,$$

implying that $\mathrm{wt}(sj) = 7 \in [\![1, 10]\!]$.

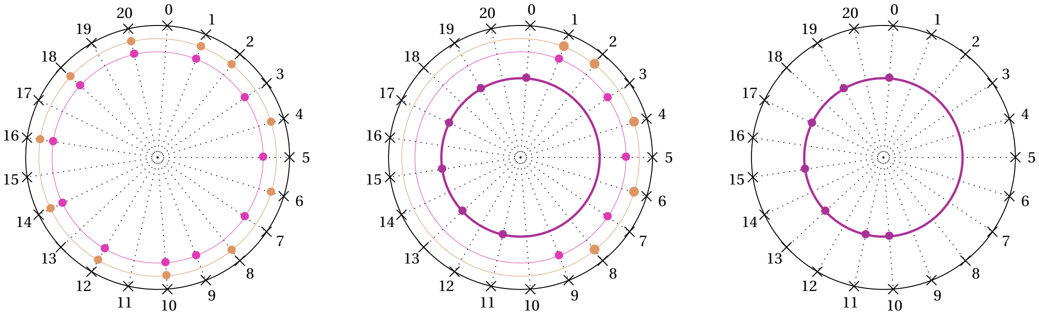


Figure 5.14: *Bit representation of sj when $j = 2^2 + 2^{10}$.*

Example 5.3 ($\mathrm{wt}(j) \equiv 0 \bmod 3$)**.** Let again $n = 21$, and $s = \mathcal{E}_0^{20} = 1398101$. Let $j = 2^4 + 2^{12} + 2^{20} = 1052688$, we have $\mathrm{wt}(j) = 3$. We will show the different steps to build $sj \bmod (2^n - 1)$ on Figure 5.15 where we construct the result in the central circle. Let us notice that this example also illustrates Remark 5.3. We have

$$\begin{aligned} sj &= 2^4 \mathcal{E}_0^{20} + 2^{12} \mathcal{E}_0^{20} + 2^{20} \mathcal{E}_0^{20} \\ &= \mathcal{O}_0^{2} + \mathcal{E}_4^{20} + \mathcal{O}_0^{10} + \mathcal{E}_{12}^{20} + \mathcal{O}_0^{18} + 2^{20} \,. \end{aligned}$$

This is the first step in Figure 5.15 where we have one circle for $\mathcal{O}_0^2 + \mathcal{E}_4^{20}$, one for $\mathcal{O}_0^{10} + \mathcal{E}_{12}^{20}$ and one for $\mathcal{O}_0^{18} + 2^{20}$. Then, we have

$$\begin{aligned} sj &= 3 \cdot \mathcal{O}_0^2 + \mathcal{E}_4^{18} + \mathcal{O}_4^{10} + \mathcal{E}_{12}^{18} + \mathcal{O}_4^{18} + 3 \cdot 2^{20} \\ &= \mathcal{A}_0^4 + \mathcal{E}_4^{18} + \mathcal{O}_4^{10} + \mathcal{E}_{12}^{18} + \mathcal{O}_4^{18} + 2^{20} \,. \end{aligned}$$

This is the second step in Figure 5.15 where the central circle stores the value $\mathcal{A}_0^4 + 2^{20}$. We again let the other values on their initial circles to better understand the evolution. Then, we have

$$\begin{aligned} sj &= \mathcal{A}_0^4 + \mathcal{E}_4^{10} + 2 \cdot \mathcal{O}_4^{10} + 2 \cdot \mathcal{E}_{12}^{18} + \mathcal{O}_{12}^{18} + 2^{20} \\ &= \mathcal{A}_0^4 + \mathcal{E}_4^{10} + \mathcal{E}_6^{12} + 2 \cdot \mathcal{E}_{12}^{18} + \mathcal{O}_{12}^{18} + 2^{20} \\ &= \mathcal{A}_0^3 + \mathcal{O}_4^{10} + 2^{12} + 2 \cdot \mathcal{E}_{12}^{18} + \mathcal{O}_{12}^{18} + 2^{20} \,. \end{aligned}$$

This is the third step in Figure 5.15 where the central circle stores the value $\mathcal{A}_0^3 + \mathcal{O}_4^{10} + 2^{12} + 2^{20}$. Finally, we have

$$\begin{aligned} sj &= \mathcal{A}_0^3 + \mathcal{O}_4^{10} + 2^{12} + \mathcal{O}_{12}^{18} + \mathcal{O}_{12}^{18} + 2^{20} \\ &= \mathcal{A}_0^3 + \mathcal{O}_4^{10} + 2^{12} + \mathcal{E}_{14}^{18} + 2 \cdot 2^{20} \\ &= 2^4 + \mathcal{O}_4^{10} + \mathcal{E}_{12}^{18} \,. \end{aligned}$$

This is the fourth step in Figure 5.15. It follows that

$$sj = 2^4 + \sum_{\ell=2}^{5} 2^{2\ell+1} + \sum_{\ell=6}^{9} 2^{2\ell} = 350896 \bmod 2^{21} - 1 \,,$$

implying that $\mathrm{wt}(sj) = 9 \in [\![3, 11]\!]$.

Example 5.4 ($\mathrm{wt}(j) \equiv 1 \bmod 3$). Let again $n = 21$, and $s = \mathcal{E}_0^{20} = 1398101$. Let $j = 1 + 2^6 + 2^{14} + 2^{18} = 278593$, we have $\mathrm{wt}(j) = 4$. We will show the different steps to build $sj \bmod (2^n - 1)$ on Figure 5.16. We have

$$\begin{aligned} sj &= \mathcal{E}_0^{20} + 2^6 \mathcal{E}_0^{20} + 2^{14} \mathcal{E}_0^{20} + 2^{18} \mathcal{E}_0^{20} \\ &= \mathcal{E}_0^{20} + \mathcal{O}_0^4 + \mathcal{E}_6^{20} + \mathcal{O}_0^{12} + \mathcal{E}_{14}^{20} + \mathcal{O}_0^{16} + \mathcal{E}_{18}^{20} \,. \end{aligned}$$

This is the first step in Figure 5.16 where we have one circle for $\mathcal{E}_0^{20}$, one for $\mathcal{O}_0^4 + \mathcal{E}_6^{20}$, one for $\mathcal{O}_0^{12} + \mathcal{E}_{14}^{20}$ and one for $\mathcal{O}_0^{16} + \mathcal{E}_{18}^{20}$. Then, we have

$$\begin{aligned} sj &= \mathcal{E}_0^{16} + \mathcal{O}_0^4 + \mathcal{E}_6^{16} + \mathcal{O}_0^{12} + \mathcal{E}_{14}^{16} + \mathcal{O}_0^{16} + 4 \cdot \mathcal{E}_{18}^{20} \\ &= 2 + \mathcal{E}_0^{16} + 3 \cdot \mathcal{O}_0^4 + \mathcal{E}_6^{16} + \mathcal{O}_6^{12} + \mathcal{E}_{14}^{16} + \mathcal{O}_6^{16} + 2^{20} \,. \end{aligned}$$

This is the second step in Figure 5.16 where the central circle stores the value $2 + 2^{20}$, keeping the other values on their initial circles. Then, we have

$$\begin{aligned} sj &= 2 + \mathcal{E}_0^4 + \mathcal{A}_1^6 + 2 \cdot \mathcal{E}_6^{12} + 2 \cdot \mathcal{O}_6^{12} + 3 \cdot \mathcal{E}_{14}^{16} + \mathcal{O}_{14}^{16} + 2^{20} \\ &= \mathcal{E}_0^4 + 2^7 + 2 \cdot \mathcal{E}_6^{12} + 2 \cdot \mathcal{O}_6^{12} + 3 \cdot \mathcal{E}_{14}^{16} + \mathcal{O}_{14}^{16} + 2^{20} \,. \end{aligned}$$

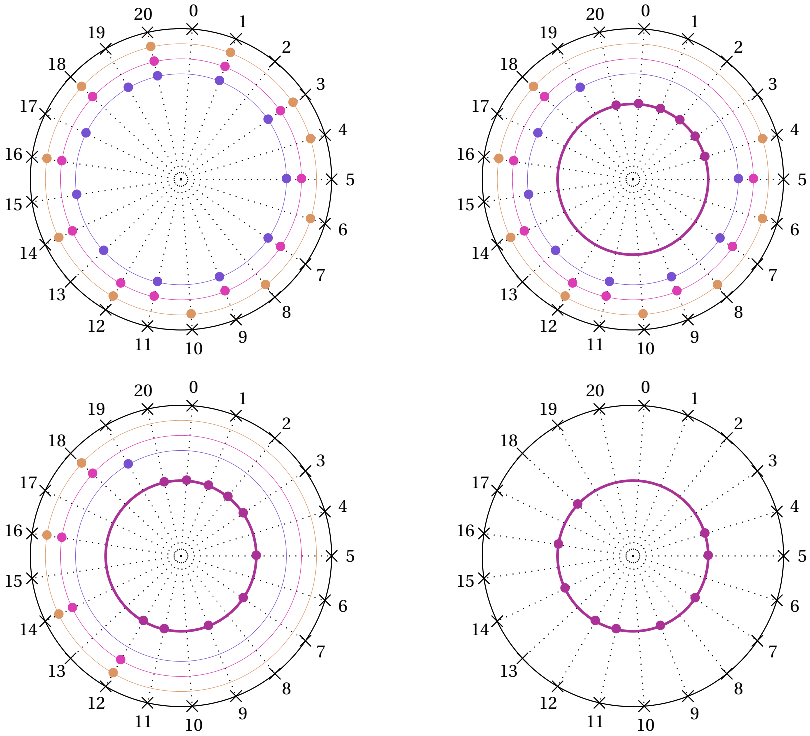


Figure 5.15: *Bit representation of* sj *when* $j = 2^4 + 2^{12} + 2^{20}$.

This is the third step in Figure 5.16 where the central circle stores the value $\mathcal{E}_0^4 + 2^7 + 2^{20}$. Finally, we have

$$\begin{aligned} sj &= \mathcal{E}_0^4 + 2^7 + 2 \cdot \mathcal{E}_6^{12} + 2 \cdot \mathcal{O}_6^{12} + 3 \cdot \mathcal{E}_{14}^{16} + \mathcal{O}_{14}^{16} + 2^{20} \\ &= \mathcal{E}_0^4 + 2^7 + \mathcal{O}_6^{12} + \mathcal{E}_8^{14} + \mathcal{A}_{14}^{17} + \mathcal{O}_{14}^{16} + 2^{20} \\ &= \mathcal{E}_0^4 + 2^{15} + \mathcal{A}_{14}^{17} + \mathcal{O}_{14}^{16} + 2^{20} \\ &= \mathcal{E}_0^4 + 2^{14} + \mathcal{O}_{14}^{16} + \mathcal{E}_{18}^{20} \; . \end{aligned}$$

This is the fourth step in Figure 5.16. It follows that

$$sj = \sum_{\ell=0}^{2} 2^{2\ell} + 2^{14} + 2^{15} + 2^{17} + \sum_{\ell=9}^{10} 2^{2\ell} = 1490965 \bmod 2^{21} - 1 \,,$$

implying that $\mathrm{wt}(sj) = 8 \in [\![4, 11]\!]$.

Proof of Proposition 5.13. Throughout this proof we will use the notation σ_n to represent $sj \bmod (2^n - 1)$. We will investigate three different cases, depending on the value of $\mathrm{wt}(j) \bmod 3$. Our starting points for the inductions will be $\mathrm{wt}(j) \in \{2, 3, 4\}$. So we will start by proving the result for the case $\mathrm{wt}(j) \equiv 2 \bmod 3$, then we will deal with the case $\mathrm{wt}(j) \equiv 0 \bmod 3$, and we will finish by the case $\mathrm{wt}(j) \equiv 1 \bmod 3$. In what follows all computations are modulo $(2^n - 1)$, with n odd.

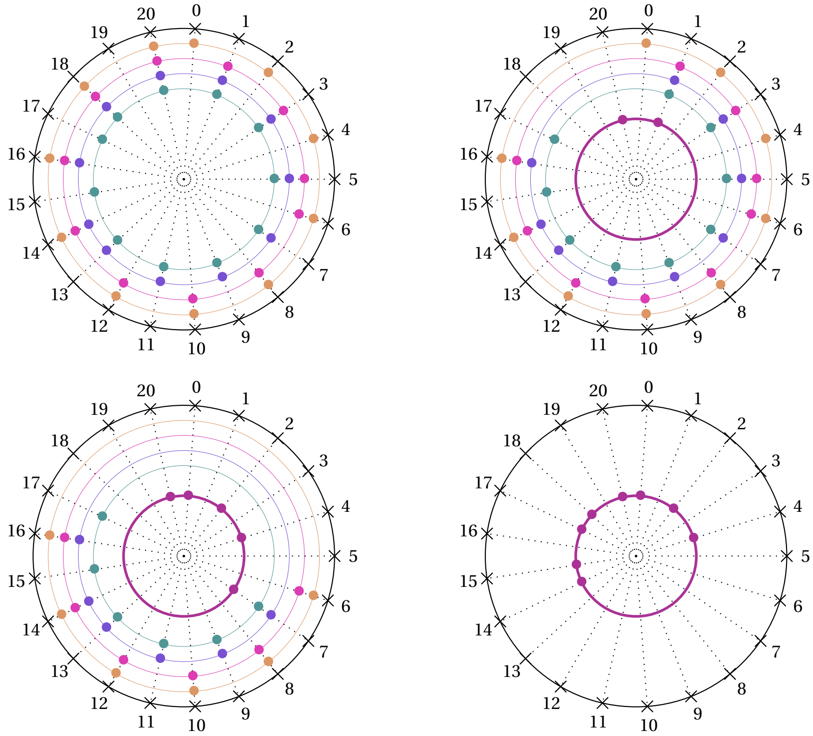


Figure 5.16: *Bit representation of sj when $j = 1 + 2^6 + 2^{14} + 2^{18}$.*

(a) First, let us take an integer j such that $\mathrm{wt}(j) \equiv 2 \bmod 3$. As a preliminary observation, let $j = 2^{i_0} + 2^{i_1}$ where $0 \leqslant i_0 < i_1 < n$, so we have $\mathrm{wt}(j) = 2$. Both i_0 and i_1 are even, since by assumption $j \preceq s$. Then,

$$
\begin{aligned}
s(2^{i_0} + 2^{i_1}) &= \sum_{\ell=0}^{(n-1)/2} 2^{2\ell+i_0} + \sum_{\ell=0}^{(n-1)/2} 2^{2\ell+i_1} \\
&= \mathcal{E}_{i_0}^{n-1+i_0} + \mathcal{E}_{i_1}^{n-1+i_1} \\
&= \mathcal{E}_{i_0}^{i_1-2} + 2\mathcal{E}_{i_1}^{n-1+i_0} + \mathcal{E}_{n+1+i_0}^{n-1+i_1} \\
&= \mathcal{E}_{i_0}^{i_1-2} + \mathcal{O}_{i_1}^{n-1+i_0} + \mathcal{E}_{n+1+i_0}^{n-1+i_1} \\
&= \mathcal{E}_{i_0}^{i_1-2} + \mathcal{O}_{i_1}^{n-3} + \mathcal{E}_{0}^{i_0} + \mathcal{O}_{i_0}^{i_1-2} \,,
\end{aligned}
$$

implying that if $i_0 = 0$ then

$$
\sigma_n = \mathcal{E}_0^{i_1-2} + \mathcal{O}_{i_1}^{n-3} + 1 + \mathcal{O}_0^{i_1-2} = 1 + \mathcal{A}_0^{i_1-1} + \mathcal{O}_{i_1}^{n-3}
$$

so that

$$
\sigma_n = 2^{i_1} + \mathcal{O}_{i_1}^{n-3} \,. \tag{5.4}
$$

If $i_0 \neq 0$, we have

$$\begin{aligned}\sigma_n &= \mathcal{E}_0^{i_0-2} + 2^{i_0} + \mathcal{A}_{i_0}^{i_1-1} + \mathcal{O}_{i_1}^{n-3} \\ &= \mathcal{E}_0^{i_0-2} + 2^{i_1} + \mathcal{O}_{i_1}^{n-3} .\end{aligned}$$

Then, it follows that if $i_0 = 0$

$$\begin{aligned}\mathrm{wt}(\sigma_n) &= 1 + ((n-3)/2 - i_1/2 + 1) , \\ &= (n - i_1 + 1)/2 ,\end{aligned}$$

and

$$\begin{aligned}\mathrm{wt}(\sigma_n) &= (i_0/2 - 1 + 1) + 1 + ((n-3)/2 - i_1/2 + 1) , \\ &= (n + i_0 - i_1 + 1)/2 ,\end{aligned}$$

otherwise. Now, we let $\mathrm{wt}(j) = 2 + 3k$ and $j = \sum_{m=0}^{3k+1} 2^{i_m}$, where $k > 1$ and the i_m are even since $j \preceq s$, with $0 \leqslant i_0 < \ldots < i_{3k+1} < n$. Then let us show that:

$$\sigma_n = \mathcal{S} + \sum_{m=1}^{k} \left(\mathcal{O}_{i_{3m-2}}^{i_{3m-1}-2} + \mathcal{E}_{i_{3m-1}}^{i_{3m}-2} + 2^{i_{3m+1}} \right) + \mathcal{O}_{i_{3k+1}}^{n-3} , \tag{5.5}$$

where

$$\mathcal{S} = \begin{cases} 2^{i_1} & \text{if } i_0 = 0 , \\ \mathcal{E}_0^{i_0-2} + 2^{i_1} & \text{otherwise} , \end{cases}$$

We prove it by induction on k.

- **For $k = 1$:** Let $j = 2^{i_0} + 2^{i_1} + 2^{i_2} + 2^{i_3} + 2^{i_4}$, where $0 \leqslant i_0 < i_1 < i_2 < i_3 < i_4 < n$, we have $\mathrm{wt}(j) = 5$. Then, by using Remark 5.3, we have

$$\begin{aligned}\sigma_n &= s(2^{i_0} + 2^{i_1}) + s(2^{i_2} + 2^{i_3} + 2^{i_4}) \\ &= \mathcal{S} + \mathcal{O}_{i_1}^{n-3} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{i_4-2} \\ &= \mathcal{S} + \mathcal{O}_{i_1}^{i_2-2} + 2^{i_2} + 2 \cdot \mathcal{O}_{i_2}^{i_3-2} + \mathcal{O}_{i_3}^{n-3} + \mathcal{E}_{i_3}^{i_4-2} \\ &= \mathcal{S} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-2} + 2^{i_3} + \mathcal{A}_{i_3}^{i_4-1} + \mathcal{O}_{i_4}^{n-3} .\end{aligned}$$

  Finally we get

$$\sigma_n = \mathcal{S} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-2} + 2^{i_4} + \mathcal{O}_{i_4}^{n-3} .$$

- **Induction step.** Let us assume that the property holds for k, i.e., for any $j_k = \sum_{m=0}^{3k+1} 2^{i_m}$ such that $\mathrm{wt}(j_k) = 2 + 3k$, sj_k satisfies Equation (5.5). Then, let $j = j_k + 2^{i_{3k+2}} + 2^{i_{3k+3}} + 2^{i_{3k+4}}$, so that we have $\mathrm{wt}(j) = 2 + 3(k+1)$.

$$\begin{aligned}\sigma_n &= sj_k + s(2^{i_{3k+2}} + 2^{i_{3k+3}} + 2^{i_{3k+4}}) \\ &= \mathcal{S} + \sum_{m=1}^{k} \left(\mathcal{O}_{i_{3m-2}}^{i_{3m-1}-2} + \mathcal{E}_{i_{3m-1}}^{i_{3m}-2} + 2^{i_{3m+1}} \right) + \mathcal{O}_{i_{3k+1}}^{n-3} \\ &\quad + \left(2^{i_{3k+2}} + \mathcal{O}_{i_{3k+2}}^{i_{3k+3}-2} + \mathcal{E}_{i_{3k+3}}^{i_{3k+4}-2} \right) .\end{aligned}$$

Then combining sums with equal terms, we get:

$$\begin{aligned}\sigma_n &= \mathcal{S} + \sum_{m=1}^{k} \left(\mathcal{O}_{i_{3m-2}}^{i_{3m-1}-2} + \mathcal{E}_{i_{3m-1}}^{i_{3m}-2} + 2^{i_{3m+1}}\right) + \mathcal{O}_{i_{3k+1}}^{i_{3k+2}-2} \\ &\quad + 2^{i_{3k+2}} + 2 \cdot \mathcal{O}_{i_{3k+2}}^{i_{3k+3}-2} + \mathcal{E}_{i_{3k+3}}^{i_{3k+4}-2} + \mathcal{O}_{i_{3k+3}}^{n-3} \\ &= \mathcal{S} + \sum_{m=1}^{k} \left(\mathcal{O}_{i_{3m-2}}^{i_{3m-1}-2} + \mathcal{E}_{i_{3m-1}}^{i_{3m}-2} + 2^{i_{3m+1}}\right) + \mathcal{O}_{i_{3k+1}}^{i_{3k+2}-2} \\ &\quad + \mathcal{E}_{i_{3k+2}}^{i_{3k+3}-2} + 2^{i_{3k+3}} + \mathcal{A}_{i_{3k+3}}^{i_{3k+4}-1} + \mathcal{O}_{i_{3k+4}}^{n-3} \\ &= \mathcal{S} + \sum_{m=1}^{k} \left(\mathcal{O}_{i_{3m-2}}^{i_{3m-1}-2} + \mathcal{E}_{i_{3m-1}}^{i_{3m}-2} + 2^{i_{3m+1}}\right) + \mathcal{O}_{i_{3k+1}}^{i_{3k+2}-2} \\ &\quad + \mathcal{E}_{i_{3k+2}}^{i_{3k+3}-2} + 2^{i_{3k+4}} + \mathcal{O}_{i_{3k+4}}^{n-3} \ .\end{aligned}$$

Thus we deduce

$$\sigma_n = \mathcal{S} + \sum_{m=1}^{k+1} \left(\mathcal{O}_{i_{3m-2}}^{i_{3m-1}-2} + \mathcal{E}_{i_{3m-1}}^{i_{3m}-2} + 2^{i_{3m+1}}\right) + \mathcal{O}_{i_{3k+4}}^{n-3} \ .$$

It follows from Equation (5.5) that:

$$\begin{aligned}\mathrm{wt}(\sigma_n) &= \frac{i_0}{2} + 1 + \sum_{m=1}^{k} \left(\frac{i_{3m-1} - i_{3m-2}}{2} + \frac{i_{3m} - i_{3m-1}}{2} + 1\right) + \frac{n - 1 - i_{3k+1}}{2} \\ &= \frac{1}{2}\left(n + 2k + 1 - \sum_{m=0}^{k} (i_{3m+1} - i_{3m})\right) \ .\end{aligned}$$

Obviously, $i_{3m+1} - i_{3m} \geqslant 2$, implying that

$$\mathrm{wt}(\sigma_n) \leqslant \frac{1}{2}\left(n + 2k + 1 - 2(k+1)\right) = (n-1)/2 \ .$$

Moreover, the largest value for $\sum_{m=0}^{k}(i_{3m+1} - i_{3m})$ is obtained when all other distances between two consecutive elements among $i_0, \ldots, i_{3k+1}$ are minimized, i.e., equal to 2, leading to $\sum_{m=0}^{k}(i_{3m+1} - i_{3m}) \leqslant (n-1) - 4k$. We then deduce that

$$\mathrm{wt}(\sigma_n) \geqslant 3k + 1 = \mathrm{wt}(j) - 1 \ .$$

Thus if $\mathrm{wt}(j) \bmod 3 = 2$, we have:

$$\mathrm{wt}\left(sj \bmod (2^n - 1)\right) \in [\![\mathrm{wt}(j) - 1, (n-1)/2]\!] \ .$$

(b) Let us now consider j such that $\mathrm{wt}(j) \bmod 3 = 0$. We let $\mathrm{wt}(j) = 3k$, and $j = \sum_{m=0}^{3k-1} 2^{i_m}$, where the i_m are even, and $0 \leqslant i_0 < \ldots < i_{3k-1} < n$. Then, we will show by induction on k that

$$\sigma_n = \sum_{m=0}^{k-1} \left(2^{i_{3m}} + \mathcal{O}_{i_{3m}}^{i_{3m+1}-2} + \mathcal{E}_{i_{3m+1}}^{i_{3m+2}-2}\right) \ . \qquad (5.6)$$

- **For $k = 1$.** Let $j = 2^{i_0} + 2^{i_1} + 2^{i_2}$ where i_0, i_1 and i_2 are even integers such that $0 \leqslant i_0 < i_1 < i_2 < n$. Then, we know from Remark 5.3 that

$$\sigma_n = 2^{i_0} + \mathcal{O}_{i_0}^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} \, .$$

- **Induction step.** Let us assume that the property holds for k, that is: for any $j_k = \sum_{m=0}^{3k-1} 2^{i_m}$, sj_k satisfies Equation (5.6). Then, for $j = j_k + 2^{i_{3k}} + 2^{i_{3k+1}} + 2^{i_{3k+2}}$, so that we have $\mathrm{wt}(j) = 3(k+1)$ and we deduce from Remark 5.3 that

$$\begin{aligned} \sigma_n &= sj_k + s\left(2^{i_{3k}} + 2^{i_{3k+1}} + 2^{i_{3k+2}}\right) \\ &= sj_k + 2^{i_{3k}} + \mathcal{O}_{i_{3k}}^{i_{3k+1}-2} + \mathcal{E}_{i_{3k+1}}^{i_{3k+2}-2} \\ &= \sum_{m=0}^{k} \left(2^{i_{3m}} + \mathcal{O}_{i_{3m}}^{i_{3m+1}-2} + \mathcal{E}_{i_{3m+1}}^{i_{3m+2}-2}\right) \, . \end{aligned}$$

Therefore, if $\mathrm{wt}(j) = 3k$, we have

$$\mathrm{wt}(\sigma_n) = \frac{1}{2}\left(2k + \sum_{m=0}^{k-1} (i_{3m+2} - i_{3m})\right) \in [\![\mathrm{wt}(j), (n-1)/2]\!] \, .$$

Obviously, $i_{3m+2} - i_{3m} \geqslant 4$, implying that

$$\mathrm{wt}(\sigma_n) \geqslant 3k = \mathrm{wt}(j) \, .$$

Moreover, the largest value for $\sum_{m=0}^{k-1}(i_{3m+2} - i_{3m})$ is obtained when all distances between i_{3m+3} and i_{3m+2}, for $m = 0, \dots k-2$ are minimized, i.e., equal to 2, leading to $\sum_{m=0}^{k-1}(i_{3m+2} - i_{3m}) \leqslant (n-1) - 2(k-1)$. We then deduce that

$$\mathrm{wt}(\sigma_n) \leqslant (n+1)/2 \, .$$

Thus if $\mathrm{wt}(j) \bmod 3 = 0$, we have:

$$\mathrm{wt}\left(sj \bmod (2^n - 1)\right) \in [\![\mathrm{wt}(j), (n+1)/2]\!] \, .$$

(c) Finally, let us consider j such that $\mathrm{wt}(j) \bmod 3 = 1$. We let $\mathrm{wt}(j) = 1 + 3k$, and $j = \sum_{m=0}^{3k} 2^{i_m}$, where the i_m are even, and $2 \leqslant i_0 < \ldots < i_{3k} < n$. Now, we will prove by induction on k that

$$\sigma_n = \mathcal{S} + \sum_{m=0}^{k-1} \left(\mathcal{E}_{i_{3m}}^{i_{3m+1}-2} + 2^{i_{3m+2}} + \mathcal{O}_{i_{3m+2}}^{i_{3m+3}-2}\right) + \mathcal{E}_{i_{3k}}^{n-1} \, , \tag{5.7}$$

where

$$\mathcal{S} = \begin{cases} 0 & \text{if } i_0 = 0 \\ \mathcal{O}_0^{i_0-2} & \text{otherwise} \end{cases} \, .$$

- **For $k = 1$:** let $j = 2^{i_0} + 2^{i_1} + 2^{i_2} + 2^{i_3}$ with i_0, i_1, i_2, i_3 even such that $0 \leqslant i_0 < i_1 < i_2 < i_3 < n$. Then, we deduce from Remark 5.3 that

$$\begin{aligned}\sigma_n &= s(2^{i_0} + 2^{i_1} + 2^{i_2}) + s2^{i_3} \\ &= 2^{i_0} + \mathcal{O}_{i_0}^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + \sum_{\ell=0}^{(n-1)/2} 2^{2\ell+i_3} \\ &= 2^{i_0} + \mathcal{O}_{i_0}^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{E}_{i_3}^{n-1} + \mathcal{O}_{0}^{i_3-2}\end{aligned}$$

implying that if $i_0 = 0$ we have

$$\begin{aligned}\sigma_n &= 1 + 2\mathcal{O}_0^{i_1-2} + \mathcal{A}_{i_1}^{i_2-1} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\ &= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} .\end{aligned}$$

Similarly if $i_0 \neq 0$, we have:

$$\begin{aligned}\sigma_n &= \mathcal{O}_0^{i_0-2} + \mathcal{E}_{i_0}^{i_1} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\ &= \mathcal{O}_0^{i_0-2} + \mathcal{E}_{i_0}^{i_1} + \mathcal{A}_{i_1}^{i_2-1} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\ &= \mathcal{O}_0^{i_0-2} + \mathcal{E}_{i_0}^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} .\end{aligned}$$

- **Induction step.** Let us assume that the property holds for k, i.e., for any $j_k = \sum_{m=0}^{3k} 2^{i_m}$, sj_k satisfies Equation (5.7). Then, for $j = j_k + 2^{i_{3k+1}} + 2^{i_{3k+2}} + 2^{i_{3k+3}}$, so that we have $\mathrm{wt}(j) = 1 + 3(k+1)$.

$$\begin{aligned}\sigma_n &= sj_k + 2^{i_{3k+1}} + \mathcal{O}_{i_{3k+1}}^{i_{3k+2}-2} + \mathcal{E}_{i_{3k+2}}^{i_{3k+3}-2} \\ &= \mathcal{S} + \sum_{m=0}^{k-1} \left(\mathcal{E}_{i_{3m}}^{i_{3m+1}-2} + 2^{i_{3m+2}} + \mathcal{O}_{i_{3m+2}}^{i_{3m+3}-2} \right) \\ &\quad + \mathcal{E}_{i_{3k}}^{n-1} + 2^{i_{3k+1}} + \mathcal{O}_{i_{3k+1}}^{i_{3k+2}-2} + \mathcal{E}_{i_{3k+2}}^{i_{3k+3}-2} .\end{aligned}$$

Then combining sums with equal terms, we get:

$$\begin{aligned}\sigma_n &= \mathcal{S} + \sum_{m=0}^{k-1} \left(\mathcal{E}_{i_{3m}}^{i_{3m+1}-2} + 2^{i_{3m+2}} + \mathcal{O}_{i_{3m+2}}^{i_{3m+3}-2} \right) \\ &\quad + \mathcal{E}_{i_{3k}}^{i_{3k+1}-2} + 2^{i_{3k+1}} + \mathcal{A}_{i_{3k+1}}^{i_{3k+2}-1} + 2 \cdot \mathcal{E}_{i_{3k+2}}^{i_{3k+3}-2} + \mathcal{E}_{i_{3k+3}}^{n-1} \\ &= \mathcal{S} + \sum_{m=0}^{k-1} \left(\mathcal{E}_{i_{3m}}^{i_{3m+1}-2} + 2^{i_{3m+2}} + \mathcal{O}_{i_{3m+2}}^{i_{3m+3}-2} \right) \\ &\quad + \mathcal{E}_{i_{3k}}^{i_{3k+1}-2} + 2^{i_{3k+2}} + \mathcal{O}_{i_{3k+2}}^{i_{3k+3}-2} + \mathcal{E}_{i_{3k+3}}^{n-1} .\end{aligned}$$

Thus, we deduce

$$\sigma_n = \mathcal{S} + \sum_{m=0}^{k} \left(\mathcal{E}_{i_{3m}}^{i_{3m+1}-2} + 2^{i_{3m+2}} + \mathcal{O}_{i_{3m+2}}^{i_{3m+3}-2} \right) + \mathcal{E}_{i_{3k+3}}^{n-1} .$$

Then, if $\mathrm{wt}(j) = 3k+1$, we have

$$\begin{aligned}\mathrm{wt}(\sigma_n) &= \frac{1}{2}\left(n+1+2k+i_0+\sum_{m=0}^{k-1}(i_{3m+1}-i_{3m}+i_{3m+3}-i_{3m+2})-i_{3k}\right)\\ &= \frac{1}{2}\left(n+1+2k-\sum_{m=0}^{k-1}(i_{3m+2}-i_{3m+1})\right)\ .\end{aligned}$$

Obviously, $i_{3m+2}-i_{3m+1} \geqslant 2$, implying that

$$\mathrm{wt}(\sigma_n) \leqslant (n+1)/2\ .$$

Moreover, the largest value for $\sum_{m=1}^{k}(i_{3m+2}-i_{3m+1})$ is obtained when all other distances between two consecutive elements among $i_0,\ldots,i_{3k}$ are minimized, i.e., equal to 2, leading to $\sum_{m=0}^{k-1}(i_{3m+2}-i_{3m+1}) \leqslant (n-1)-4k$. We then deduce that

$$\mathrm{wt}(\sigma_n) \geqslant 3k+1 = \mathrm{wt}(j)\ .$$

Thus if $\mathrm{wt}(j) \bmod 3 = 1$, we have:

$$\mathrm{wt}\left(sj \bmod (2^n-1)\right) \in [\![\mathrm{wt}(j),(n+1)/2]\!]\ .$$

□

As an immediate consequence, we obtain the following corollary.

Corollary 5.4. *There is a plateau between the first two rounds of* MiMC_3^{-1}*, i.e.:*

$$B_s^1 = B_s^2 = \frac{n+1}{2}\ .$$

Proof. First, as $\mathcal{E}_{s,1} = \{0,s\}$ we directly have

$$B_s^1 = \mathrm{wt}(s) = \frac{n+1}{2}\ .$$

Then using Proposition 5.13 that covers cases where $\mathrm{wt}(j) \geqslant 2$, and observing that $\mathrm{wt}(js) = 0$ if $\mathrm{wt}(j) = 0$ and $\mathrm{wt}(js) = \mathrm{wt}(s) = (n+1)/2$ if $\mathrm{wt}(j) = 1$, we get:

$$B_s^2 = \max\{\mathrm{wt}(e), e \in \mathcal{E}_{s,2}\} = \max\{\mathrm{wt}(js), j \preceq s\} = \frac{n+1}{2}\ .$$

□

Since there is a plateau between the first and second round for both MiMC_3 and MiMC_3^{-1}, we may wonder whether this corresponds to a more general phenomenon, since in Section 5.1.3 we also proved that $B_d^1 = B_d^2$, when $d = 2^k-1$. However, there is not necessarily a plateau for MiMC_d^{-1} in this case.

Example 5.5. In $\mathbb{F}_{2^{11}}$, we have $15 = 2^4-1$, so according to Proposition 5.3 we have $B_{15}^1 = B_{15}^2$. But for MiMC_{15}^{-1}, the inverse of 15 is 273, so the algebraic degree of the first round is $\mathrm{wt}(273) = 3$, while it is 5 after two rounds. Indeed, the Hamming weight of $(273 \times 273) \bmod (2^{11}-1)$ is 5.

5.4.2 Influence of the Encryption Degree

In the previous section we answered the question concerning the plateau between the first two rounds. We are now interested in investigating the case of the plateau in the last rounds at $n-2$. Studying the algebraic degree of MiMC_3^{-1} over iterations is much more difficult than for MiMC_3 since the underlying round function x^s has a much higher degree. However, the following result from [BC13] shows how the encryption degree can influence the decryption degree.

Proposition 5.14. *[BC13] For any $i \in [1, n-1]$, if the degree of the encryption function is strictly less than $(n-1)/i$, then the degree of the decryption function is strictly less than $n-i$.*

Based on this result, we can exhibit a lower bound on the number of rounds needed by the decryption function to reach degree $(n-i)$ (for some round constants).

Corollary 5.5. *Let r_{n-i} denote the smallest value of r such that $B_s^r \geqslant n-i$ for $1 \leqslant i \leqslant (n-1)/4$. Then*

$$r_{n-i} \geqslant \left\lceil \frac{1}{\log_2 3}\left(2\left\lceil \frac{1}{2}\left\lceil \frac{n-1}{i}\right\rceil\right\rceil + 1\right)\right\rceil .$$

Most notably,

$$r_{n-2} \geqslant \left\lceil \frac{1}{\log_2 3}\left(2\left\lceil \frac{n-1}{4}\right\rceil + 1\right)\right\rceil .$$

Proof. From Proposition 5.14, we know that, if $B_s^r \geqslant n-i$, then $B_3^r \geqslant (n-1)/i$. By hypothesis $i \leqslant (n-1)/4$, implying $B_3^r \geqslant 4$, from which we deduce that $r \geqslant 4$. It follows that Proposition 5.10 applies so that

$$2 \times \left\lceil \frac{\lfloor r\log_2 3\rfloor}{2} - 1\right\rceil \geqslant B_3^r \geqslant \frac{n-1}{i} .$$

B_3^r is an integer so we have necessarily

$$2 \times \left\lceil \frac{\lfloor r\log_2 3\rfloor}{2} - 1\right\rceil \geqslant B_3^r \geqslant \left\lceil \frac{n-1}{i}\right\rceil .$$

Moreover, B_3^r, is even so

$$\left\lceil \frac{\lfloor r\log_2 3\rfloor}{2} - 1\right\rceil \geqslant \left\lceil \frac{1}{2}\left\lceil \frac{n-1}{i}\right\rceil\right\rceil .$$

Then we get

$$\frac{\lfloor r\log_2 3\rfloor - 1}{2} \geqslant \left\lceil \frac{\lfloor r\log_2 3\rfloor}{2} - 1\right\rceil \geqslant \left\lceil \frac{1}{2}\left\lceil \frac{n-1}{i}\right\rceil\right\rceil .$$

Therefore,

$$r \geqslant \left\lceil \frac{1}{\log_2 3}\left(2\left\lceil \frac{1}{2}\left\lceil \frac{n-1}{i}\right\rceil\right\rceil + 1\right)\right\rceil .$$

In particular, for $i = 2$ we have

$$r \geqslant \left\lceil \frac{1}{\log_2 3}\left(2\left\lceil \frac{n-1}{4}\right\rceil + 1\right)\right\rceil ,$$

since $n-1$ is even. □

i	1	2	3	4	5
$n-i$	22	21	20	19	18
$(n-1)/i$	22	11	7.33	5.5	4.4
$\min\{r \text{ s.t. } B_3^r \geqslant (n-1)/i\}$ $\geqslant \min\{r \text{ s.t. } B_s^r \geqslant n-i\}$	15	9	6	5	3

(a) *when* $n = 23$

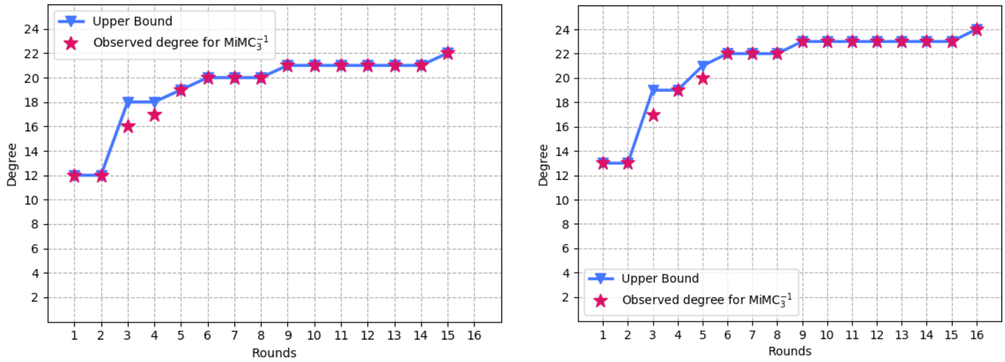
i	1	2	3	4	5	6
$n-i$	24	23	22	21	20	19
$(n-1)/i$	24	12	8	6	4.8	4
$\min\{r \text{ s.t. } B_3^r \geqslant (n-1)/i\}$ $\geqslant \min\{r \text{ s.t. } B_s^r \geqslant n-i\}$	16	9	6	5	3	3

(b) *when* $n = 25$

Table 5.3: *Computing upper bound on the algebraic degree of* MiMC_3^{-1}.

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
B_3^r	2	2	4	4	6	8	10	10	12	14	16	18	18	20	22	24
Bound for B_s^r $(n = 23)$	12	12	18	18	19	20	20	20	21	21	21	21	21	21	22	-
Bound for B_s^r $(n = 25)$	13	13	19	19	21	22	22	22	23	23	23	23	23	23	23	24

Table 5.4: *Upper bound on the algebraic degree of* MiMC_3^{-1} *for* $n = 23$ *and* 25.



(a) *When* $n = 23$.

(b) *When* $n = 25$.

Figure 5.17: *Upper bound on the algebraic degree of* MiMC_3^{-1}.

Example 5.6. As an illustration, for $n = 25$ and $n = 23$, the results of Corollary 5.5 applied with $1 \leqslant i \leqslant 6$, are given in Table 5.3.

We then deduce in Table 5.4 the evolution of the algebraic degree of MiMC_3^{-1} for $n = 23$ and $n = 25$. These values are compared on Figure 5.17 with the exact degree (i.e. the degree computed with a C implementation of Corollary 5.1).

In Proposition 5.13 we exhibited bounds on the Hamming weight of exponents $js \bmod (2^n - 1)$ when $j \leq s$. However, to better understand the behavior of the algebraic degree of MiMC_3^{-1} for a larger number of rounds, and hence obtain a more accurate bound, it is necessary to study in more details all the exponents $js \bmod (2^n - 1)$. Therefore, in Appendix A we will propose some directions to study the Hamming weight of exponents $js \bmod (2^n - 1)$ when $\mathrm{wt}(j) \in \{2, 3, 4, 5\}$.

Conclusion

In this chapter we have investigated both the univariate polynomial representation, and the algebraic degree of iterated power functions. In particular, we have seen that for some choices of the iterated power function $x \mapsto x^d$ in MiMC_d, we have relatively sparse univariate polynomial representations with families of missing exponents clearly identified. While it is not yet clear how to exploit such sparse univariate polynomials to build a distinghuisher, we can use this observation to deduce bounds on the algebraic degree of the cipher. It is worth mentioning that the bound on the algebraic degree of MiMC_3 will be of fundamental interest in the next chapter to determine the complexity of high-order differential attacks.

Moreover, we have provided bounds for different instances of MiMC_d and identified some plateaus that slightly slow down the growth of the algebraic degree. We also proved that there is a plateau between the first two rounds of MiMC_3^{-1}, and gave some direction to better understand the behaviour of the algebraic degree of the inverse transformation.

As a consequence, our results contribute to a better understanding of the univariate representation and the algebraic degree of block ciphers and permutations defined over large finite fields.

CHAPTER 6

Tracing exponents when iterating power functions

While an upper bound on the algebraic degree allows an attacker to perform some higher-order differential attacks, as in [Eic+20], it does not give any guarantee that such attacks cannot be significantly improved. Various solver-based methods have been proposed to provide bounds on the algebraic degree of Arithmetization-Oriented primitives. In this chapter we propose a different vision that limits the reliance on solvers and attempts to better understand the mathematical properties of MiMC. Our goal is to explicitly exhibit maximum-weight exponents while iterating the round function. More precisely, our result provides some guarantees on the algebraic degree of the primitive, and then on the minimal complexity for a higher-order differential attack.

In Section 6.1 we provide a procedure, relying on an inductive proof (for most rounds) and MILP-based algorithm (for a few sporadic cases), to determine the exponents reaching the bound on the algebraic degree. We complete such an analysis by trying to find all maximum-weight exponents in Section 6.2. Then, in Section 6.3 we investigate other instances of MiMC and give some brief ideas for finding trails to construct exponents. In Section 6.4 we also consider the construction of exponents for rounds 3 and 4 of the inverse transformation from which we deduce a lower bound on the algebraic degree. Finally, in Section 6.5, we see the consequences of our analysis when applying higher-order differential attacks.

Contents

6.1 Constructing exponents of MiMC_3

In this chapter we will extensively use the notion of *trail* when referring to the tracing of exponents.

Definition 6.1 (Trail). Let $e_{r_1} \in \mathcal{E}_{d,r_1}$ and let e_{r_2} be an integer where $r_2 > r_1$. We say that there is a trail from e_{r_1} to e_{r_2} if there exists a sequence of Cover and Mult_d of length $(r_2 - r_1)$ (see definitions in Chapter 5) such that

$$e_{r_2} \in (\mathsf{Mult}_d \circ \mathsf{Cover}) \dots (\mathsf{Mult}_d \circ \mathsf{Cover}) (\{e_{r_1}\}) ,$$

implying that $e_{r_2} \in \mathcal{E}_{d,r_2}$.

The aim of this chapter is to find trails to build maximum-weight exponents which reach the upper bound on the algebraic degree given in Chapter 5. We summarize the main propositions of this chapter in Table 6.1.

d	Number of exponents	Rounds	Corresponding proposition
3	one	$\{4, \dots, 16265\}$	Theorem 6.1
	all	$\{6, \dots, 411\}$	Proposition 6.5
$2^j + 1, j > 1$ $2^j - 1, j > 2$	one	-	observations in Section 6.3
3^{-1}	one	3	Proposition 6.6
		4	Proposition 6.7

Table 6.1: Corresponding propositions on maximum-weight exponents for each instance of MiMC_d studied.

Let us first focus on the maximum-weight exponents for MiMC_3. In this case, the gap between our upper bound and the trivial lower bound from Chapter 5 raises concerns about the complexity of the most efficient higher-order differential attacks that could be mounted. This issue is addressed in this section, where we show that, for all but a few round-reduced versions of MiMC_3, the upper bound exhibited in Proposition 5.10 coincides with the exact value of B_3^r. Figure 6.1 compares the observed degree (i.e. the degree computed with a C implementation of Proposition 5.1 in Chapter 5) with the upper bound, in the particular case where the degree of extension is $n \geqslant 31$. We indeed notice that the observed degree coincides with the upper bound.

We recall that B_3^r represents the maximal algebraic degree, reached for at least one sequence of round constants. Then it may happen that, for some specific choice of constants, some monomials do not appear. Figure 6.2 also shows that a trail is not unique. For instance 54 is a maximum-weight exponent at round 4, but it can be derived from 27 or 18, both appearing in round 3, as follows

$$\begin{tikzcd} 3 \arrow[r, "\mathsf{Mult}_3 \circ \mathsf{Cover}"] & 9 \arrow[r, "\mathsf{Mult}_3 \circ \mathsf{Cover}"] & 27 \arrow[r, "\mathsf{Mult}_3 \circ \mathsf{Cover}"] & 54 \\ 3 \arrow[r, "\mathsf{Mult}_3 \circ \mathsf{Cover}"] & 6 \arrow[r, "\mathsf{Mult}_3 \circ \mathsf{Cover}"] & 18 \arrow[r, "\mathsf{Mult}_3 \circ \mathsf{Cover}"] & 54 . \end{tikzcd}$$

We highlighted those trails in bold on Figure 6.2. The numbers squared in red are the exponents of maximum weight at rounds 2, 3 and 4 respectively. We can indeed see that most of them are not uniquely constructed. Given the high number of possible trails, in this chapter we will restrict ourselves to construct exponents with maximum weight only.

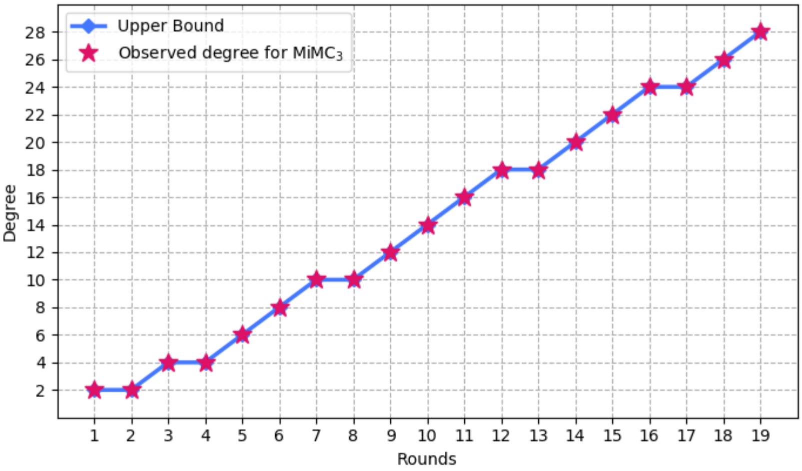


Figure 6.1: *Comparison between the observed degree for* MiMC$_3$ *and the bound from Proposition 5.10 (for $n \geqslant 31$).*

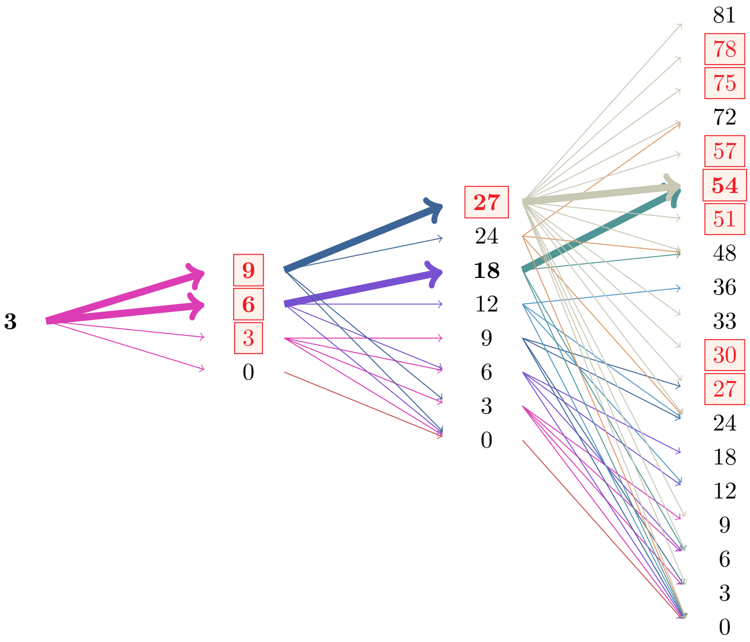


Figure 6.2: *Getting next-round exponents for* MiMC$_3$.

More precisely, our approach consists in investigating Conjecture 6.1, which exhibits an exponent in the univariate polynomial representing MiMC$_3$ whose weight equals the upper bound defined in Proposition 5.10. In what follows, we let $(k_{3,r})_{r>0}$ and $(b_{3,r})_{r>0}$ be two sequences defined by

$$k_{3,r} = \lfloor r \log_2 3 \rfloor \text{ and } b_{3,r} = k_{3,r} \bmod 2\,.$$

Conjecture 6.1. *Let $(\omega_{3,r})_{r\geqslant 4}$ be the sequence of integers defined by*

$$\omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}}, \quad \textit{where } \alpha_{b_{3,r}} = \begin{cases} 7 & \textit{if } b_{3,r} = 0 \\ 5 & \textit{if } b_{3,r} = 1\,. \end{cases}$$

Then, for all $r \geqslant 4$, it holds that $\omega_{3,r} \in \mathcal{E}_{3,r}$.

While the most general case remains a conjecture at the time of writing, we show in this section that the conjecture is true for all $r \leqslant 16265$, except for a few sporadic cases for which a proof remains out of reach. We have chosen to stop at this point since 16266 is one of the cases not covered by our inductive procedure and for which we need a MILP solver, but it is too costly (see Section 6.1.3).

Our proof of this theorem is divided in two parts which correspond to Sections 6.1.2 and 6.1.3 of this section.

- We present an inductive procedure establishing that, for most values of r, $\omega_{3,r} \in \mathcal{E}_{3,r}$ using the fact that $\omega_{3,r-\ell} \in \mathcal{E}_{3,r-\ell}$ for some $\ell < r$.
- We describe a MILP-based computationally intensive procedure for proving that $\omega_{3,r} \in \mathcal{E}_{3,r}$. Although this procedure works for any round, it is very expensive so we will only use it for some sporadic values of r, corresponding to the cases which are not covered by the inductive procedure.
- These results and algorithms are then put together in order to prove Theorem 6.1.

6.1.1 Properties of $(b_{3,r})_{r>0}$ and $(k_{3,r})_{r>0}$

Before giving the inductive proof, we observe some properties of the sequence $(k_{3,r})_{r>0}$. The sequence $(b_{3,r})_{r>0}$ will help us understand the particular sequences encountered in the study of $(k_{3,r})_{r>0}$. In particular, the following proposition exhibits a relation between the variations of $(b_{3,r})_{r>0}$ and of $(k_{3,r})_{r>0}$.

Proposition 6.1. *If $b_{3,r} = b_{3,r-1}$ then $k_{3,r} - k_{3,r-1} = 2$, otherwise $k_{3,r} - k_{3,r-1} = 1$.*

Proof. By definition, $k_{3,r} = \lfloor r \log_2 3 \rfloor$. As a consequence, since $\log_2 3 \approx 1.59$, the sequence $k_{3,r}$ increases by 1 or 2 for each increment of r. If this increase is by 1, then the parities of $k_{3,r}$ and $k_{3,r-1}$ have to be different i.e. $b_{3,r} \oplus b_{3,r-1} = 1$. Otherwise, they have to be identical, i.e. $b_{3,r} \oplus b_{3,r-1} = 0$. □

Let $(s_r)_{r>0}$ be the sequence of *switches* from one parity to another, i.e.

$$s_1 = 0 \quad \text{and} \quad s_r = b_{3,r} \oplus b_{3,r-1}\,.$$

It can be shown that $(k_{3,r})_{r>0}$ is determined by the sequence $(s_r)_{r>0}$. Indeed we can rewrite Proposition 6.1 as

$$k_{3,r} = \begin{cases} k_{3,r-1} + 2 & \text{if } s_r = 0 \\ k_{3,r-1} + 1 & \text{if } s_r = 1\,. \end{cases}$$

From which we deduce the following proposition.

Proposition 6.2. *For any $\ell \geqslant 1$, and any $r > \ell$, we have*

$$k_{3,r} - k_{3,r-\ell} = 2\ell - \sum_{i=0}^{\ell-1} s_{r-i} \in \{k_{3,\ell}, k_{3,\ell}+1\} \, .$$

Proof. As previously observed, we have

$$k_{3,r} - k_{3,r-1} \; = \; 2 - s_r \, ,$$

from which we deduce

$$k_{3,r} - k_{3,r-\ell} \; = \; k_{3,r} - k_{3,r-1} + k_{3,r-1} - k_{r-2} + \ldots + k_{r-\ell+1} - k_{3,r-\ell} \; = \; 2\ell - \sum_{i=0}^{\ell-1} s_{r-i} \, .$$

Now let us prove that $k_{3,r} - k_{3,r-\ell}$ can only takes two values. We have $k_{3,r} - k_{3,r-\ell} = \lfloor r \log_2(3) \rfloor - \lfloor (r-\ell) \log_2(3) \rfloor$. Using that

$$\lfloor x - y \rfloor \leqslant \lfloor x \rfloor - \lfloor y \rfloor \leqslant \lfloor x - y \rfloor + 1 \, ,$$

we can write

$$\lfloor \ell \log_2(3) \rfloor \; \leqslant \; k_{3,r} - k_{3,r-\ell} \; \leqslant \; \lfloor \ell \log_2(3) \rfloor + 1 \, ,$$

or equivalently

$$\lfloor \ell \log_2(3) \rfloor \; \leqslant \; 2\ell - \sum_{i=0}^{\ell-1} s_{r-i} \; \leqslant \; \lfloor \ell \log_2(3) \rfloor + 1 \, ,$$

which implies that the number of switches, i.e. the Hamming weight of the subsequence $(s_{r-i})_{0 \leqslant i < \ell}$, can take two values only. □

Remark 6.1. We can use the same argument on the sequence $(b_{3,r})_{r>0}$ so that

$$\begin{aligned} b_{3,r} \oplus b_{3,r-\ell} &= b_{3,r} \oplus b_{3,r-1} \oplus b_{3,r-1} \oplus b_{3,r-2} \oplus \ldots \oplus b_{3,r-\ell+1} \oplus b_{3,r-\ell} \\ &= \bigoplus_{i=0}^{\ell-1} s_{r-i} \\ &= (k_{3,r} - k_{3,r-\ell}) \bmod 2 \, . \end{aligned}$$

We then deduce the following proposition.

Proposition 6.3. *Let $r \geqslant 3$. Then there exists $1 \leqslant \ell < r$ such that*

$$k_{3,r} - k_{3,r-\ell} = k_{3,\ell}$$

if and only if $(s_1 \ldots s_r)$ is not a palindrome, i.e. if there exists i, $0 \leqslant i < r$ such that

$$s_{r-i} \neq s_{i+1} \, .$$

Proof. From Proposition 6.2, we have, for any $1 \leqslant \ell < r$,

$$k_{3,r} - k_{3,r-\ell} \; = \; 2\ell - \sum_{i=0}^{\ell-1} s_{r-i}$$

$$\text{and } k_{3,\ell} - k_{3,1} \; = \; 2(\ell-1) - \sum_{j=0}^{\ell-2} s_{\ell-j} = 2\ell - 2 - \sum_{i=2}^{\ell} s_i \, .$$

It follows that

$$k_{3,r} - k_{3,r-\ell} - k_{3,\ell} = -k_{3,1} + 2 - \left(\sum_{i=0}^{\ell-1} s_{r-i} - \sum_{i=2}^{\ell} s_i \right) .$$

Since $k_{3,1} = \lfloor \log_2 3 \rfloor = 1$ we deduce that

$$k_{3,r} - k_{3,r-\ell} - k_{3,\ell} = 1 - \left(\sum_{i=0}^{\ell-1} (s_{r-i} - s_{i+1}) \right) ,$$

where the last equality comes from the fact that $s_1 = 0$. It follows that, if $(s_1 \dots s_r)$ is a palindrome, then all terms in the sum vanish and $k_{3,r} - k_{3,r-\ell} = k_{3,\ell} + 1$ for all $1 \leqslant \ell < r$. Conversely, if $(s_1 \dots s_r)$ is not a palindrome and if ℓ denotes the smallest index such that $s_{r-\ell+1} \neq s_\ell$, we obtain that

$$k_{3,r} - k_{3,r-\ell} - k_{3,\ell} = 1 - (-1)^{s_\ell} \in \{0, 2\} ,$$

by observing that $s_{r-\ell+1} - s_\ell = (-1)^{s_\ell}$ since it differs from 0. Using that $k_{3,r} - k_{3,r-\ell} - k_{3,\ell} \in \{0, 1\}$, we deduce that $s_\ell = 0$ and $k_{3,r} - k_{3,r-\ell} - k_{3,\ell} = 0$. □

In Table 6.2 we give the first values for each of the sequences $(k_{3,r})_{r>0}$, $(b_{3,r})_{r>0}$ and $(s_r)_{r>0}$. For example, we can notice that for $r \in \{2, 7\}$, the sequence $(s_1 \dots s_r)$ is a palindrome.

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$k_{3,r}$	1	3	4	6	7	9	11	12	14	15	17	19	20	22	23	25	26	28	30	31
$b_{3,r}$	1	1	0	0	1	1	1	0	0	1	1	1	0	0	1	1	0	0	0	1
s_r	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	1	0	0	1

Table 6.2: *Sequences $(k_{3,r})_{r>0}$, $(b_{3,r})_{r>0}$ and $(s_r)_{r>0}$ for the first rounds.*

Remark 6.2. Let us observe that $(s_1 \dots s_r)$ is a palindrome for $r \in \{1, 2, 7, 12, 53, \dots\}$. Then the sequence formed by the values r such that $(s_1 \dots s_r)$ is a palindrome is a subset of

$$\mathfrak{D} = \{1, 2, 3, 5, 7, 12, 17, 29, 41, 53, 94, 147, 200, 253, 306, 359, 665, 971, \dots\} ,$$

which corresponds to the sequence of the first denominators of the semiconvergents of $\log_2 3$. The "semiconvergents" of a real number x is the sequence $(p_i/q_i)_{i \geqslant 0}$ such that all p_i and q_i are positive integers, and such that the sequence $(|x - p_i/q_i|)_{i \geqslant 0}$ is strictly decreasing. More details on this sequence and a link with music theory will be given in Chapter 7.

For small values of r, we have computed the set $\mathcal{L}_r = \{\ell,\ 1 \leqslant \ell < r, \text{ s.t. } k_{3,r-\ell} = k_{3,r} - k_{3,\ell}\}$ involved in the previous proposition, and we have noticed the following property, which has been checked up to $r \leqslant 16265$, but which remains a conjecture in the general case.

Conjecture 6.2. *Let $r \geqslant 3$ be such that $(s_1 \dots s_r)$ is not a palindrome. Let $\mathcal{L}_r$ and $\mathcal{P}_r$ be the two sets defined as follows:*

$$\mathcal{L}_r = \{\ell,\ 1 \leqslant \ell < r,\ \textit{s.t. } k_{3,r-\ell} = k_{3,r} - k_{3,\ell}\}$$
$$\mathcal{P}_r = \{r_i < r \textit{ s.t. } (s_1 \dots s_{r_i}) \textit{ is a palindrome}\} .$$

Then $\min(\mathcal{L}_r) \in \mathcal{P}_r$ *and* $\max(\mathcal{P}_r) \in \mathcal{L}_r$.

Table 6.3 show that Conjecture 6.2 is indeed satisfied for the first rounds. With our experiments we managed to prove that the property is satisfied up to $r \leqslant 16265$.

r	$\mathcal{L}_r$	$\mathcal{P}_r$
3	$\{1,2\}$	$\{1,2\}$
4	$\{2\}$	$\{1,2\}$
5	$\{1,2,3,4\}$	$\{1,2\}$
6	$\{2,4\}$	$\{1,2\}$
7	-	-
8	$\{1,2,4,6,7\}$	$\{1,2,7\}$
9	$\{2,7\}$	$\{1,2,7\}$
10	$\{1,2,3,4,6,7,8,9\}$	$\{1,2,7\}$
11	$\{2,4,7,9\}$	$\{1,2,7\}$
12	-	-
13	$\{1,2,4,6,7,9,11,12\}$	$\{1,2,7,12\}$
14	$\{2,7,12\}$	$\{1,2,7,12\}$
15	$\{1,2,3,4,6,7,8,9,11,12,13,14\}$	$\{1,2,7,12\}$
16	$\{2,4,7,9,12,14\}$	$\{1,2,7,12\}$
17	$\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$	$\{1,2,7,12\}$
18	$\{2,4,6,7,9,11,12,14,16\}$	$\{1,2,7,12\}$
19	$\{7,12\}$	$\{1,2,7,12\}$
20	$\{1,2,4,6,7,8,9,11,12,13,14,16,18,19\}$	$\{1,2,7,12\}$

Table 6.3: *Sets $\mathcal{L}_r$ and $\mathcal{P}_r$ for the first rounds.*

6.1.2 Inductive Procedure

Our objective is now to prove Proposition 6.4, in which we identify a process establishing that $\omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}} \in \mathcal{E}_{3,r}$ knowing that $\omega_{3,r-\ell} \in \mathcal{E}_{3,r-\ell}$ for $\ell \in \mathcal{L}_r$. This result is valid up to a certain value of r, i.e. $r \leqslant 16265$, and also excludes a few sporadic cases. These constraints originate from the following two observations, which may be valid in the general case, but remain open.

We first need to compare powers of 3 and powers of 2. For some sporadic cases, we can simply check the result experimentally.

Observation 6.1. Let $r \geqslant 4$ be such that $s_1...s_r$ is a palindrome. If $r \leqslant 16265$, then $r \in \{7,12,53,359,665\}$ and we have

$$3^r > 2^{k_{3,r}} + 2^r \,,$$

where $k_{3,r} = \lfloor r \log_2 3 \rfloor$.

We then deduce that the property is satisfied for any round r such that $4 \leqslant r \leqslant 16265$.

Corollary 6.1. *Let $(k_{3,r})_{r>0}$ be the sequence defined by $k_{3,r} = \lfloor r \log_2 3 \rfloor$. If $4 \leqslant r \leqslant 16265$, then*

$$3^r > 2^{k_{3,r}} + 2^r \,.$$

Proof. We prove it by induction on r.

- **For $r = 4$:** we have $k_{3,r} = 6$, and $3^4 = 81 > 80 = 2^6 + 2^4$.

- **Induction step.** We suppose that for all $i < r$, we have $3^i > 2^{k_{3,i}} + 2^i$. If $(s_1, \ldots, s_r)$ is a palindrome then $r \in \{7, 12, 53, 359, 665\}$, we know from Observation 6.1 that the property holds. Otherwise, there exists $\ell \in \mathcal{L}_r$, implying that

$$3^r \;=\; 3^{r-\ell}3^\ell \;>\; (2^{k_{3,r-\ell}} + 2^{r-\ell})(2^{k_{3,\ell}} + 2^\ell) \;=\; 2^{k_{3,r}} + 2^{k_{3,r-\ell}+\ell} + 2^{k_{3,\ell}+r-\ell} + 2^r \;.$$

Therefore, we have $3^r > 2^{k_{3,r}} + 2^r$.

□

We also conjecture that this bound is valid for any value of r. Although such bounds have already been investigated in the number theory literature, at the time of writing we are not able to prove the result in the general case. It is also worth noting that, in our case, Corollary 6.1 is sufficient because we are already limited by the next observation.

Indeed, we also need the following remark, on the representation of all elements in $\mathbb{Z}/3^t\mathbb{Z}$ as a sum of even powers of 2.

Observation 6.2. Let $1 \leqslant t \leqslant 21$, then

$$\forall x \in \mathbb{Z}/3^t\mathbb{Z},\ \exists \varepsilon_2, \ldots, \varepsilon_{2t+2} \in \{0,1\},\ \text{s.t. } x = \sum_{j=2}^{2t+2} \varepsilon_j 4^j \bmod 3^t \;.$$

This observation has also been obtained with a simple implementation to check the property. However, we conjecture that this result holds in general for any value of t. In the observation above we need at most $2t+1$ exponents, but we do not exclude that more coefficients are needed for larger values of t.

Example 6.1. Let us check that the observation holds for small values of t.

- For $t = 1$, we have $2t + 2 = 4$ and

$$4^2 = 4^3 = 4^4 = 1 \bmod 3$$

Then

$$0 = 4^2 + 4^3 + 4^4 \bmod 3 \quad 1 = 4^2 \bmod 3 \quad 2 = 4^2 + 4^3 \bmod 3$$

- For $t = 2$, we have $2t + 2 = 6$ and

$$4^2 = 4^5 = 7 \bmod 9 \quad 4^3 = 4^6 = 1 \bmod 9 \quad 4^4 = 4 \bmod 9$$

Then

$$\begin{array}{lll} 0 = 4^2 + 4^4 + 4^5 \bmod 9 & 1 = 4^3 \bmod 9 & 2 = 4^2 + 4^4 \bmod 9 \\ 3 = 4^2 + 4^3 + 4^4 \bmod 9 & 4 = 4^4 \bmod 9 & 5 = 4^3 + 4^4 \bmod 9 \\ 6 = 4^3 + 4^2 + 4^5 \bmod 9 & 7 = 4^2 \bmod 9 & 8 = 4^2 + 4^3 \bmod 9 \end{array}$$

We now prove that, in most cases, the fact that the exponent

$$\omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}}, \ \text{ where } \alpha_{b_{3,r}} = \begin{cases} 7 & \text{if } b_{3,r} = 0 \\ 5 & \text{if } b_{3,r} = 1\,, \end{cases}$$

belongs to $\mathcal{E}_{3,r}$ can be derived from the fact that $\omega_{3,r-\ell} \in \mathcal{E}_{3,r-\ell}$. The overall procedure is described in Proposition 6.4. The idea is to study the binary representation of the exponents involved in the trail from $\omega_{3,r-\ell}$ to $\omega_{3,r}$. To do so, we first observe in Remark 6.3 the binary decomposition of $\omega_{3,r}/3$. Then, we give two examples on the choice of a "good" integer ℓ to build a trail.

In the following, we will also use the overline on $b_{3,r}$ to denote its complementary, i.e. if $b_{3,r} = 0$ then $\overline{b_{3,r}} = 1$ and similarly if $b_{3,r} = 1$ then $\overline{b_{3,r}} = 0$.

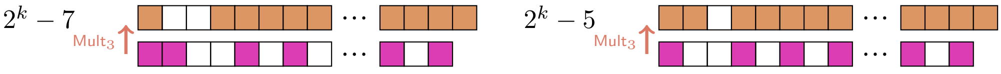
Remark 6.3. We recall (see page 131) that, for any even k,

$$(2^k - 1)/3 = \sum_{i=0}^{k/2-1} 2^{2i},$$

implying that

- for k even,
$$\frac{2^k - 7}{3} = \frac{2^k - 1}{3} - 2 = 3 + \sum_{i=2}^{k/2-1} 2^{2i}$$
- for k odd,
$$\frac{2^k - 5}{3} = \frac{2^k - 2}{3} - 1 = 1 + \sum_{i=1}^{(k-1)/2-1} 2^{2i+1}.$$

Figure 6.3 shows the binary representation of these two integers. On the first line the squares 🟧 represent the active bits of $\omega_{3,r}$, and on the second line the squares 🟪 the active bits of $\omega_{3,r}/3$.



(a) *k even.*

(b) *k odd.*

Figure 6.3: *Bit representations of $\omega_{3,r}$ and $\omega_{3,r}/3$.*

Therefore, for any $i \geqslant 3$,

$$\frac{\omega_{3,i}}{3} = \frac{2^{k_{3,i}} - \alpha_{b_{3,i}}}{3} = (8 - \alpha_{\overline{b_{3,i}}}) + \sum_{j=1+\overline{b_{3,i}}}^{\left\lfloor \frac{k_{3,i}}{2} \right\rfloor - 1} 2^{2j+b_{3,i}}. \tag{6.1}$$

In the following we will be using this type of figure extensively to help us visualize what is happening at the bit level.

We also point out that the existence of appropriate integers ℓ from which the trail can start depends on the parity of $k_{3,r}$ and $k_{3,i}$ for $i \leqslant r$. Let us consider some examples to see how to find such "good" integers ℓ.

Example 6.2 (Round 5)**.** We can show that $\omega_{3,5} \in \mathcal{E}_{3,5}$ using $\omega_{3,4} \in \mathcal{E}_{3,4}$. Indeed, we have

$$\omega_{3,5} = 2^{k_{3,5}} - \alpha_{b_5} = 2^7 - 5 = 123 \quad \text{and} \quad \omega_{3,4} = 2^{k_{3,4}} - \alpha_{b_4} = 2^6 - 7 = 57$$

where $123/3 = 41 \preceq 57$. Figure 6.4 illustrates this situation. On the first line the squares 🟧 represent the active bits of 123, and on the second and third line the squares 🟪 the active bits of 41 and 57.

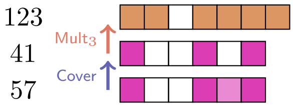


Figure 6.4: *Bit representations of the exponents involved in a trail between rounds 4 and 5.*

Example 6.3 (Round 6)**.** We can show that $\omega_{3,6} \in \mathcal{E}_{3,6}$ using $\omega_{3,4} \in \mathcal{E}_{3,4}$. Indeed, we have

$$\omega_{3,6} = 2^{k_{3,6}} - \alpha_{b_6} = 2^9 - 5 = 507 \quad \text{and} \quad \omega_{3,4} = 2^{k_{3,4}} - \alpha_{b_4} = 2^6 - 7 = 57$$

where $507/3 = 169 \preceq 171$ and $171/3 = 57$. Figure 6.5 illustrates this situation. On the first line the squares 🟧 represent the active bits of 507, on the second and third lines the squares 🟪 the active bits of 169 and 171, and on the fourth and fifth lines the squares 🟪 the active bits of 57.

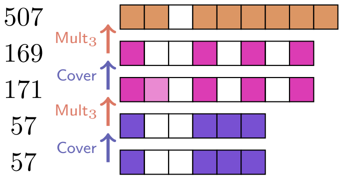


Figure 6.5: *Bit representations of the exponents involved in a trail between rounds 4 and 6.*

However, it would be impossible to show this using $\omega_{3,5} = 123 \in \mathcal{E}_{3,5}$ since $169 > 123$.

Let us then generalize the procedure for any round r and any integer ℓ.

Proposition 6.4. *Let $(k_{3,r})_{r>0}$ be the sequence defined by $k_{3,r} = \lfloor r \log_2 3 \rfloor$, and $(b_{3,r})_{r>0}$ the sequence defined by $b_{3,r} = k_{3,r} \bmod 2$. Let $r \geqslant 5$, and $\ell \in \mathcal{L}_r$ such that one of the following situations occurs:*

(1) *$\ell = 1$,*

(2) *$\ell = 2$,*

(3) *$2 < \ell \leqslant 22$ such that $k_{3,r} \geqslant k_{3,\ell} + 3\ell + b_{3,r} + 1$, and one of the following situations occurs:*

- *ℓ is even, or*
- *ℓ is odd, with $b_{r-\ell} = \overline{b_{3,r}}$;*

(4) *$2 < \ell \leqslant 22$ is odd such that $k_{3,r} \geqslant k_{3,\ell} + 3\ell + \overline{b_{3,r}} + 5$ and $b_{3,r-\ell} = b_{3,r}$.*

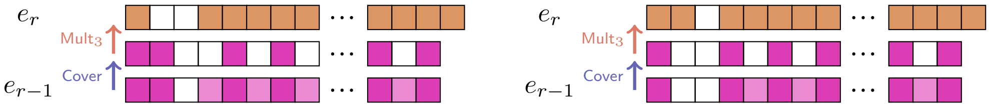
Then $\omega_{3,r-\ell} \in \mathcal{E}_{3,r-\ell}$ implies that $\omega_{3,r} \in \mathcal{E}_{3,r}$.

Proof. The proof consists, for given r and ℓ, in exhibiting a sequence of exponents $(e_{r-\ell} \dots e_r)$ such that $e_r = \omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}}$ and each e_{r-i}, $0 < i \leqslant \ell$, belongs to $\mathcal{E}_{3,r-i}$. It is worth noting that proving that $e_{j+1} \in \mathcal{E}_{3,j+1}$ boils down to exhibiting some $e_j \in \mathcal{E}_{3,j}$ such that $(e_{j+1}/3) \preceq e_j$. Then the general idea is to reduce the expression of e_{j+1} to sums which are multiples of 3. Let us now investigate the different cases for ℓ.

(1) When $\ell = 1$, we have $k_{3,r-1} = k_{3,r} - 1$ by definition of $\mathcal{L}_r$. From Proposition 6.1, we deduce that $b_{3,r-1} = \overline{b_{3,r}}$. By hypothesis, $\omega_{3,r-1} = 2^{k_{3,r}-1} - \alpha_{\overline{b_{3,r}}}$ belongs to $\mathcal{E}_{3,r-1}$. Moreover, from Equation (6.1), we deduce that

$$\frac{2^{k_{3,r}} - \alpha_{b_{3,r}}}{3} = (8 - \alpha_{\overline{b_{3,r}}}) + \sum_{j=1+\overline{b_{3,r}}}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+b_{3,r}} \preceq e_{r-1} \ ,$$

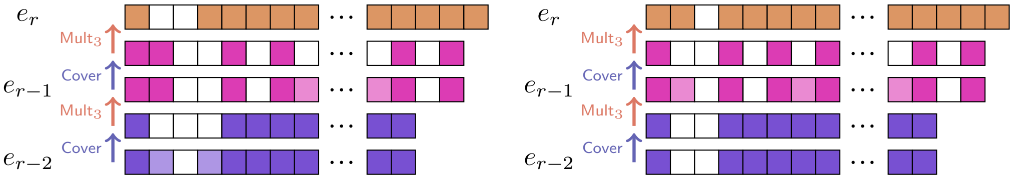
implying that $\omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}}$ belongs to $\mathcal{E}_{3,r}$. Figure 6.6 illustrates the above procedure. On the first lines the squares 🟧 represent the active bits of e_r and on the third lines the squares 🟪 the active bits of e_{r-1}.



(a) $b_r = 0$. **(b)** $b_r = 1$.

Figure 6.6: *How to derive $\omega_{3,r}$ from $\omega_{3,r-\ell}$ when $\ell = 1$.*

(2) Let $\ell = 2$. Our aim is to describe to procedure illustrated with Figure 6.7. On the first lines the squares 🟧 represent the active bits of e_r, on the third lines the squares 🟪 the active bits of e_{r-1}, and on the fifth lines the squares 🟦 the active bits of e_{r-2}.



(a) $b_r = 0$. **(b)** $b_r = 1$.

Figure 6.7: *How to derive $\omega_{3,r}$ from $\omega_{3,r-\ell}$ when $\ell = 2$.*

From Proposition 6.2, we have $k_{r-2} = k_{3,r} - 3$ and $b_{r-2} = \overline{b_{3,r}}$. Therefore, by hypothesis, $\omega_{3,r-2} = 2^{k_{3,r}-3} - \alpha_{\overline{b_{3,r}}}$ belongs to $\mathcal{E}_{3,r-2}$. Let us choose

$$e_{r-1} = 3 + \sum_{j=1+\overline{b_{3,r}}}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+b_{3,r}} + \sum_{j=3}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 3 + b_r} 2^{2j+\overline{b_{3,r}}} \ ,$$

so that, regardless of the value of $b_{3,r}$, one of the sums corresponds to even powers of 2, the other to odd powers. Then, combining both sums, we get

$$e_{r-1} = 3 + S + \sum_{j=3}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 3 + b_{3,r}} \left(2^{2j+\overline{b_{3,r}}} + 2^{2j+b_{3,r}}\right) + 2^{k_{3,r}-2} \ ,$$

where $S = 2^4$, if $b_r = 0$, and $S = 2^3 + 2^5$, if $b_r = 1$, implying that

$$e_{r-1} = 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 2^2(8 - \alpha_{\overline{b_{3,r}}}) - 2^{4+\overline{b_r}} - 1\,.$$

Noting that

$$-2^2(8 - \alpha_{\overline{b_{3,r}}}) - 2^{4+\overline{b_{3,r}}} - 1 = 3 \times (-2^2(8 - \alpha_{\overline{b_{3,r}}}) - 3)$$

we get

$$e_{r-1} = 3 \times 2^{k_{3,r}-3} + 3 \times (-2^2(8 - \alpha_{\overline{b_{3,r}}}) - 3)\,.$$

Indeed, if $b_{3,r} = 0$, then we have

$$-4 \times 3 - 2^5 - 1 = -45 = 3 \times (-15) = 3 \times (-4 \times 3 - 3)\,,$$

and if $b_{3,r} = 1$, then we have

$$-4 \times 1 - 2^4 - 1 = -21 = 3 \times (-7) = 3 \times (-4 \times 1 - 3)\,.$$

We then deduce that

$$e_{r-1}/3 = (2^{k_{3,r}-3} - 1) - (2^2(8 - \alpha_{\overline{b_{3,r}}}) + 2) \preceq \omega_{3,r-2}\ ,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,

$$(2^{k_{3,r}} - \alpha_{b_{3,r}})/3 = (8 - \alpha_{\overline{b_{3,r}}}) + \sum_{j=1+\overline{b_{3,r}}}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+b_{3,r}} \preceq e_{r-1}\ ,$$

implying that $\omega_{3,r} \in \mathcal{E}_{3,r}$.

(3) Let ℓ be an integer such that $2 < \ell \leqslant 22$ and $k_{3,r} \geqslant k_{3,\ell} + 3\ell + b_{3,r} + 1$. While the proposition considers two cases, we split the first one into two, so that we consider three cases:

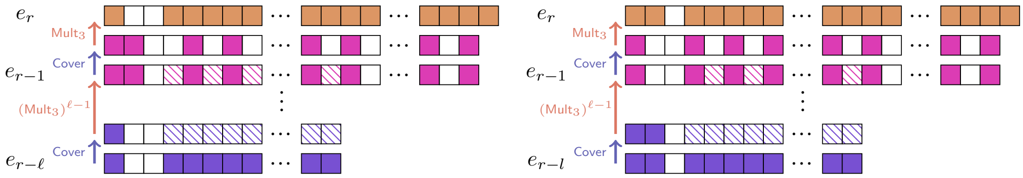
- **(a)** ℓ is even, with $b_{r-\ell} = b_{3,r}$,
- **(b)** ℓ is even, with $b_{r-\ell} = \overline{b_{3,r}}$,
- **(c)** ℓ is odd, with $b_{r-\ell} = \overline{b_{3,r}}$.

We will explain the procedure given in Figures 6.9, 6.9 and 6.10. On the first lines the squares 🟧 represent the active bits of e_r, on the third lines the squares 🟥 the active bits of e_{r-1}, where the squares ▨ are the $\varepsilon_i 2^i$ in the sum S, and on the fifth lines the squares 🟪 the active bits of $e_{r-\ell}$.

By hypothesis, $\omega_{3,r-\ell} = 2^{k_{3,r}-k_{3,\ell}} - \alpha_{b_{r-\ell}}$ belongs to $\mathcal{E}_{3,r-\ell}$.

We now choose

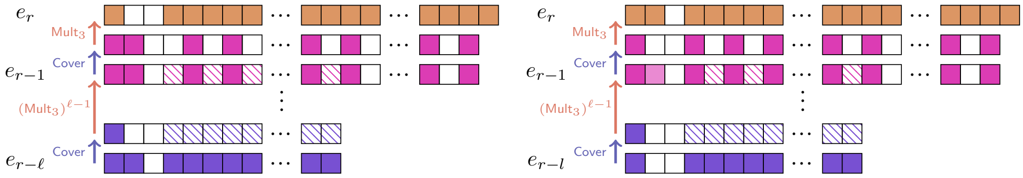
$$e_{r-1} = (8 - \alpha_{\overline{b_{3,r}}}) + \sum_{j=1+\overline{b_{3,r}}}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+b_{3,r}} + S\ ,$$



(a) $b_r = 0$.

(b) $b_r = 1$.

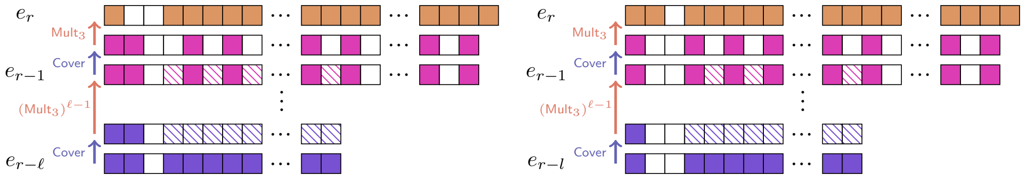
Figure 6.8: *How to derive* $\omega_{3,r}$ *from* $\omega_{3,r-\ell}$ *when* $\ell > 2$ *is even and* $b_{r-\ell} = b_{3,r}$.



(a) $b_r = 0$.

(b) $b_r = 1$.

Figure 6.9: *How to derive* $\omega_{3,r}$ *from* $\omega_{3,r-\ell}$ *when* $\ell > 2$ *is even and* $b_{r-\ell} = \overline{b_{3,r}}$.



(a) $b_r = 0$.

(b) $b_r = 1$.

Figure 6.10: *How to derive* $\omega_{3,r}$ *from* $\omega_{3,r-\ell}$ *when* $\ell > 2$ *is odd and* $b_{r-\ell} = \overline{b_{3,r}}$.

with

$$S = \begin{cases} \displaystyle\sum_{j=1+b_{3,r}}^{2\ell-1+b_{3,r}} \varepsilon_j 2^{2j+\overline{b_{3,r}}} & \text{in Cases } \textbf{(a)}, \textbf{(c)} \\ \displaystyle 2b_{3,r} + \sum_{j=1+b_{3,r}}^{2\ell-1+b_{3,r}} \varepsilon_j 2^{2j+\overline{b_{3,r}}} & \text{in Case } \textbf{(b)} \end{cases}$$

where the $(2\ell-1)$ coefficients $\varepsilon_j \in \{0,1\}$ are chosen such that $e_{r-1} \equiv 0 \bmod 3^{\ell-1}$. Indeed, it is known from Observation 6.2 that such a choice is always possible since $\ell \leqslant 22$.

We then use that

$$\begin{aligned} e_{r-1} &= \left((8 - \alpha_{\overline{b_{3,r}}}) + S + \sum_{j=1+\overline{b_{3,r}}}^{2\ell} 2^{2j+b_{3,r}} \right) + \sum_{j=2\ell+1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+b_{3,r}} \\ &< 2^{4\ell+b_{3,r}+1} + \sum_{j=2\ell+1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+b_{3,r}} \,. \end{aligned}$$

It follows that

$$\begin{aligned}
3e_{r-1} &< 3 \times \left(2^{4\ell+b_{3,r}+1} + \sum_{j=2\ell+1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor -1} 2^{2j+b_{3,r}} \right) \\
&\leqslant 2^{4\ell+b_{3,r}+1} + 2^{4\ell+b_{3,r}+2} + \sum_{j=4\ell+b_{3,r}+2}^{2\left\lfloor \frac{k_{3,r}}{2} \right\rfloor -1+b_{3,r}} 2^j \\
&\leqslant 2^{4\ell+b_{3,r}+1} + 2^{k_{3,r}} \,.
\end{aligned}$$

By hypothesis we have $k_{3,r} \geqslant k_{3,\ell} + 3\ell + b_{3,r} + 1$ so we deduce that

$$3e_{r-1} < 2^{k_{3,r}-k_{3,r-\ell}+\ell} + 2^{k_{3,r}} \,.$$

Moreover, since $\ell \leqslant 22$, we deduce from Observation 6.1 that

$$3e_{r-1} < 2^{k_{3,r}-k_{3,\ell}} \left(2^\ell + 2^{k_{3,\ell}}\right) \leqslant 2^{k_{3,r}-k_{3,\ell}} 3^\ell \,,$$

which implies that $e_{r-1} < 3^{\ell-1} 2^{k_{3,r}-k_{3,\ell}}$.
We deduce that, for proving that $e_{r-1}/3^{\ell-1} \preceq \omega_{3,r-\ell}$, it is sufficient to show that this holds for their remainders modulo 8. This last result comes from the following facts, for each of the three cases:

(a) ℓ is even, so $\left(3^{\ell-1}\right)^{-1} \equiv 3^{-1} \equiv 3 \bmod 8$. Since $S \equiv 0 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv 3e_{r-1} \equiv 3(8-\alpha_{\overline{b_{3,r}}}) \equiv (8-\alpha_{b_{3,r}}) \bmod 8$,

(b) ℓ is even, so $\left(3^{\ell-1}\right)^{-1} \equiv 3^{-1} \equiv 3 \bmod 8$. Since $S \equiv 2b_{3,r} \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv 3e_{r-1} \equiv 3(8-\alpha_{\overline{b_{3,r}}} + 2b_{3,r}) \equiv 1 \bmod 8$,

(c) ℓ is odd, so $\left(3^{\ell-1}\right)^{-1} \equiv 1^{-1} \equiv 1 \bmod 8$. Since $S \equiv 0 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv e_{r-1} \equiv (8-\alpha_{\overline{b_{3,r}}}) \bmod 8$.

So, we obtain that

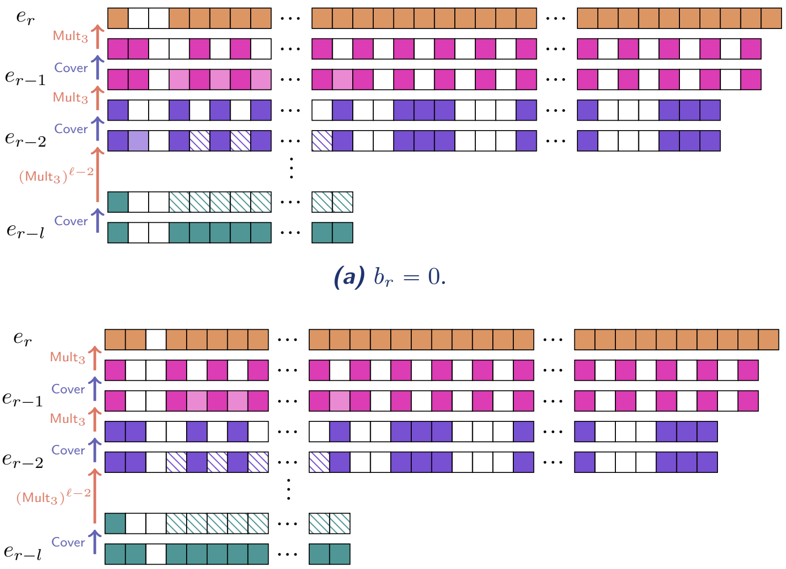
$$e_{r-1}/3^{\ell-1} \preceq \omega_{3,r-\ell} \,,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,

$$\frac{2^{k_{3,r}} - \alpha_{b_{3,r}}}{3} = (8-\alpha_{\overline{b_{3,r}}}) + \sum_{j=1+\overline{b_{3,r}}}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor -1} 2^{2j+b_{3,r}} = e_{r-1} - S \preceq e_{r-1} \,,$$

which proves that $\omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}} \in \mathcal{E}_{3,r}$.

(4) Let ℓ be an odd integer such that $2 < \ell \leqslant 22$, and satisfying $k_{3,r} \geqslant k_{3,\ell} + 3\ell + \overline{b_{3,r}} + 5$, and $b_{3,r-\ell} = b_{3,r}$. We will give the details of the procedure shown in Figure 6.11. On the first lines the squares 🟧 represent the active bits of e_r, on the third lines the squares 🟥 the active bits of e_{r-1}, on the fifth lines the squares 🟪 the active bits of e_{r-2}, where the squares ▨ are the $\varepsilon_i 2^i$ in the sum S, and on the seventh lines the squares 🟩 the active bits of $e_{r-\ell}$.



(a) $b_r = 0$.

(b) $b_r = 1$.

Figure 6.11: *How to derive* $\omega_{3,r}$ *from* $\omega_{3,r-\ell}$ *when* $\ell > 2$ *is odd and* $b_{r-\ell} = b_{3,r}$.

By hypothesis, $\omega_{3,r-\ell} = 2^{k_{3,r}-k_{3,\ell}} - \alpha_{b_{3,r}}$ belongs to $\mathcal{E}_{3,r-\ell}$. To simplify the notation, let $\gamma = \left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 3 \left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 5$. We now choose

$$e_{r-2} = (8 - \alpha_{b_{3,r}}) + \sum_{j=1+b_{3,r}}^{\gamma+b_{3,r}} 2^{2j+\overline{b_{3,r}}} + S + \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor+1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} ,$$

with

$$S = 2\overline{b_{3,r}} + \sum_{j=1+\overline{b_{3,r}}}^{\gamma} \varepsilon_j 2^{2j+b_{3,r}} ,$$

where the ε_j are chosen such that $e_{r-2} \equiv 0 \bmod 3^{\ell-2}$, which is always possible from Observation 6.2 since $\ell \leqslant 22$ and the number of coefficients ε_j in the sum is

$$\gamma - \overline{b_{3,r}} \geqslant \frac{k_{3,r} - b_{3,r} - k_{3,\ell} + \ell}{2} - 5 - \overline{b_{3,r}} \geqslant \frac{4\ell - \overline{b_{3,r}} - b_{3,r} + 5}{2} - 5 ,$$

so that $\gamma - \overline{b_{3,r}} \geqslant 2\ell - 3 = 2(\ell - 2) + 1$. Then, we have

$$\begin{aligned} e_{r-2} &< \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor+1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-6\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor-7} \\ &\leqslant \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor+1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-k_{3,\ell}+\ell-7} . \end{aligned}$$

It follows that

$$\begin{aligned}
9e_{r-2} &< 9 \times \left(\sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-k_{3,\ell}+\ell-7} \right) \\
&\leqslant 9 \times \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} 7 \times 2^{k_{3,r}-6j} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-7} \\
&\leqslant (2^6 - 1) \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} 2^{k_{3,r}-6j} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-7} \\
&\leqslant \sum_{j=0}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor} 2^{k_{3,r}-6j} - \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} 2^{k_{3,r}-6j} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-7} \, ,
\end{aligned}$$

from which we deduce that

$$\begin{aligned}
9e_{r-2} &\leqslant 2^{k_{3,r}} - 2^{k_{3,r}-6\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 6} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-7} \\
&< 2^{k_{3,r}} + 2^{k_{3,r}-k_{3,\ell}+\ell} \, .
\end{aligned}$$

Using Corollary 6.1 we get

$$9e_{r-2} < 2^{k_{3,r}-k_{3,\ell}} \left(2^{k_{3,\ell}} + 2^{\ell} \right) < 3^{\ell} 2^{k_{3,r}-k_{3,\ell}} \, .$$

We then deduce that

$$e_{r-2} < 3^{\ell-2} 2^{k_{3,r}-k_{3,\ell}} \, .$$

Therefore, it is now sufficient to prove that $e_{r-2}/3^{\ell-2} \equiv 1 \bmod 8$ in order to prove that $e_{r-2}/3^{\ell-2} \preceq \omega_{3,r-\ell}$. This result on the remainders modulo 8 comes from the fact that $3^{\ell-2} \equiv 3 \bmod 8$ since ℓ is odd. Moreover $S \equiv 2\overline{b_{3,r}} \bmod 8$, leading to

$$e_{r-2}/3^{\ell-2} \equiv 3e_{r-2} \equiv 3(8 - \alpha_{b_{3,r}} + 2\overline{b_{3,r}}) \equiv 1 \bmod 8 \, .$$

So, we have

$$e_{r-2}/3^{\ell-2} \preceq \omega_{3,r-\ell} \, ,$$

implying that e_{r-2} belongs to $\mathcal{E}_{3,r-2}$. Let now

$$e_{r-1} = (8 - \alpha_{\overline{b_{3,r}}}) + \sum_{j=1+\overline{b_{3,r}}}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+b_{3,r}} + \sum_{j=1+b_{3,r}}^{\gamma+b_{3,r}} 2^{2j+\overline{b_{3,r}}} \, .$$

We use that

$$(8 - \alpha_{\overline{b_{3,r}}}) + b_{3,r} 2^3 = 3(8 - \alpha_{b_{3,r}}) \, .$$

Then, let us observe that for any $K \geqslant 6$:

$$3 \left(\sum_{j=1+b_{3,r}}^{K-5+b_{3,r}} 2^{2j+\overline{b_{3,r}}} \right) = \sum_{j=1+b_{3,r}}^{K-5+b_{3,r}} 2^{2j+\overline{b_{3,r}}} + \sum_{j=1+\overline{b_{3,r}}}^{K-4} 2^{2j+b_{3,r}} - b_{3,r} 2^3$$

implying that

$$e_{r-1} = 3(8-\alpha_{b_{3,r}}) + 3\left(\sum_{j=1+b_{3,r}}^{\gamma+b_{3,r}} 2^{2j+\overline{b_{3,r}}}\right) + \sum_{j=\gamma+2}^{\left\lfloor \frac{k_{3,r}}{2}\right\rfloor -1} 2^{2j+b_{3,r}}\ .$$

Moreover, since

$$\begin{aligned}\sum_{j=\gamma+2}^{\left\lfloor \frac{k_{3,r}}{2}\right\rfloor -1} 2^{2j+b_{3,r}} &= \sum_{j=1}^{3\left\lfloor \frac{k_{3,\ell}-\ell}{6}\right\rfloor +3} 2^{k_{3,r}-2i} \\ &= \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6}\right\rfloor +1} \left(2^{k_{3,r}-6i} + 2^{k_{3,r}-6i+2} + 2^{k_{3,r}-6i+4}\right)\end{aligned}$$

we deduce that

$$\sum_{j=\gamma+2}^{\left\lfloor \frac{k_{3,r}}{2}\right\rfloor -1} 2^{2j+b_{3,r}} = 3\left(\sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6}\right\rfloor +1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)}\right).$$

Then we obtain

$$\begin{aligned}\frac{e_{r-1}}{3} &= (8-\alpha_{b_{3,r}}) + \sum_{j=1+b_{3,r}}^{\gamma+b_{3,r}} 2^{2j+\overline{b_{3,r}}} + \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6}\right\rfloor +1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} \\ &= e_{r-2} - S \\ &\preceq e_{r-2}\ ,\end{aligned}$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Finally,

$$\frac{2^{k_{3,r}}-\alpha_{b_{3,r}}}{3} = (8-\alpha_{\overline{b_{3,r}}}) + \sum_{j=1+\overline{b_{3,r}}}^{\left\lfloor \frac{k_{3,r}}{2}\right\rfloor -1} 2^{2j+b_{3,r}} \preceq e_{r-1}\ ,$$

implying that $\omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}} \in \mathcal{E}_{3,r}$.

□

6.1.3 MILP-based Algorithm

The induction procedure from Proposition 6.4 relies on some assumptions which are not satisfied for some values of r. These sporadic cases then need to be handled in a different (but more expensive) way. According to Proposition 6.3, rounds r such that $(s_1 \dots s_r)$ is a palindrome are the only ones for which there is no $\ell < r$ such that $k_{3,r-\ell} = k_{3,r} - k_{3,\ell}$. Then, Proposition 6.4 does not apply to these values of r. Moreover, in this proposition, we impose $\ell \leqslant 22$, since Observation 6.2 has been proved up to $\ell \leqslant 22$ only. Also, we add an additional constraint on $k_{3,r} - k_{3,\ell} - 3\ell$. This constraint is mainly due to the $2t+1$ coefficients needed to construct an element of $\mathbb{Z}/3^t\mathbb{Z}$ with powers of 4 in Observation 6.2. Indeed in the inductive proof, when we want to construct multiples of $3^{\ell+1}$ or $3^{\ell+2}$, we add a sum S that must be sufficiently low in order to apply Observation 6.1 which compares powers of 3^r with powers of $2^{k_{3,r}}$.

Let $1 \leqslant r \leqslant 16265$, such that we are not in a case of a palindromic sequence, then by computing the minimum values in $\mathcal{L}_r$, we can exhibit all the rounds for which there is no ℓ satisfying the two constraints of Proposition 6.4:

- If $r = 19, 24$, then $\min(\mathcal{L}_r)$ is respectively 7 or 12. However, the hypotheses of Proposition 6.4 are not satisfied:

$$k_{3,19} = 30 < 33 = k_{3,7} + 3 \times 7 + b_{19} + 1,$$
$$k_{3,24} = 38 < 56 = k_{3,12} + 3 \times 12 + b_{24} + 1.$$

- If r belongs to the set

$$\{665\lambda + 53\mu, 0 \leqslant \lambda \leqslant 24, 0 \leqslant \mu \leqslant 6\}\text{U}\{359 + 665\lambda + 53\mu, 0 \leqslant \lambda \leqslant 23, 0 \leqslant \mu \leqslant 5\}\ ,$$

  then we have $\min(\mathcal{L}_r) \geqslant 53$.

Let us recall that, when the univariate degree 3^r is lower than $2^n - 1$, we necessarily have $3^r \in \mathcal{E}_{3,r}$. Consequently, for these particular r, we will search for ℓ such that $3^{r-\ell} \in \mathcal{E}_{3,r-\ell}$ implies that $\omega_{3,r} \in \mathcal{E}_{3,r}$. This can be done by exhibiting a sequence of operations, composed of Cover and Mult$_3$, which generates $\omega_{3,r}$ from $3^{r-\ell}$. These functions a priori need to be iterated ℓ times but, since $x \in \mathsf{Cover}(x)$, we can ignore some calls to Cover.

It is possible to encode the existence of such a sequence of operations as a MILP problem that is then solved using `PySCIPOpt` [Gam+20], an off-the-shelf solver. This encoding works as follows. Integers are represented via their binary representation over n bits. We use two sets of intermediate variables for each round r, namely $(a_i^r)_{0\leqslant i<n}$ and $(b_i^r)_{0\leqslant i<n}$, corresponding to the integers a^r and b^r which are such that

$$b^r \in \mathsf{Cover}(\{a^r\}) \text{ and } a^{r+1} \in \mathsf{Mult}_3\left(\{b^r\}\right)\ .$$

The relation $b^r = \mathsf{Cover}(a^r)$ is easily encoded as a set of MILP equations since it corresponds to $b_i^r \leqslant a_i^r$ for all $i \in \{0, ..., n-1\}$. In order to ensure that $a^{r+1} = 3b^r$, we use a bitwise description of the multiplication by 3 that can be found for instance in [Bro+21]. By setting $a^{r-\ell} = 3^{r-\ell}$ and $a^r = \omega_{3,r}$, we have that the existence of a solution to all the previously described equations is equivalent to the fact that a^r is in $(\mathsf{Mult}_3 \circ \mathsf{Cover})^\ell(\{3^{r-\ell}\})$, meaning that it is indeed in $\mathcal{E}_{3,r}$. We illustrate the following procedure in Figure 6.12.

This technique is rather slow, and it cannot be applied to large values of r. Indeed, the experiments were ran on a cluster with an Intel Xeon Gold 5218 processor and 192GB of RAM, for which we were limited to one week of computation. However, it plays a crucial role in our proof of Theorem 6.1.

Table 6.4 provides the values of all $r \leqslant 16265$ corresponding to the length of a palindromic sequence for which it has been checked with our MILP-based algorithm that $\omega_{3,r} \in \mathcal{E}_{3,r}$. The next palindromic sequence is for $r = 16266$ and is out of reach using our MILP solver.

Similarly, Table 6.5 covers the first values of r for which there is no ℓ satisfying one of the situations of Proposition 6.4.

The first value of r for which the cost becomes too high to obtain a result from the solver is $r = 465$. Thus, if $R = \{665\lambda + 53\mu,\ 0 \leqslant \lambda \leqslant 23, 0 \leqslant \mu \leqslant 5\}$, then, up to 16265, the only

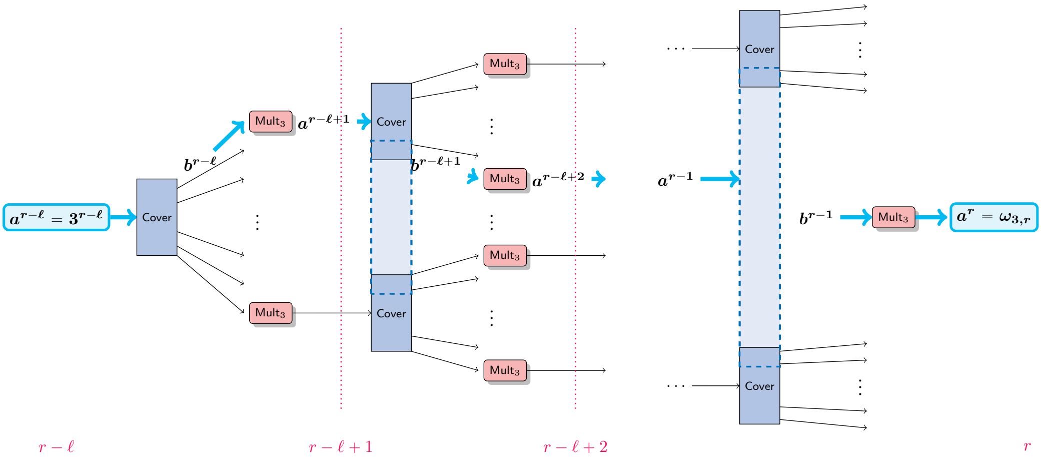


Figure 6.12: *How to search for maximum-weight exponents with MILP.*

r	7	12	53	359	665
$2^{k_{3,r}} - \alpha_{b_{3,r}}$	$2^{11}-5$	$2^{19}-5$	$2^{84}-7$	$2^{569}-5$	$2^{1054}-7$
ℓ	2	3	4	6	7

Table 6.4: *Lengths r of palindromic sequences for which it has been proved with a MILP algorithm that $\omega_{3,r} \in \mathcal{E}_{3,r}$, using that $3^{r-\ell} \in \mathcal{E}_{3,r-\ell}$.*

r	19	24	106	159	212
$2^{k_{3,r}} - \alpha_{b_{3,r}}$	$2^{30}-7$	$2^{38}-7$	$2^{168}-7$	$2^{252}-7$	$2^{336}-7$
ℓ	4	3	6	5	6

r	265	318	412	518	624
$2^{k_{3,r}} - \alpha_{b_{3,r}}$	$2^{420}-7$	$2^{504}-7$	$2^{653}-5$	$2^{821}-5$	$2^{989}-5$
ℓ	5	6	9	7	7

Table 6.5: *ℓ such that $3^{r-\ell} \in \mathcal{E}_{3,r-\ell}$ implies $\omega_{3,r} \in \mathcal{E}_{3,r}$.*

rounds for which we cannot definitively prove the presence of maximum-weight exponents are the following ones (in red in Figure 6.13):

$$\mathcal{F} = \big((359+R)\cup(665+R)\cup(718+R)\big)\backslash\mathcal{V}\,, \quad \text{where } \mathcal{V} = \{359, 412, 518, 624, 665\}\,.$$

The last relevant point we need is to check that the rounds belonging to $\mathcal{F}$ do not raise any problem to build a recurrence on elements of $\boldsymbol{R} = \{4 \leqslant r \leqslant 16265 \ \text{ s.t. } r \notin \mathcal{F}\}$. The following observation has been checked by computer, by looping through all $\ell \in \mathcal{L}_r$.

Observation 6.3. For any $r \in \boldsymbol{R}$, there exists $\ell \in \mathcal{L}_r$ such that $r - \ell$ belongs to $\boldsymbol{R}$.

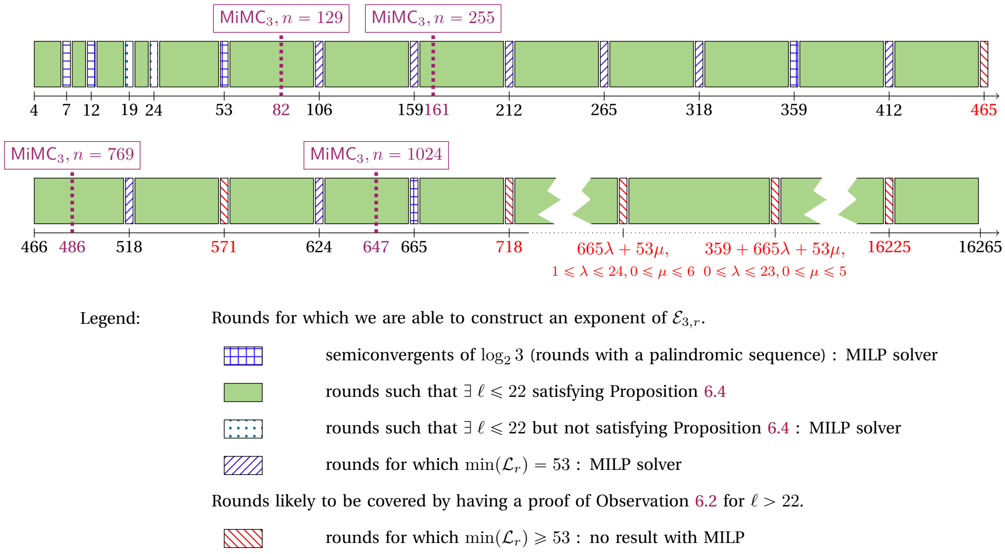

MiMC$_3$, $n = 129$
MiMC$_3$, $n = 255$
4
7
12
19
24
53
82
106
159
161
212
265
318
359
412
465
MiMC$_3$, $n = 769$
MiMC$_3$, $n = 1024$
466
486
518
571
624
647
665
718
$665\lambda + 53\mu$,
$1 \leqslant \lambda \leqslant 24, 0 \leqslant \mu \leqslant 6$
$359 + 665\lambda + 53\mu$,
$0 \leqslant \lambda \leqslant 23, 0 \leqslant \mu \leqslant 5$
16225
16265
Legend:
Rounds for which we are able to construct an exponent of $\mathcal{E}_{3,r}$.
▦ semiconvergents of $\log_2 3$ (rounds with a palindromic sequence) : MILP solver
🟩 rounds such that $\exists\, \ell \leqslant 22$ satisfying Proposition 6.4
⋮ rounds such that $\exists\, \ell \leqslant 22$ but not satisfying Proposition 6.4 : MILP solver
▨ rounds for which $\min(\mathcal{L}_r) = 53$: MILP solver
Rounds likely to be covered by having a proof of Observation 6.2 for $\ell > 22$.
▧ rounds for which $\min(\mathcal{L}_r) \geqslant 53$: no result with MILP

***Figure 6.13:** Rounds for which we are able to exhibit a maximum-weight exponent.*

6.1.4 Combining Both Steps

As a consequence, we are now able to construct, by induction, maximum-weight exponents for all rounds until 464, and for almost all rounds until 16265.

Theorem 6.1. *Let $\boldsymbol{R}$ be the set $\{4, \ldots, 16265\} \backslash \mathcal{F}$, where $\mathcal{F} = \big((359 + R) \cup (665 + R) \cup (718 + R)\big) \backslash \mathcal{V}$ with*

$$R = \{665\lambda + 53\mu,\ 0 \leqslant \lambda \leqslant 23, 0 \leqslant \mu \leqslant 5\},$$
$$\mathcal{V} = \{359, 412, 518, 624, 665\}\ .$$

Then $\omega_{3,r} \in \mathcal{E}_{3,r}$ for all $r \in \boldsymbol{R}$.

Proof. We prove the result by induction on r. Let $(\mathcal{H}_r)$ be the following hypothesis:

$$(\mathcal{H}_r) : \forall 4 \leqslant i < r, i \in \boldsymbol{R},\ \omega_{3,i} = 2^{k_{3,i}} - \alpha_{b_{3,i}} \in \mathcal{E}_{3,i}$$

- **For $r = 5$:**
$$(\mathcal{H}_5) : \forall 4 \leqslant i < 5, i \in \boldsymbol{R},\ \omega_{3,i} \in \mathcal{E}_{3,i}$$
is satisfied since:
$$2^{k_{3,4}} - \alpha_{b_4} = 2^6 - 7 = 57 \in \mathcal{E}_{3,4}\ .$$

- **Induction step.** We assume that $(\mathcal{H}_r)$ is satisfied, then we will show that $(\mathcal{H}_{r+1})$ is also satisfied. If $(s_1, \ldots, s_r)$ is a palindrome, or if there is no ℓ that satisfies the conditions of Proposition 6.4 then $\omega_{3,r} \in \mathcal{E}_{3,r}$ as summarized in Table 6.4 and Table 6.5.
Otherwise, according to Proposition 6.3, we know that $\mathcal{L}_r \neq \varnothing$ so that there exists $\ell \in \mathcal{L}_r$. Moreover, we know from Observation 6.3 that there is always a round $r - \ell \in \boldsymbol{R}$ so that we can use Proposition 6.4, and prove that we have $\omega_{3,r} \in \mathcal{E}_{3,r}$ since $\omega_{3,r-\ell} \in \mathcal{E}_{3,r-\ell}$.

□

We are now able to give precise guarantees on the algebraic degree of $\mathsf{MiMC}_3[r]$. The result given in Corollary 6.2 will then be of fundamental interest in Section 6.5 when studying higher-order differential attacks.

Corollary 6.2. *Let* $r \in \boldsymbol{R}$ *be an integer, then the algebraic degree after* r *rounds of* MiMC_3 *satisfies:*

$$B_3^r = 2 \times \lceil k_{3,r}/2 - 1 \rceil \,,$$

where $k_{3,r} = \lfloor r \log_2 3 \rfloor$.

Proof. Proposition 5.10 proves that $2 \times \lceil k_{3,r}/2 - 1 \rceil$ is an upper bound on the degree, and Theorem 6.1 exhibits some exponents that reach the degree at each round when $r \in \boldsymbol{R}$. □

Although Corollary 6.2 does not allow to cover all the rounds, the number of rounds of MiMC_3 we are interested in is fully covered ($\simeq 80$ when $n = 129$), as shown in Figure 6.13. For the hash functions, we need to cover 486 and 687 rounds. In these cases, we have the exact value of B_3^r for all rounds needed, except for $r \in \{465, 571\}$. Recalling that $(B_3^r)_{r \geqslant 1}$ is a non decreasing sequence (see Proposition 5.2) and that B_3^r is upper bounded by $2 \times \lceil k_{3,r}/2 - 1 \rceil$ (see Proposition 5.10), we have:

$$734 = B_3^{464} \leqslant B_3^{465} \leqslant 736 \,,$$
$$902 = B_3^{570} \leqslant B_3^{571} \leqslant 904 \,.$$

By observing that $\lceil k_{3,r}/2 - 1 \rceil \leqslant \lceil k_{3,r-1}/2 - 1 \rceil + 1$, we deduce that, between two consecutive rounds, the degree increases by 2 or remains stable, in which case we have a plateau. More precisely, as shown in Corollary 6.3, there is a plateau in the growth of the algebraic degree between rounds r and $r+1$, when $k_{3,r}$ is odd and $k_{3,r+1}$ is even.

Corollary 6.3. *Let* $(b_{3,r})_{r \geqslant 4}$ *be the sequence defined by* $b_{3,r} = k_{3,r} \bmod 2$. *Then we have*

$$B_3^r = B_3^{r+1} \quad \textit{if and only if} \quad (b_{3,r} b_{3,r+1}) = (10) \,.$$

Proof. According to Corollary 6.2, we have $B_3^r = 2 \times \lceil k_{3,r}/2 - 1 \rceil$. Then, let us investigate the four cases depending on the sequence $(b_{3,r} b_{3,r+1})$.

- If $(b_{3,r} b_{3,r+1}) = (00)$, then
$$B_3^r = k_{3,r} - 2 \quad \text{and} \quad B_3^{r+1} = k_{3,r+1} - 2 = k_{3,r} \,.$$
- If $(b_{3,r} b_{3,r+1}) = (01)$, then
$$B_3^r = k_{3,r} - 2 \quad \text{and} \quad B_3^{r+1} = k_{3,r+1} - 1 = k_{3,r} \,.$$
- If $(b_{3,r} b_{3,r+1}) = (10)$, then
$$B_3^r = k_{3,r} - 1 \quad \text{and} \quad B_3^{r+1} = k_{3,r+1} - 2 = k_{3,r} - 1 \,.$$
- If $(b_{3,r} b_{3,r+1}) = (11)$, then
$$B_3^r = k_{3,r} - 1 \quad \text{and} \quad B_3^{r+1} = k_{3,r+1} - 1 = k_{3,r} + 1 \,.$$

It follows that the only sequence such that $B_3^r = B_3^{r+1}$ is $(b_{3,r} b_{3,r+1}) = (10)$. □

This implies that two consecutive plateaus correspond to 3 switches in the parity of $(k_{3,r})_{r>0}$. From Proposition 6.2, we know that

$$\sum_{i=1}^{\ell} s_{r+i} \in \{2\ell - 1 - k_{3,\ell}, 2\ell - k_{3,\ell}\} \ . \tag{6.2}$$

We deduce that $\sum_{i=1}^{4} s_{r+i} \leqslant 2$ and $\sum_{i=1}^{8} s_{r+i} \geqslant 4$, which implies that, if there is a plateau between rounds r and $(r+1)$, then the next plateau starts at round $(r+4)$, $(r+5)$ or $(r+6)$. By using (6.2) for $2 \leqslant \ell \leqslant 7$, we deduce that there are exactly three possible patterns for a subsequence of $(s_r)_{r>0}$ starting by 1 and having Hamming weight 3, namely

$$\begin{aligned} s_{r+1} \dots s_{r+5} &= 10101 \ , \\ s_{r+1} \dots s_{r+6} &= 101001 \ , \\ s_{r+1} \dots s_{r+6} &= 100101 \ . \end{aligned}$$

Overall, Corollary 6.2 ensures that the higher-order differential attacks described in Section 6.5 have minimal complexity.

6.2 More maximum-weight exponents for MiMC$_3$

In the previous section we have identified one exponent at each round that reaches the degree, but in practice, it is not unique. Indeed, Figure 6.14 shows the number of maximum-weight exponents per round, derived from the C implementation of Proposition 5.1 that gives all the exponents appearing in each round, and in particular those of maximum weight.

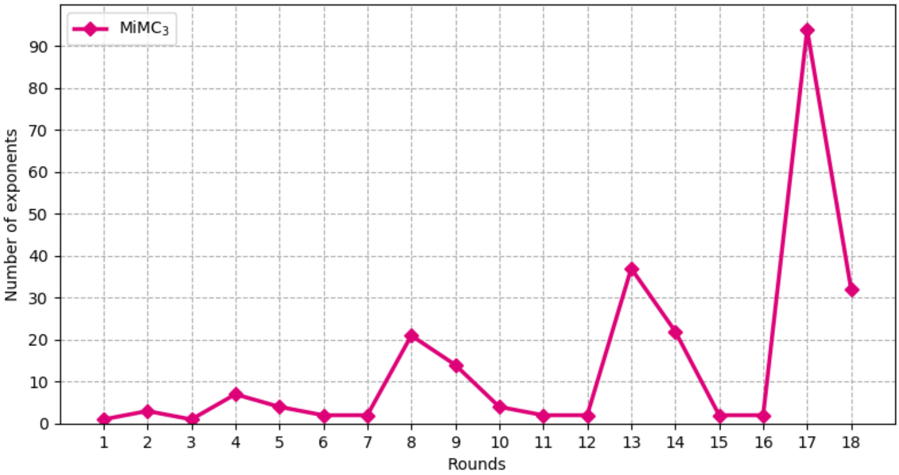


Figure 6.14: Number of maximum-weight exponents

We can observe that for some rounds there are very few maximum-weight exponents. Such an event is linked with $b_{3,r}$, i.e. the parity of $k_{3,r} = \lfloor \log_2 3 \rfloor$, as we will see in the following. We complete Theorem 6.1 with other exponents of maximum weight. Then we will distinguish cases depending on the parity of $\lfloor r \log_2 3 \rfloor$ and the previous rounds. Our approach consists in investigating Conjecture 6.3.

Conjecture 6.3. *Let $r \geqslant 6$. Then, the maximum-weight exponents in $\mathcal{E}_{3,r}$ include the set $\mathcal{M}_{3,r}$ defined as follows, where α can take any value in $\{2, 5\}$:*

- *if $k_{3,r}$ is odd:*

$$\mathcal{M}_{3,r} := \{2^{k_{3,r}} - \alpha\} ,$$

- *if $k_{3,r}$ is even:*
  - *if $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (000)$:*

$$\mathcal{M}_{3,r} := \{2^{k_{3,r}-1} - \alpha, 2^{k_{3,r}} - \alpha - 2\} ,$$

  - *if $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (100)$:*

$$\mathcal{M}_{3,r} := \{2^{k_{3,r}-1} - \alpha\} \cup \left\{2^{k_{3,r}} - 2^{2j_1+1} - \alpha, 0 \leqslant j_1 \leqslant \frac{k_{3,r}}{2} - 2\right\} ,$$

  - *if $(b_{3,r-1}b_{3,r}) = (10)$:*

$$\begin{aligned}\mathcal{M}_{3,r} := \{2^{k_{3,r}-1} - \alpha\} &\cup \left\{2^{k_{3,r}} - 2^{2j_1+1} - \alpha, 0 \leqslant j_1 \leqslant \frac{k_{3,r}}{2} - 2\right\} \\ &\cup \left\{2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 2^{2j_2} - \alpha, 2 \leqslant j_2 \leqslant \frac{k_{3,r}}{2} - 1\right\} \\ &\cup \{2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 6\} .\end{aligned}$$

  Moreover, when $(b_{3,r-1}b_{3,r}) = (10)$, and $k_{3,r-5}$ is odd, with $k_{3,r-5} = k_{3,r} - 7$, $\mathcal{E}_{3,r}$ also includes:

$$\begin{aligned}&\left\{2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 2^{2j_3+1} - \alpha, 0 \leqslant j_3 \leqslant \frac{k_{3,r}}{2} - 2\right\} \\ \cup &\left\{2^{k_{3,r}+1} - 2^{k_{3,r}-3} - 2^{2j_4} - \alpha, 2 \leqslant j_4 \leqslant \frac{k_{3,r}}{2} - 2\right\} ,\end{aligned}$$

While the most general case remains a conjecture at the time of writing, in what follows, we show that the conjecture is true for all $r \leqslant 411$. For the sake of consistency, we will use the notation of the previous section. In particular, we rely on sequences $(e_{r-\ell} \ldots e_r)$ such that each e_{r-i}, $0 < i \leqslant \ell$, belongs to $\mathcal{E}_{3,r-i}$ and our procedure is again divided in two parts.

- We present an inductive procedure establishing that, for most values of r, $e_r \in \mathcal{E}_{3,r}$ using the fact that $e_{r-\ell} \in \mathcal{E}_{3,r-\ell}$ for some $\ell < r$.
- We describe a MILP-based computationally intensive procedure to prove that $e_r \in \mathcal{E}_{3,r}$ for some sporadic values of r, corresponding to the cases which are not covered by the inductive procedure.
- These results and algorithms are then put together in order to prove Proposition 6.5.

$k_{3,r}$	$b_{3,r-2}$	$b_{3,r-1}$	$b_{3,r}$	Corresponding lemma
odd	0	0	1	Lemma 6.1-Figure 6.15
	0	1	1	Lemma 6.1-Figure 6.16
	1	1	1	Lemma 6.1-Figure 6.17
even	1	1	0	Lemma 6.3-Figure 6.23
	1	0	0	Lemma 6.2-Figure 6.22
	0	0	0	Lemma 6.4-Figure 6.24

Table 6.6: *Corresponding lemma for each sequence $(b_{3,r-2}b_{3,r-1}b_{3,r})$ studied.*

6.2.1 Inductive Procedure

As we need to distinguish cases depending on the parity of $\lfloor r \log_2 3 \rfloor$ and the previous rounds, we will give the results in distinct lemmas as explained in Table 6.6.

First, let us consider a round r such that $k_{3,r} = \lfloor r \log_2 3 \rfloor$ is odd. The following lemma exhibits some conditions under which the maximum-weight exponent $2^{k_{3,r}} - 2$ belongs to $\mathcal{E}_{3,r}$.

Lemma 6.1. *Let $(k_{3,r})_{r>0}$ be the sequence defined by $k_{3,r} = \lfloor r \log_2 3 \rfloor$, and $(b_{3,r})_{r>0}$ the sequence defined by $b_{3,r} = k_{3,r} \bmod 2$. Let $r \geqslant 6$, with $b_{3,r} = 1$, and $\ell \in \mathcal{L}_r$ such that one of the following situations occurs:*

(1) $\ell = 2$,

(2) $2 < \ell \leqslant 22$ *such that* $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 2$, *and one of the following situations occurs:*

- *ℓ is even, or*
- *ℓ is odd, with $b_{3,r-\ell} = b_{3,r} = 1$;*

(3) $2 < \ell \leqslant 22$ *is odd such that* $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 5$ *and* $b_{3,r-\ell} = \overline{b_{3,r}} = 0$.

If $2^{k_{3,r}-k_{3,\ell}} - 2 \in \mathcal{E}_{3,r-\ell}$ *when* $b_{3,r-\ell} = b_{3,r} = 1$ *or if* $2^{k_{3,r}-k_{3,\ell}} - 7 \in \mathcal{E}_{3,r-\ell}$ *when* $b_{3,r-\ell} = \overline{b_{3,r}} = 0$, *then* $2^{k_{3,r}} - 2 \in \mathcal{E}_{3,r}$.

Before giving the proof, we propose Figures 6.15, 6.16 and 6.17 to give a first idea of the procedure we will use. Figures 6.15 and 6.16 have been obtained by combining the first item of the lemma with the result given in Proposition 6.4. For example, on Figure 6.15, we see that we can derive $2^{k_{3,r}} - 5$, from $2^{k_{3,r-1}} - 7$ appearing at round $(r-1)$ (Proposition 6.4) and $2^{k_{3,r}} - 2$, from $2^{k_{3,r-3}} - 7$ appearing at round $(r-2)$ (the above lemma).

On Figure 6.16, we observe that both $2^{k_{3,r}} - 5$ and $2^{k_{3,r}} - 2$ can be derived from $2^{k_{3,r-3}} - 7$ appearing at round $(r-2)$ (Proposition 6.4 and the above lemma respectively).

To illustrate the idea behind the other items of the lemma, we propose to give an example for the case ℓ odd, with $b_{3,r-\ell} = 0$. On Figure 6.17, we notice that both $2^{k_{3,r}} - 5$ and $2^{k_{3,r}} - 2$ can be derived from $2^{k_{3,r-11}} - 7$ appearing at round $(r-7)$ i.e. $\ell = 7$. The trail for $2^{k_{3,r}} - 5$ was found in Proposition 6.4 and the trail for $2^{k_{3,r}} - 2$ will be given in the following proof.

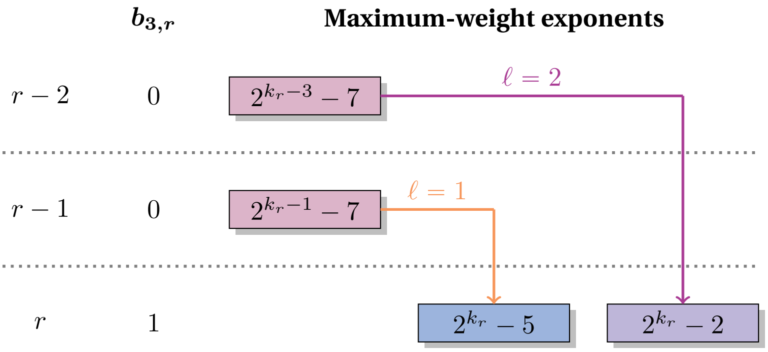


Figure 6.15: *Tracing exponents when* $(b_{3,r-1}b_{3,r}) = (01)$.

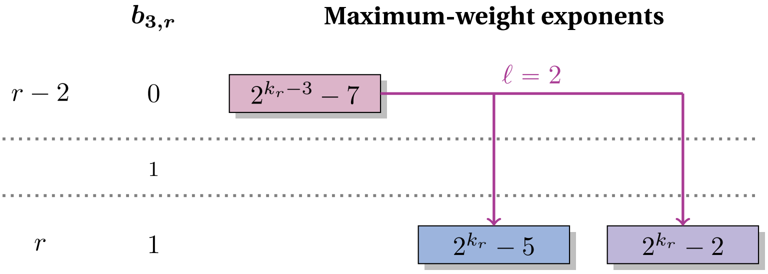


Figure 6.16: *Tracing exponents when* $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (011)$.

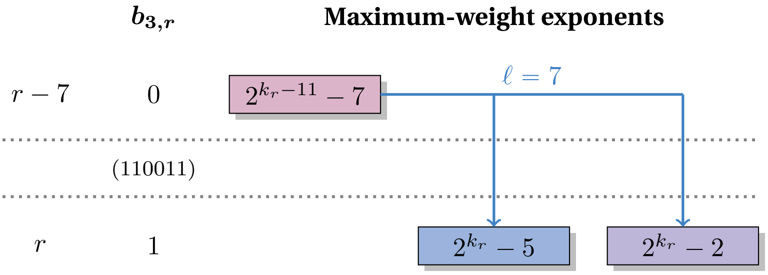


Figure 6.17: *Tracing exponents when* $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (111)$.

Proof of Lemma 6.1. **(1)** Let $\ell = 2$. We have $k_{3,r-2} = k_{3,r} - 3$ and $b_{3,r-2} = \overline{b_{3,r}} = 0$. Therefore, by hypothesis, $e_{r-2} = 2^{k_{3,r}-3} - 7$ belongs to $\mathcal{E}_{3,r-2}$. Let us choose

$$e_{r-1} = 11 + \sum_{j=5}^{k_{3,r}-4} 2^j + 2^{k_{3,r}-2} .$$

Then, we have

$$e_{r-1} = 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 21 .$$

We deduce that

$$e_{r-1}/3 = 2^{k_{3,r}-3} - 7 = \omega_{3,r-2} ,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,

$$(2^{k_{3,r}}-2)/3 = \sum_{j=0}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor -1} 2^{2j+1} \preceq e_{r-1} \ ,$$

implying that $2^{k_{3,r}}-2 \in \mathcal{E}_{3,r}$.

(2) Let ℓ be an integer such that $2 < \ell \leqslant 22$, and $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 2$. While the proposition considers two cases, we split the first one into two, so that we consider three cases:

(a) ℓ is even, with $b_{3,r-\ell} = b_{3,r} = 1$,

(b) ℓ is even, with $b_{3,r-\ell} = \overline{b_{3,r}} = 0$,

(c) ℓ is odd, with $b_{3,r-\ell} = b_{3,r} = 1$.

Figures 6.18, 6.19 and 6.20 illustrate the procedure below. On the first lines the squares 🟧 represent the active bits of e_r, on the third lines the squares ■ the active bits of e_{r-1}, where the squares ▨ are the $\varepsilon_i 2^i$ in the sum S, and on the fifth lines the squares 🟪 the active bits of $e_{r-\ell}$.

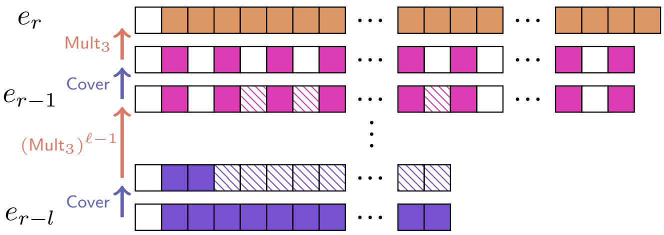


Figure 6.18: *How to derive $2^{k_{3,r}}-2$ when $\ell > 2$ is even and $b_{3,r-\ell} = b_{3,r} = 1$.*

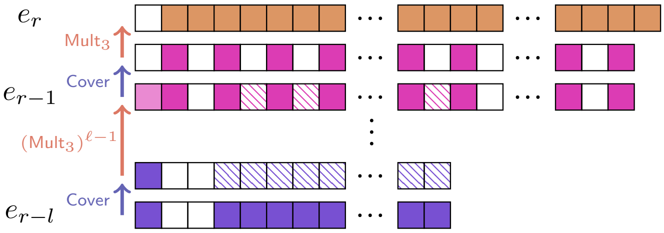


Figure 6.19: *How to derive $2^{k_{3,r}}-2$ when $\ell > 2$ is even and $b_{3,r-\ell} = \overline{b_{3,r}} = 0$.*

By hypothesis, $e_{r-\ell} = 2^{k_{3,r}-k_{3,\ell}}-2$ belongs to $\mathcal{E}_{3,r-\ell}$ in Cases **(a)**,**(c)**, and $e_{r-\ell} = 2^{k_{3,r}-k_{3,\ell}}-7$ belongs to $\mathcal{E}_{3,r-\ell}$ in Case **(b)**.

We now choose

$$e_{r-1} = 2 + \sum_{j=1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor -1} 2^{2j+1} + S \ ,$$

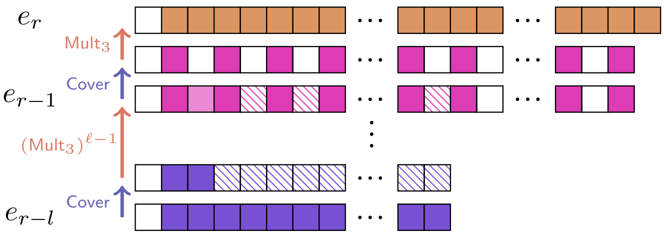


Figure 6.20: *How to derive* $2^{k_{3,r}} - 2$ *when* $\ell > 2$ *is odd and* $b_{3,r-\ell} = b_{3,r} = 1$.

with

$$S = \begin{cases} \sum_{j=2}^{2\ell} \varepsilon_j 2^{2j} & \text{in Case } \textbf{(a)} \\ 1 + \sum_{j=2}^{2\ell} \varepsilon_j 2^{2j} & \text{in Case } \textbf{(b)} \\ 4 + \sum_{j=2}^{2\ell} \varepsilon_j 2^{2j} & \text{in Case } \textbf{(c)} \end{cases}$$

where the $(2\ell - 1)$ coefficients $\varepsilon_j \in \{0, 1\}$ are chosen such that $e_{r-1} \equiv 0 \bmod 3^{\ell-1}$. Indeed, it is known from Observation 6.2 that such a choice is always possible since $\ell \leqslant 22$.

We then use that

$$\begin{aligned} e_{r-1} &= \left(2 + S + \sum_{j=1}^{2\ell} 2^{2j+1}\right) + \sum_{j=2\ell+1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+1} \\ &< 2^{4\ell+2} + \sum_{j=1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 2\ell - 1} 2^{k_{3,r} - 2j} . \end{aligned}$$

It follows that

$$\begin{aligned} 3e_{r-1} &< 3 \times \left(2^{4\ell+2} + \sum_{j=1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 2\ell - 1} 2^{k_{3,r} - 2j} \right) \\ &\leqslant 2^{4\ell+2} + 2^{k_{3,r}} \\ &\leqslant 2^{k_{3,r} - k_{3,\ell} + \ell} + 2^{k_{3,r}} \end{aligned}$$

where the last inequality comes from the hypothesis on ℓ. Moreover, since $\ell \leqslant 22$, we deduce from Observation 6.1 that

$$3e_{r-1} < 2^{k_{3,r} - k_{3,\ell}} \left(2^{\ell} + 2^{k_{3,\ell}}\right) \leqslant 2^{k_{3,r} - k_{3,\ell}} 3^{\ell} ,$$

which implies that $e_{r-1} < 3^{\ell-1} 2^{k_{3,r} - k_{3,\ell}}$.

Then, we can investigate each case separately:

(a) ℓ is even, so $\left(3^{\ell-1}\right)^{-1} \equiv 3^{-1} \equiv 3 \bmod 8$. Since $S \equiv 0 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv 3e_{r-1} \equiv 3 \times 2 \equiv 6 \bmod 8\,,$

(b) ℓ is even, so $\left(3^{\ell-1}\right)^{-1} \equiv 3^{-1} \equiv 3 \bmod 8$. Since $S \equiv 1 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv 3e_{r-1} \equiv 3 \times 3 \equiv 1 \bmod 8\,,$

(c) ℓ is odd, so $\left(3^{\ell-1}\right)^{-1} \equiv 1^{-1} \equiv 1 \bmod 8$. Since $S \equiv 4 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv e_{r-1} \equiv 6 \bmod 8\,.$

So, we obtain that

$$e_{r-1}/3^{\ell-1} \preceq e_{r-\ell}\;,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,

$$(2^{k_{3,r}} - 2)/3 = 2 + \sum_{j=1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+1} \preceq e_{r-1}\;,$$

which proves that $2^{k_{3,r}} - 2 \in \mathcal{E}_{3,r}$.

(3) Let $\ell > 2$ be odd such that $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 5$. Figure 6.21 illustrates the procedure we describe below. On the first lines the squares 🟧 represent the active bits of e_r, on the third lines the squares 🟥 the active bits of e_{r-1}, on the fifth lines the squares 🟪 the active bits of e_{r-2}, where the squares ▨ are the $\varepsilon_i 2^i$ in the sum S, and on the seventh lines the squares 🟩 the active bits of $e_{r-\ell}$.

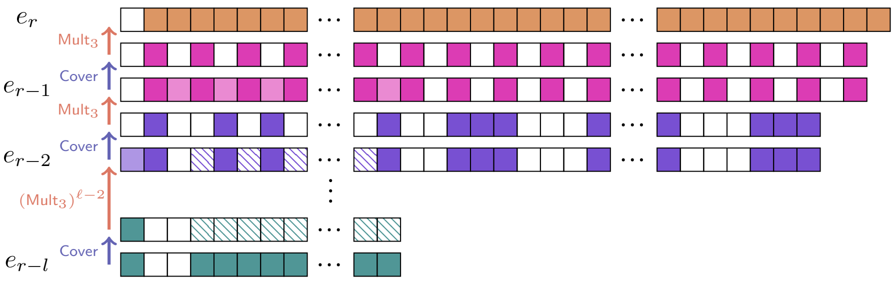


Figure 6.21: *How to derive $2^{k_{3,r}} - 2$ when $\ell > 2$ is odd and $b_{3,r-\ell} = \overline{b_{3,r}} = 0$.*

When ℓ is odd and $b_{3,r-\ell} = \overline{b_{3,r}} = 1$, by hypothesis, $e_{r-\ell} = 2^{k_{3,r}-k_{3,\ell}} - 7$ belongs to $\mathcal{E}_{3,r-\ell}$. Let us again simplify the notation using a new variable γ. Now, we let $\gamma = \left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 3\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 4$. We choose

$$e_{r-2} = 2 + \sum_{j=2}^{\gamma+1} 2^{2j} + S + \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)}\;,$$

with

$$S = 1 + \sum_{j=1}^{\gamma} \varepsilon_j 2^{2j+1} \,,$$

where the ε_j are chosen such that $e_{r-2} \equiv 0 \bmod 3^{\ell-2}$, which is always possible from Observation 6.2 since $\ell \leqslant 22$ and the number of coefficients ε_j in the sum is

$$\gamma \geqslant \frac{k_{3,r} - 1 - k_{3,\ell} + \ell}{2} - 4 \geqslant \frac{4\ell + 4}{2} - 4 \geqslant 2\ell - 3 \,.$$

Then, we have

$$\begin{aligned} e_{r-2} &< \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-6\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 5} \\ &\leqslant \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-k_{3,\ell}+\ell-5} \,. \end{aligned}$$

It follows that

$$\begin{aligned} 9e_{r-2} &< 9 \times \left(\sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-k_{3,\ell}+\ell-5} \right) \\ &\leqslant (2^6 - 1) \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} 2^{k_{3,r}-6j} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-5} \,, \end{aligned}$$

from which we deduce

$$\begin{aligned} 9e_{r-2} &\leqslant 2^{k_{3,r}} - 2^{k_{3,r}-6\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 6} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-5} \\ &< 2^{k_{3,r}} + 2^{k_{3,r}-k_{3,\ell}+\ell} \\ &\leqslant 2^{k_{3,r}-k_{3,\ell}} \left(2^{k_{3,\ell}} + 2^{\ell} \right) < 3^{\ell} 2^{k_{3,r}-k_{3,\ell}} \end{aligned}$$

where the last inequality comes from Corollary 6.1 since $\ell \leqslant 22$. We then deduce that $e_{r-2} < 3^{\ell-2} 2^{k_{3,r}-k_{3,\ell}}$.
Then $3^{\ell-2} \equiv 3 \bmod 8$ since ℓ is odd, and $S \equiv 1 \bmod 8$, leading to

$$e_{r-2}/3^{\ell-2} \equiv 3e_{r-2} \equiv 3 \times 3 \equiv 1 \bmod 8 \,.$$

So, we have

$$e_{r-2}/3^{\ell-2} \preceq e_{r-\ell} \,,$$

implying that e_{r-2} belongs to $\mathcal{E}_{3,r-2}$.

Let now

$$e_{r-1} = 6 + \sum_{j=2}^{\gamma+1} 2^{2j} + \sum_{j=1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+1} \,.$$

Then, we have

$$e_{r-1}/3 = 2 + \sum_{j=2}^{\gamma+1} 2^{2j} + \sum_{i=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} 2^{k_{3,r}-6i}(1+2+2^2) \preceq e_{r-2} \ ,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$.

Finally,

$$(2^{k_{3,r}}-2)/3 = 2 + \sum_{j=1}^{\left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 1} 2^{2j+1} \preceq e_{r-1} \ ,$$

implying that $2^{k_{3,r}} - 2 \in \mathcal{E}_{3,r}$.

□

Now we focus on the case where $k_{3,r}$ is even (or equivalently $b_{3,r} = 0$), and exhibit in Lemmas 6.2, 6.3 and 6.4 some maximum-weight exponents in this case.

First, we construct exponents of maximum weight for round r when $k_{3,r}$ and $k_{3,r-1}$ are even and $k_{3,r-2}$ is odd. We will use α to denote both 2 and 5, since some results are valid whatever the value of α is.

Lemma 6.2. *Let $(k_{3,r})_{r>0}$ be the sequence defined by $k_{3,r} = \lfloor r \log_2 3 \rfloor$, and $(b_{3,r})_{r>0}$ the sequence defined by $b_{3,r} = k_{3,r} \bmod 2$. Let $r \geqslant 6$, and $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (100)$. For all $\alpha \in \{2,5\}$, if*

$$\{2^{k_{3,r}-3} - \alpha\} \subseteq \mathcal{E}_{3,r-2} \ ,$$

and

$$\{2^{k_{3,r}-2} - 7\} \cup \{2^{k_{3,r}-1} - 2^{k_{3,r}-3} - 2^{2j_2} - \alpha, 2 \leqslant j_2 \leqslant k_{3,r}/2 - 1\} \subseteq \mathcal{E}_{3,r-1} \ ,$$

then

$$\{2^{k_{3,r}-1} - \alpha\} \cup \{2^{k_{3,r}} - 2^{2j_1+1} - \alpha, 0 \leqslant j_1 \leqslant k_{3,r}/2 - 2\} \subseteq \mathcal{E}_{3,r} \ .$$

We summarize in Figure 6.22 all the trails we will exhibited in the proof.

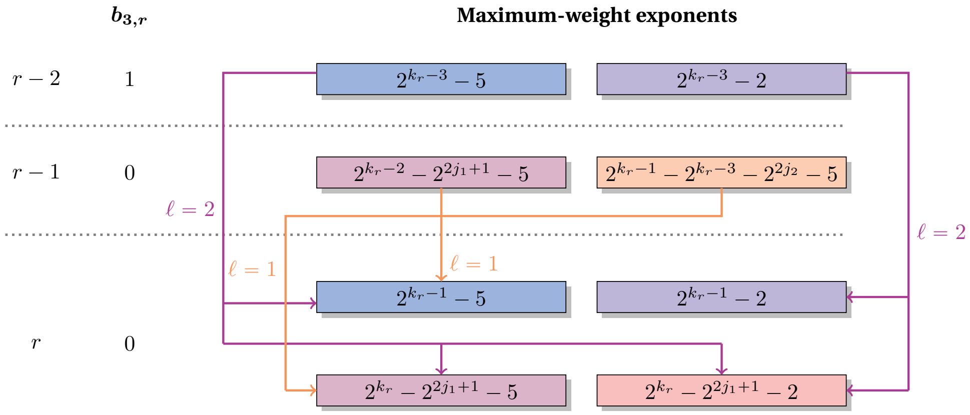


Figure 6.22: *Tracing exponents when* $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (100)$.

Proof of Lemma 6.2. We will successively prove that each of the exponents mentioned in the lemma belongs to $\mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}-1}-2$ i.e. $\alpha=2$.** By hypothesis, $e_{r-2}=2^{k_{3,r}-3}-2$ belongs to $\mathcal{E}_{3,r-2}$. Let us choose
$$e_{r-1}=2+\sum_{i=3}^{k_{3,r}-5}2^i+2^{k_{3,r}-3}\ .$$
Then, we have
$$e_{r-1}/3=\sum_{i=1}^{k_{3,r}-5}2^i\preceq e_{r-2}\ ,$$
implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,
$$(2^{k_{3,r}-1}-2)/3=\sum_{j=0}^{\frac{k_{3,r}}{2}-2}2^{2j+1}\preceq e_{r-1}\ ,$$
implying that $2^{k_{3,r}-1}-2\in\mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}-1}-5$ i.e. $\alpha=5$.** By hypothesis, $2^{k_{3,r}-2}-7$ belongs to $\mathcal{E}_{3,r-1}$. Then, we have
$$(2^{k_{3,r}-1}-5)/3=1+\sum_{i=1}^{\frac{k_{3,r}}{2}-2}2^{2i+1}\preceq 2^{k_{3,r}-2}-7,$$
implying that $2^{k_{3,r}-1}-5$ belongs to $\mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}}-4$ i.e. $j_1=0,\alpha=2$.** Let us choose
$$e_{r-1}=\sum_{i=2}^{k_{3,r}-6}2^i+2^{k_{3,r}-4}+2^{k_{3,r}-2}\ .$$
We notice that
$$\begin{aligned}3\times\left(\sum_{i=1}^{\frac{k_{3,r}}{2}-3}2^{2i}+2^{k_{3,r}-5}+2^{k_{3,r}-4}\right)&=\sum_{i=1}^{\frac{k_{3,r}}{2}-3}\left(2^{2i}+2^{2i+1}\right)+2^{k_{3,r}-5}+2^{k_{3,r}-2}\\&=\sum_{i=2}^{k_{3,r}-6}2^i+2^{k_{3,r}-4}+2^{k_{3,r}-2}\\&=e_{r-1}\ .\end{aligned}$$
It follows that
$$e_{r-1}/3=\sum_{i=1}^{\frac{k_{3,r}}{2}-3}2^{2i}+2^{k_{3,r}-5}+2^{k_{3,r}-4}\preceq e_{r-2}\ ,$$
implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,
$$(2^{k_{3,r}}-4)/3=\sum_{j=1}^{\frac{k_{3,r}}{2}-1}2^{2j}\preceq e_{r-1}\ ,$$
implying that $2^{k_{3,r}}-4\in\mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}} - 7$ i.e. $j_1 = 0, \alpha = 5$.** This case corresponds to Theorem 6.1.
- **For $2^{k_{3,r}} - 10$ i.e. $j_1 = 1, \alpha = 2$.** By hypothesis, $2^{k_{3,r}-1} - 2^{k_{3,r}-3} - 2^{2j_2} - \alpha$ belongs to $\mathcal{E}_{3,r-1}$. For $j_2 = 2$ and $\alpha = 2$, this exponent corresponds to

$$2^{k_{3,r}-1} - 2^{k_{3,r}-3} - 6 = 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 6\,.$$

Moreover, we have

$$(2^{k_{3,r}} - 10)/3 = 2 + \sum_{i=2}^{\frac{k_{3,r}}{2}-1} 2^{2i} \leq 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 6\,,$$

implying that $2^{k_{3,r}} - 10$ belongs to $\mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}} - 13$ i.e. $j_1 = 1, \alpha = 5$.** By hypothesis, $e_{r-2} = 2^{k_{3,r}-3} - 5$ belongs to $\mathcal{E}_{3,r-2}$. Let us choose

$$e_{r-1} = 1 + \sum_{i=2}^{\frac{k_{3,r}}{2}-1} 2^{2i} + \sum_{i=2}^{\frac{k_{3,r}}{2}-3} 2^{2i+1}\,.$$

Then, we have

$$e_{r-1}/3 = 3 + \sum_{i=3}^{k_{3,r}-4} 2^{i} \leq e_{r-2}\,,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,

$$(2^{k_{3,r}} - 13)/3 = 1 + \sum_{i=2}^{\frac{k_{3,r}}{2}-1} 2^{2i} \leq e_{r-1}\,,$$

implying that $2^{k_{3,r}} - 13 \in \mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}} - 2^{2j_1+1} - \alpha$ with $j_1 \geqslant 2$.** By hypothesis, for $j_2 \in [\![2, j_1]\!]$, we have

$$2^{k_{3,r}-1} - 2^{k_{3,r}-3} - 2^{2j_2} - \alpha = 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 2^{2j_2} - \alpha \in \mathcal{E}_{3,r-1}\,.$$

We have

$$(2^{k_{3,r}} - 2^{2j_1+1} - \alpha)/3 = (8-\alpha)/3 + \sum_{i=1}^{j_1-1} 2^{2i+1} + \sum_{i=j_1+1}^{\frac{k_{3,r}}{2}-1} 2^{2i}\,.$$

Let us notice that $(8-\alpha)/3 = 2$, if $\alpha = 2$, and $(8-\alpha)/3 = 1$, if $\alpha = 5$, so that if $\alpha = 2$, we have both

$$(2^{k_{3,r}} - 2^{2j_1+1} - 2)/3 \leq 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 2^{2j_2} - 2\,,$$

and

$$(2^{k_{3,r}} - 2^{2j_1+1} - 2)/3 \leq 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 2^{2j_2} - 5\,,$$

and if $\alpha = 5$, we have

$$(2^{k_{3,r}} - 2^{2j_1+1} - 5)/3 \leq 2^{k_{3,r}-2} + 2^{k_{3,r}-3} - 2^{2j_2} - 5\,.$$

It follows that $2^{k_{3,r}} - 2^{2j_1+1} - \alpha \in \mathcal{E}_{3,r}$.

□

Similarly, we now construct exponents for round r when $k_{3,r}$ is even and $k_{3,r-1}$ is odd. It is worth noting that when $(b_{3,r-1}b_{3,r}) = (10)$, there is a plateau between rounds $(r-1)$ and r, implying that all maximum-weight exponents in $\mathcal{E}_{3,r-1}$ are also maximum-weight exponents in $\mathcal{E}_{3,r}$. The following lemma then exhibits some additional maximum-weight exponents in this case.

Lemma 6.3. *Let $(k_{3,r})_{r>0}$ be the sequence defined by $k_{3,r} = \lfloor r \log_2 3 \rfloor$, and $(b_{3,r})_{r>0}$ the sequence defined by $b_{3,r} = k_{3,r} \bmod 2$. Let $r \geqslant 6$, and $(b_{3,r-1}b_{3,r}) = (10)$. If $\{2^{k_{3,r}-1} - \alpha\} \subseteq \mathcal{E}_{3,r-1}$ for $\alpha \in \{2,5\}$ then for all $\alpha \in \{2,5\}$*

$$\begin{aligned}\{2^{k_{3,r}-1} - \alpha\} \cup \{2^{k_{3,r}} - 2^{2j_1+1} - \alpha, 0 \leqslant j_1 \leqslant k_{3,r}/2 - 2\}& \\ \cup \{2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 2^{2j_2} - \alpha, 2 \leqslant j_2 \leqslant k_{3,r}/2 - 1\}& \\ \cup \{2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 6\}& \quad \subseteq \mathcal{E}_{3,r} \, .\end{aligned}$$

Moreover, if $(b_{3,r-5} \dots b_{3,r}) = (100110)$ we also have:

$$\begin{aligned}\{2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 2^{2j_3+1} - \alpha, 0 \leqslant j_3 \leqslant k_{3,r}/2 - 2\}& \\ \cup \{2^{k_{3,r}+1} - 2^{k_{3,r}-3} - 2^{2j_4} - \alpha, 2 \leqslant j_4 \leqslant k_{3,r}/2 - 2\}& \quad \subseteq \mathcal{E}_{3,r} \, .\end{aligned}$$

As for the previous lemmas, we also summarize the procedure in Figure 6.23. We illustrate the particular case where $(b_{3,r-5} \dots b_{3,r}) = (100110)$ (in the other cases, the four exponents at the bottom of the figure do not belong to $\mathcal{E}_{3,r}$).

Proof of Lemma 6.3. By hypothesis, $2^{k_{3,r}-1} - \alpha$ belongs to $\mathcal{E}_{3,r-1}$. Hence, we trivially have $2^{k_{3,r}-1} - \alpha \in \mathcal{E}_{3,r}$. Then, let us examine the other types of exponents mentioned in the lemma.

- **For $2^{k_{3,r}} - 2^{2j_1+1} - \alpha$ with $j_1 \geqslant 0$.** We have

$$(2^{k_{3,r}} - 2^{2j_1+1} - \alpha)/3 = (8-\alpha)/3 + \sum_{i=1}^{j_1-1} 2^{2i+1} + \sum_{i=j_1+1}^{\frac{k_{3,r}}{2}-1} 2^{2i} \preceq 2^{k_{3,r}-1} - \beta_\alpha \, ,$$

  implying that $2^{k_{3,r}} - 2^{2j_1+1} - \alpha \in \mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 2^{2j_2} - \alpha$ with $j_2 \geqslant 2$.** First, we observe that

$$\begin{aligned}3 \times \left(\sum_{i=1}^{j_2-1} 2^{2i+1} + 2^{2j_2} + \sum_{i=2j_2+1}^{k_{3,r}-2} 2^i \right) &= \sum_{i=3}^{2j_2} 2^i + 2^{2j_2} + 2 \times \sum_{i=2j_2+1}^{k_{3,r}-2} 2^i + 2^{k_{3,r}-1} \\ &= \sum_{i=3}^{2j_2-1} 2^i + \sum_{i=2j_2+1}^{k_{3,r}-2} 2^i + 2^{k_{3,r}} \, .\end{aligned}$$

  Then, we have

$$(2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 2^{2j_2} - \alpha)/3 = (8-\alpha)/3 + \sum_{i=1}^{j_2-1} 2^{2i+1} + 2^{2j_2} + \sum_{i=2j_2+1}^{k_{3,r}-2} 2^i \, ,$$

  implying that if $\alpha = 2$, we have both

$$(2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 2^{2j_2} - 2)/3 \preceq 2^{k_{3,r}-1} - 2 \, ,$$

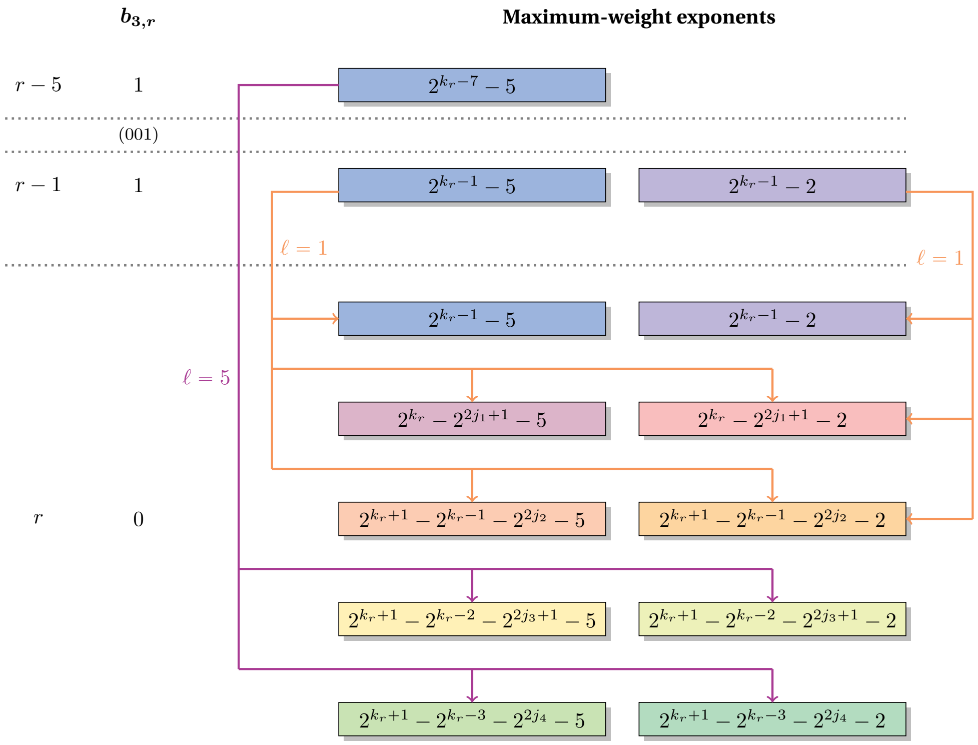

$b_{3,r}$
Maximum-weight exponents
$r-5$
1
$2^{k_r-7}-5$
(001)
$r-1$
1
$2^{k_r-1}-5$
$2^{k_r-1}-2$
$\ell=1$
$\ell=1$
$2^{k_r-1}-5$
$2^{k_r-1}-2$
$\ell=5$
$2^{k_r}-2^{2j_1+1}-5$
$2^{k_r}-2^{2j_1+1}-2$
r
0
$2^{k_r+1}-2^{k_r-1}-2^{2j_2}-5$
$2^{k_r+1}-2^{k_r-1}-2^{2j_2}-2$
$2^{k_r+1}-2^{k_r-2}-2^{2j_3+1}-5$
$2^{k_r+1}-2^{k_r-2}-2^{2j_3+1}-2$
$2^{k_r+1}-2^{k_r-3}-2^{2j_4}-5$
$2^{k_r+1}-2^{k_r-3}-2^{2j_4}-2$

Figure 6.23: *Tracing exponents when* $(b_{3,r-5}\dots b_{3,r})=(100110)$.

and

$$(2^{k_{3,r}+1}-2^{k_{3,r}-1}-2^{2j_2}-2)/3 \preceq 2^{k_{3,r}-1}-5\ ,$$

and if $\alpha=5$, we have

$$(2^{k_{3,r}+1}-2^{k_{3,r}-1}-2^{2j_2}-5)/3 \preceq 2^{k_{3,r}-1}-5\ .$$

As a consequence, we have $2^{k_{3,r}+1}-2^{k_{3,r}-1}-2^{2j_2}-\alpha\in\mathcal{E}_{3,r}$.

- **For $2^{k_{3,r}+1}-2^{k_{3,r}-1}-6$.** We also have,

$$(2^{k_{3,r}+1}-2^{k_{3,r}-1}-6)/3 = 2^{k_{3,r}-1}-2\ ,$$

implying that $2^{k_{3,r}+1}-2^{k_{3,r}-1}-6\in\mathcal{E}_{3,r}$.

Now, let us assume that $(b_{3,r-5}\dots b_{3,r})=(100110)$. By induction hypothesis, we have $e_{r-5}=2^{k_{3,r}-7}-5$ belongs to $\mathcal{E}_{3,r-5}$. Indeed, let

$$e_{r-2}=1+\sum_{i=2}^{\frac{k_{3,r}}{2}-2}2^{2i}+2^{k_{3,r}-3}+S\ ,$$

where

$$S=\sum_{j=1}^{\frac{k_{3,r}}{2}-5}\varepsilon_j 2^{2j+1}\quad\text{with } \varepsilon_j\in\{0,1\},\ \text{and such that } S\equiv 0 \bmod 8\ .$$

We choose the ε_j such that $e_{r-2} \equiv 0 \bmod 3^3$ which is always possible from Observation 6.2. Then, we have

$$e_{r-2} < 2^{k_{3,r}-3} + 2^{k_{3,r}-4} + 2^{k_{3,r}-6} + 2^{k_{3,r}-7} = 3^3 2^{k_{3,r}-7} .$$

And, using $3^3 \equiv 3 \bmod 8$ and $S \equiv 0 \bmod 8$, we get:

$$e_{r-2}/3^3 \equiv 3e_{r-2} \equiv 3 \bmod 8 .$$

So, we deduce that

$$e_{r-2}/3^3 \preceq e_{r-5} ,$$

implying that e_{r-2} belongs to $\mathcal{E}_{3,r-2}$. Let

$$e_{r-1} = 2^{k_{3,r}} - 2^{k_{3,r}-2} - 2^{k_{3,r}-3} - 13 = 2^{k_{3,r}-1} + 2^{k_{3,r}-3} - 13 .$$

We observe that

$$\begin{aligned} 3 \times \left(1 + \sum_{i=2}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-3}\right) &= 3 + \sum_{i=4}^{k_{3,r}-3} 2^i + 2^{k_{3,r}-3} + 2^{k_{3,r}-2} \\ &= 3 + \sum_{i=4}^{k_{3,r}-4} 2^i + 2^{k_{3,r}-1} , \end{aligned}$$

leading to

$$e_{r-1}/3 = 1 + \sum_{i=2}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-3} \preceq e_{r-2} .$$

It follows that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Then let us distinguish two cases.

- **For $\boldsymbol{2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 2^{2j_3+1} - \alpha}$ with $\boldsymbol{j_3 \geqslant 1}$.** Let

  $$e_r = 2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 2^{2j_3+1} - \alpha, \quad \text{with } 1 \leqslant j_3 \leqslant \frac{k_{3,r}}{2} - 2 .$$

  We observe that

  $$\begin{aligned} 3 \times \left(\sum_{i=1}^{j_3-1} 2^{2i+1} + \sum_{i=j_3+1}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-1}\right) &= \sum_{i=3}^{2j_3} 2^i + \sum_{i=2j_3+2}^{k_{3,r}-3} 2^{2i} + 2^{k_{3,r}-1} + 2^{k_{3,r}} \\ &= 2^{k_{3,r}} + 2^{k_{3,r}-1} + 2^{k_{3,r}-2} - 2^{2j_3+1} - 8 , \end{aligned}$$

  leading to

  $$e_r/3 = (8-\alpha)/3 + \sum_{i=1}^{j_3-1} 2^{2i+1} + \sum_{i=j_3+1}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-1} \preceq e_{r-1} .$$

  It follows that e_r belongs to $\mathcal{E}_{3,r}$.

- **For $\mathbf{2^{k_{3,r}+1} - 2^{k_{3,r}-3} - 2^{2j_4} - \alpha}$ with $\mathbf{j_4 \geqslant 2}$.** Let

$$e_r = 2^{k_{3,r}+1} - 2^{k_{3,r}-3} - 2^{2j_4} - \alpha, \quad \text{with } 2 \leqslant j_4 \leqslant \frac{k_{3,r}}{2} - 2\,.$$

We observe that

$$\begin{aligned} 3 \times \left(\sum_{i=1}^{j_4-2} 2^{2i+1} + \sum_{i=2j_4-1}^{k_{3,r}-4} 2^i \right) &= \sum_{i=3}^{2j_4-2} 2^i + 2^{2j_4-1} + 2 \times \sum_{i=2j_4}^{k_{3,r}-4} 2^i + 2^{k_{3,r}-3} \\ &= \sum_{i=3}^{2j_4-1} 2^i + \sum_{i=2j_4+1}^{k_{3,r}-4} 2^i + 2^{k_{3,r}-2}\,, \end{aligned}$$

leading to

$$e_r/3 = (8-\alpha)/3 + \sum_{i=1}^{j_4-2} 2^{2i+1} + \sum_{i=2j_4-1}^{k_{3,r}-4} 2^i + 2^{k_{3,r}-1} \preceq e_{r-1}\,.$$

It follows that e_r belongs to $\mathcal{E}_{3,r}$.

Finally, let us prove the two remaining cases, i.e. when $j_3 = 0$.

- **For $\mathbf{2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 4}$ i.e. $\mathbf{j_3 = 0, \alpha = 2}$.** Let

$$e_{r-2} = 2 + \sum_{i=2}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-3} + S\,,$$

where

$$S = 1 + \sum_{j=1}^{\frac{k_{3,r}}{2}-5} \varepsilon_j 2^{2j+1} \quad \text{with } \varepsilon_j \in \{0,1\}, \text{ and such that } S \equiv 1 \bmod 8\,.$$

We choose the ε_j such that $e_{r-2} \equiv 0 \bmod 3^3$, which is always possible from Observation 6.2. Then, we have

$$e_{r-2} < 2^{k_{3,r}-3} + 2^{k_{3,r}-4} + 2^{k_{3,r}-6} + 2^{k_{3,r}-7} = 3^3 2^{k_{3,r}-7}\,.$$

And, knowing that $3^3 \equiv 3 \bmod 8$ and $S \equiv 1 \bmod 8$, we get:

$$e_{r-2}/3^3 \equiv 3e_{r-2} \equiv 3 \times 3 \equiv 1 \bmod 8\,.$$

So, we deduce that

$$e_{r-2}/3^3 \preceq e_{r-5}\,,$$

implying that e_{r-2} belongs to $\mathcal{E}_{3,r-2}$. Let us now consider e_{r-1} defined by

$$e_{r-1} = 2^{k_{3,r}} - 2^{k_{3,r}-2} - 2^{k_{3,r}-3} - 10 = 2^{k_{3,r}-1} + 2^{k_{3,r}-3} - 10\,.$$

Then, we have

$$e_{r-1}/3 = 2 + \sum_{i=2}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-3} \preceq e_{r-2}\,,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. In the end,

$$(2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 4)/3 = 4 + \sum_{i=2}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-1} \preceq e_{r-1} \ ,$$

implying that $e_r = 2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 4 \in \mathcal{E}_{3,r}$.

- **For $\mathbf{2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 7}$ i.e. $\boldsymbol{j_3 = 0, \alpha = 5}$.** We have

$$e_r/3 = 3 + \sum_{i=2}^{\frac{k_{3,r}}{2}-2} 2^{2i} + 2^{k_{3,r}-1} \preceq e_{r-1} \ ,$$

implying that in the three cases $e_r \in \mathcal{E}_{3,r}$.

□

Finally, let us consider round r where $k_{3,r}$, $k_{3,r-1}$ and $k_{3,r-2}$ are even, or equivalently $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (000)$.

Lemma 6.4. *Let $(k_{3,r})_{r>0}$ be the sequence defined by $k_{3,r} = \lfloor r \log_2 3 \rfloor$, and $(b_{3,r})_{r>0}$ the sequence defined by $b_{3,r} = k_{3,r} \bmod 2$. Let $r \geqslant 6$, and $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (000)$.*

- *If $\{2^{k_{3,r}-5} - \alpha\} \subseteq \mathcal{E}_{3,r-3}$, for all $\alpha \in \{2,5\}$, and $\{2^{k_{3,r}-2} - 7\} \subseteq \mathcal{E}_{3,r-1}$ then*

$$\{2^{k_{3,r}-1} - \alpha\} \subseteq \mathcal{E}_{3,r} \ \textit{for all}\ \alpha \in \{2,5\} \ .$$

- *Let $r \geqslant 6$, and $\ell \in \mathcal{L}_r$ such that one of the following situations occurs:*

  (1) *$2 < \ell \leqslant 22$ such that $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 1$, and one of the following situations occurs:*

  - *ℓ is even, or*
  - *ℓ is odd, with $b_{3,r-\ell} = b_{3,r} = 0$;*

  (2) *$2 < \ell \leqslant 22$ is odd such that $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 6$ and $b_{3,r-\ell} = \overline{b_{3,r}} = 1$.*

  Hence, if $2^{k_{3,r}-k_{3,\ell}} - 4 \in \mathcal{E}_{3,r-\ell}$ when $b_{3,r-\ell} = b_{3,r} = 0$ or if $2^{k_{3,r}-k_{3,\ell}} - 5 \in \mathcal{E}_{3,r-\ell}$ when $b_{3,r-\ell} = \overline{b_{3,r}} = 1$ then $2^{k_{3,r}} - 4 \in \mathcal{E}_{3,r}$.

Before giving the proof, we propose Figure 6.24 to illustrate the different trails. The first item of the above lemma corresponds to arrows with $\ell = 1$ or with $\ell = 3$, meaning that the trail starts at round $(r-1)$ or $(r-3)$ respectively. Then, to explain the idea behind the second item of the lemma, we propose to give an example for the case ℓ odd, with $b_{3,r-\ell} = 0$. On Figure 6.24, we observe that both $2^{k_{3,r}} - 7$ and $2^{k_{3,r}} - 4$ can be derived from $2^{k_{3,r}-11} - 5$ appearing at round $(r-7)$ i.e. $\ell = 7$. The trail for $2^{k_{3,r}} - 7$ was found in Proposition 6.4 and the trail for $2^{k_{3,r}} - 4$ will be given in the following proof.

Proof of Lemma 6.4. We prove the first item of the lemma.

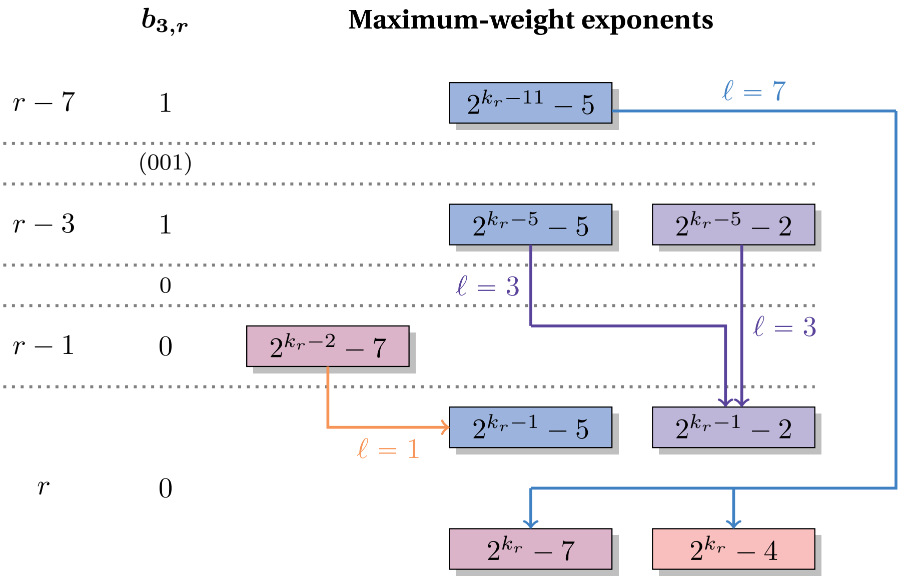


Figure 6.24: *Tracing exponents when* $(b_{3,r-2}b_{3,r-1}b_{3,r})=(000)$.

- By hypothesis, $2^{k_{3,r}-2}-7$ belongs to $\mathcal{E}_{3,r-1}$. Then, we have

$$(2^{k_{3,r}-1}-5)/3=1+\sum_{i=1}^{\frac{k_{3,r}}{2}-2}2^{2i+1}\preceq 2^{k_{3,r}-2}-7,$$

implying that $2^{k_{3,r}-1}-5$ belongs to $\mathcal{E}_{3,r}$.

Then, by hypothesis, $e_{r-3}=2^{k_{3,r}-5}-\alpha$ belongs to $\mathcal{E}_{3,r-3}$. Let

$$e_{r-2}=14+\sum_{i=5}^{k_{3,r}-9}2^i+2^{k_{3,r}-7}+2^{k_{3,r}-6}+2^{k_{3,r}-5}\ .$$

Then, we have

$$e_{r-2}/3=2+\sum_{i=3}^{k_{3,r}-9}2^i+2^{k_{3,r}-6}\preceq e_{r-3}\ ,$$

implying that e_{r-2} belongs to $\mathcal{E}_{3,r-2}$. Moreover, let

$$e_{r-1}=10+\sum_{i=5}^{k_{3,r}-9}2^i+2^{k_{3,r}-7}+2^{k_{3,r}-5}+2^{k_{3,r}-3}\ .$$

Then, we have

$$e_{r-1}/3=14+\sum_{i=3}^{\frac{k_{3,r}}{2}-5}2^{2i}+2^{k_{3,r}-7}+2^{k_{3,r}-6}+2^{k_{3,r}-5}\preceq e_{r-2}\ ,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Finally,

$$(2^{k_{3,r}-1}-2)/3 = \sum_{i=0}^{\frac{k_{3,r}}{2}-2} 2^{2i+1} \preceq e_{r-1} \ ,$$

implying that $2^{k_{3,r}-1}-2 \in \mathcal{E}_{3,r}$.

- **(1)** Let ℓ be an integer such that $2 < \ell \leqslant 22$, such that $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 1$. While the proposition considers two cases, we split the first one into two, so that we consider three cases:

  (a) ℓ is even, with $b_{3,r-\ell} = b_{3,r} = 0$,

  (b) ℓ is even, with $b_{3,r-\ell} = \overline{b_{3,r}} = 1$,

  (c) ℓ is odd, with $b_{3,r-\ell} = b_{3,r} = 0$.

  Figures 6.26, 6.26 and 6.27 illustrate the procedure below. On the first lines the squares 🟧 represent the active bits of e_r, on the third lines the squares ■ the active bits of e_{r-1}, where the squares ▨ are the $\varepsilon_i 2^i$ in the sum S, and on the fifth lines the squares 🟪 the active bits of $e_{r-\ell}$.

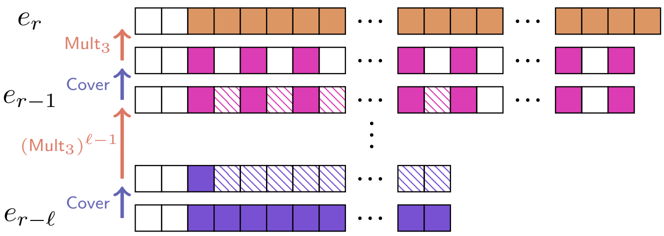


Figure 6.25: *How to derive $2^{k_{3,r}}-4$ when $\ell > 2$ is even and $b_{3,r-\ell} = b_{3,r} = 0$.*

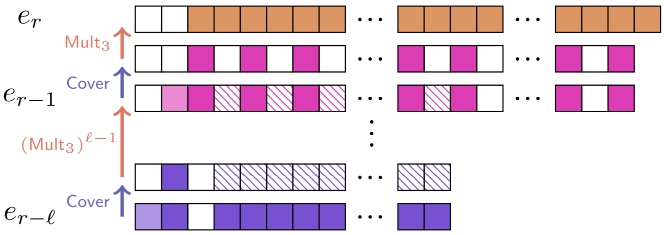


Figure 6.26: *How to derive $2^{k_{3,r}}-4$ when $\ell > 2$ is even and $b_{3,r-\ell} = \overline{b_{3,r}} = 1$.*

By hypothesis, $e_{r-\ell} = 2^{k_{3,r}-k_{3,\ell}} - 4$ belongs to $\mathcal{E}_{3,r-\ell}$ in Cases **(a)**,**(c)**, and $e_{r-\ell} = 2^{k_{3,r}-k_{3,\ell}} - 5$ belongs to $\mathcal{E}_{3,r-\ell}$ in Case **(b)**.

We now choose

$$e_{r-1} = 4 + \sum_{j=2}^{\frac{k_{3,r}}{2}-1} 2^{2j} + S \ ,$$

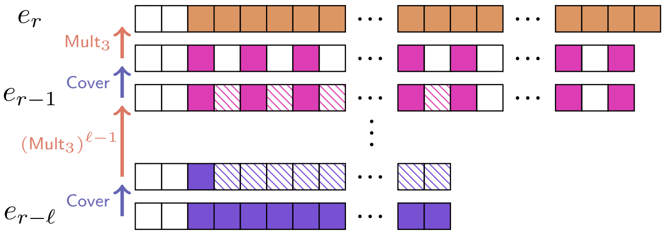


Figure 6.27: *How to derive* $2^{k_{3,r}} - 4$ *when* $\ell > 2$ *is odd and* $b_{3,r-\ell} = b_{3,r} = 0$.

with

$$S = \begin{cases} \sum_{j=1}^{2\ell-1} \varepsilon_j 2^{2j+1} & \text{in Cases (a), (c)} \\ 2 + \sum_{j=1}^{2\ell-1} \varepsilon_j 2^{2j+1} & \text{in Case (b)} \end{cases}$$

where the $(2\ell - 1)$ coefficients $\varepsilon_j \in \{0, 1\}$ are chosen such that e_{r-1} is divisible by $3^{\ell-1}$. Indeed, it is known from Observation 6.2 that such a choice is always possible since $\ell \leqslant 22$.

We then use that

$$\begin{aligned} e_{r-1} &= \left(4 + S + \sum_{j=2}^{2\ell} 2^{2j}\right) + \sum_{j=2\ell+1}^{\frac{k_{3,r}}{2}-1} 2^{2j} \\ &< 2^{4\ell+1} + \sum_{j=1}^{\frac{k_{3,r}}{2}-2\ell-1} 2^{k_{3,r}-2j} . \end{aligned}$$

It follows that

$$\begin{aligned} 3e_{r-1} &< 3 \times \left(2^{4\ell+1} + \sum_{j=1}^{\frac{k_{3,r}}{2}-2\ell-1} 2^{k_{3,r}-2j}\right) \\ &\leqslant 2^{4\ell+1} + 2^{k_{3,r}} \\ &\leqslant 2^{k_{3,r}-k_{3,\ell}+\ell} + 2^{k_{3,r}} , \end{aligned}$$

where the last inequality comes from the hypothesis on ℓ. Moreover, since $\ell \leqslant 22$, we deduce from Corollary 6.1 that

$$3e_{r-1} < 2^{k_{3,r}-k_{3,\ell}} \left(2^\ell + 2^{k_{3,\ell}}\right) \leqslant 2^{k_{3,r}-k_{3,\ell}} 3^\ell ,$$

which implies that $e_{r-1} < 3^{\ell-1} 2^{k_{3,r}-k_{3,\ell}}$.

Then, we investigate each case separately:

(a) ℓ is even, so $\left(3^{\ell-1}\right)^{-1} \equiv 3^{-1} \equiv 3 \bmod 8$. Since $S \equiv 0 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv 3e_{r-1} \equiv 3 \times 4 \equiv 4 \bmod 8$,

(b) ℓ is even, so $\left(3^{\ell-1}\right)^{-1} \equiv 3^{-1} \equiv 3 \bmod 8$. Since $S \equiv 2 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv 3e_{r-1} \equiv 3 \times 6 \equiv 2 \bmod 8$,

(c) ℓ is odd, so $\left(3^{\ell-1}\right)^{-1} \equiv 1^{-1} \equiv 1 \bmod 8$. Since $S \equiv 0 \bmod 8,$ we have $e_{r-1}/3^{\ell-1} \equiv e_{r-1} \equiv 4 \bmod 8$.

So, we obtain that

$$e_{r-1}/3^{\ell-1} \preceq e_{r-\ell} ,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$. Moreover,

$$(2^{k_{3,r}} - 4)/3 = 4 + \sum_{j=2}^{\frac{k_{3,r}}{2}-1} 2^{2j} \preceq e_{r-1} ,$$

which proves that $2^{k_{3,r}} - 4 \in \mathcal{E}_{3,r}$.

(2) Let $\ell > 2$, such that $k_{3,r} \geqslant k_{3,\ell} + 3\ell + 6$. Figure 6.28 illustrates the procedure we will describe. On the first lines the squares 🟧 represent the active bits of e_r, on the third lines the squares 🟥 the active bits of e_{r-1}, on the fifth lines the squares 🟪 the active bits of e_{r-2}, where the squares ▨ are the $\varepsilon_i 2^i$ in the sum S, and on the seventh lines the squares 🟩 the active bits of $e_{r-\ell}$.

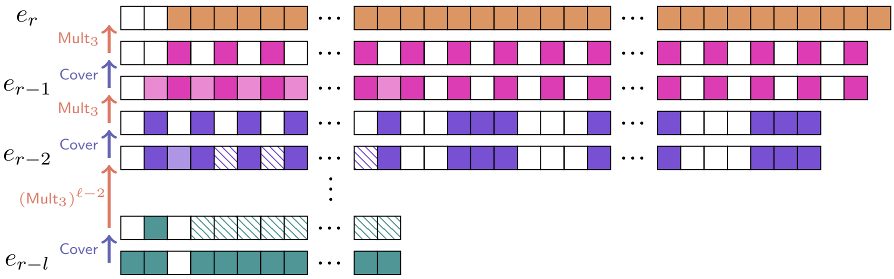


Figure 6.28: How to derive $2^{k_{3,r}} - 4$ when $\ell > 2$ is odd and $b_{3,r-\ell} = \overline{b_{3,r}} = 1$.

When ℓ is odd and $b_{3,r-\ell} = \overline{b_{3,r}} = 1$, by hypothesis, $e_{r-\ell} = 2^{k_{3,r}-k_{3,\ell}} - 5$ belongs to $\mathcal{E}_{3,r-\ell}$. Let us simplify the notation using γ, defined by $\gamma = \left\lfloor \frac{k_{3,r}}{2} \right\rfloor - 3\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 5.$ We now choose

$$e_{r-2} = 2 + \sum_{j=1}^{\gamma} 2^{2j+1} + S + \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor+1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} ,$$

with

$$S = 4 + \sum_{j=2}^{\gamma} \varepsilon_j 2^{2j}$$

where the ε_j are chosen such that $e_{r-2} \equiv 0 \bmod 3^{\ell-2}$, which is always possible from Observation 6.2 since $\ell \leqslant 22$ and the number of coefficients ε_j in the sum is

$$\gamma - 1 \geqslant \frac{k_{3,r} - k_{3,\ell} + \ell}{2} - 6 \geqslant \frac{4\ell + 6}{2} - 6 \geqslant 2\ell - 3\,.$$

Then, we have

$$\begin{aligned} e_{r-2} &< \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r} - 6\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 8} \\ &\leqslant \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-k_{3,\ell}+\ell-8}\,. \end{aligned}$$

It follows that

$$\begin{aligned} 9e_{r-2} &< 9 \times \left(\sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} \sum_{i=0}^{2} 2^{k_{3,r}-(6j-i)} + 2^{k_{3,r}-k_{3,\ell}+\ell-8} \right) \\ &\leqslant (2^6 - 1) \sum_{j=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} 2^{k_{3,r}-6j} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-8} \\ &\leqslant 2^{k_{3,r}} - 2^{k_{3,r} - 6\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor - 5} + 9 \times 2^{k_{3,r}-k_{3,\ell}+\ell-8} \\ &< 2^{k_{3,r}} + 2^{k_{3,r}-k_{3,\ell}+\ell} \\ &\leqslant 2^{k_{3,r}-k_{3,\ell}} \left(2^{k_{3,\ell}} + 2^{\ell} \right) \\ &< 3^{\ell} 2^{k_{3,r}-k_{3,\ell}}\,, \end{aligned}$$

where the last inequality comes from Corollary 6.1 since $\ell \leqslant 22$. We then deduce that $e_{r-2} < 3^{\ell-2} 2^{k_{3,r}-k_{3,\ell}}$.
Then $3^{\ell-2} \equiv 3 \bmod 8$ since ℓ is odd, and $S \equiv 4 \bmod 8$, leading to

$$e_{r-2}/3^{\ell-2} \equiv 3e_{r-2} \equiv 3 \times 6 \equiv 2 \bmod 8\,.$$

So, we have

$$e_{r-2}/3^{\ell-2} \preceq e_{r-\ell}\,,$$

implying that e_{r-2} belongs to $\mathcal{E}_{3,r-2}$.
Let now

$$e_{r-1} = 6 + \sum_{j=2}^{\frac{k_{3,r}}{2}-1} 2^{2j} + \sum_{j=1}^{\gamma} 2^{2j+1}\,.$$

Then, we have

$$e_{r-1}/3 = 2 + \sum_{j=1}^{\gamma} 2^{2j+1} + \sum_{i=1}^{\left\lfloor \frac{k_{3,\ell}-\ell}{6} \right\rfloor + 1} 2^{k_{3,r}-6i}(1 + 2 + 2^2) \preceq e_{r-2}\,,$$

implying that e_{r-1} belongs to $\mathcal{E}_{3,r-1}$.

Finally,

$$(2^{k_{3,r}} - 4)/3 = 4 + \sum_{j=2}^{\frac{k_{3,r}}{2}-1} 2^{2j} \leq e_{r-1} \ ,$$

which proves that $2^{k_{3,r}} - 4 \in \mathcal{E}_{3,r}$.

□

Remark 6.4. To simplify this proof we have given a way of deriving the exponents reaching the upper bound on the algebraic degree, but we have not aimed to minimize the length of the involved trail. Trying to find the smallest trail is then an interesting open problem. For example, we have already seen, in Proposition 6.4, that $2^{k_{3,r}} - 7 \in \mathcal{E}_{3,r}$ can be derived from

$$\begin{cases} 2^{k_{3,r}-11} - 5 \in \mathcal{E}_{3,r-7} & \text{when } (b_{3,r-7} \dots b_{3,r}) = (10011000)\ , \\ 2^{k_{3,r}-19} - 5 \in \mathcal{E}_{3,r-12} & \text{when } (b_{3,r-12} \dots b_{3,r}) = (1001100011000)\ . \end{cases}$$

But, it is not necessary to refer back as many rounds since we can construct these exponents as follows. If $(b_{3,r-7} \dots b_{3,r}) = (10011000)$ then

$$2^{k_{3,r}-3} - 2^{k_{3,r}-7} - 2^{k_{3,r}-8} - 5 \in \mathcal{E}_{3,r-2}\ ,$$

which implies $2^{k_{3,r}} - 7 \in \mathcal{E}_{3,r}$. Similarly if $(b_{3,r-12} \dots b_{3,r}) = (1001100011000)$ then

$$2^{k_{3,r}-11} - 2^{k_{3,r}-15} - 2^4 - 5 \in \mathcal{E}_{3,r-7}\ ,$$

which implies $2^{k_{3,r}} - 7 \in \mathcal{E}_{3,r}$. We note that such exponents, appearing respectively at rounds $r-2$ and $r-7$, can also be constructed from maximum-weight exponents. Indeed, we have

$$2^{k_{3,r}-3} - 2^{k_{3,r}-7} - 2^{k_{3,r}-8} - 5 \in \mathcal{E}_{3,r-2}$$

when

$$2^{k_{3,r}-9} - 2^{k_{3,r}-11} - 2^{k_{3,r}-12} - 5 \in \mathcal{E}_{3,r-6}\ ,$$

since $(b_{3,r-7} \dots b_{3,r-2}) = (10011)$ (see Lemma 6.3). Similarly, we have

$$2^{k_{3,r}-11} - 2^{k_{3,r}-15} - 2^4 - 5 \in \mathcal{E}_{3,r-7}$$

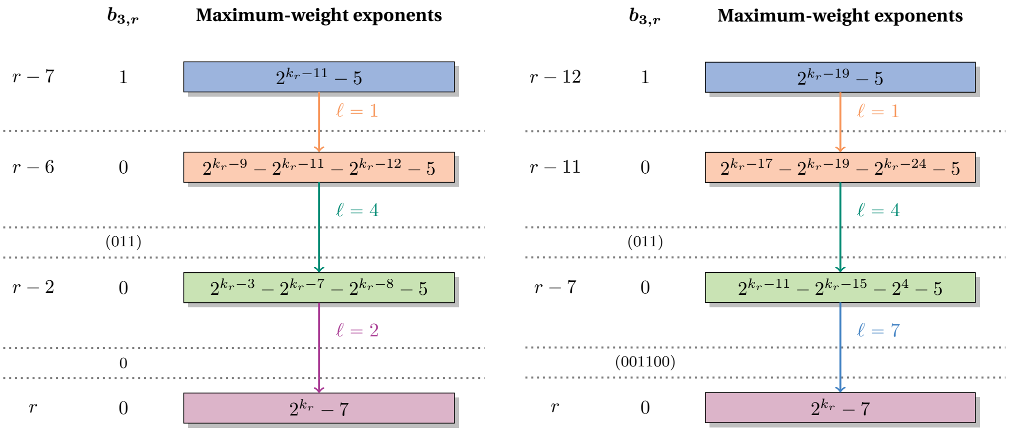
when

$$2^{k_{3,r}-17} - 2^{k_{3,r}-19} - 2^{k_{3,r}-24} - 5 \in \mathcal{E}_{3,r-11}\ ,$$

since $(b_{3,r-12} \dots b_{3,r-7}) = (10011)$ (see Lemma 6.3). Therefore, we have the pattern of Figure 6.29.

6.2.2 MILP-based algorithm

The induction procedure from Lemma 6.1 and Lemma 6.4 relies on some assumptions which are not satisfied for some values of r. These sporadic cases exactly correspond to those already observed previously, which we will also handle with a MILP-based algorithm. Table 6.7 provides the values of all $r \leqslant 411$ corresponding to the length of a palindromic sequence for which it has been checked with our MILP-based algorithm that $e_r \in \mathcal{E}_{3,r}$.



(a) *When* $(b_{3,r-7}\dots b_{3,r}) = (10011000)$. **(b)** *When* $(b_{3,r-12}\dots b_{3,r}) = (1001100011000)$.

Figure 6.29: *Tracing exponents when* $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (000)$ *with intermediate rounds.*

r	7	12	53	359
e_r	$2^{11}-2$	$2^{19}-2$	$2^{84}-4$	$2^{569}-2$
ℓ	4	3	4	6

Table 6.7: *Lengths* r *of palindromic sequences for which it has been proved with a MILP algorithm that* $e_r \in \mathcal{E}_{3,r}$*, using that* $3^{r-\ell} \in \mathcal{E}_{3,r-\ell}$.

r	19	24	106	159	212	265
e_r	$2^{30}-4$	$2^{38}-4$	$2^{168}-4$	$2^{252}-4$	$2^{336}-4$	$2^{420}-4$
ℓ	4	5	6	5	6	5

Table 6.8: ℓ *such that* $3^{r-\ell} \in \mathcal{E}_{3,r-\ell}$ *implies* $e_r \in \mathcal{E}_{3,r}$.

Similarly, Table 6.8 covers the first values of $r \leqslant 411$ for which there is no ℓ satisfying one of the situations of the above lemmas.

As this technique is rather slow, it cannot be applied to large values of r. In particular, the first value of r for which the cost becomes too high to obtain a result from the solver is $r = 412$. We summarize in Figure 6.30 all the rounds for which we are able to give more maximum-weight exponents than the exponents from Theorem 6.1.

6.2.3 Combining both steps

As a consequence, we are now able to construct by induction a subset of maximum-weight exponents for all rounds until 411. First we need the following observation.

Observation 6.4. For any $6 \leqslant r \leqslant 411$, one of the assumptions of Lemmas 6.1, 6.2, 6.3 and 6.4 is satisfied.

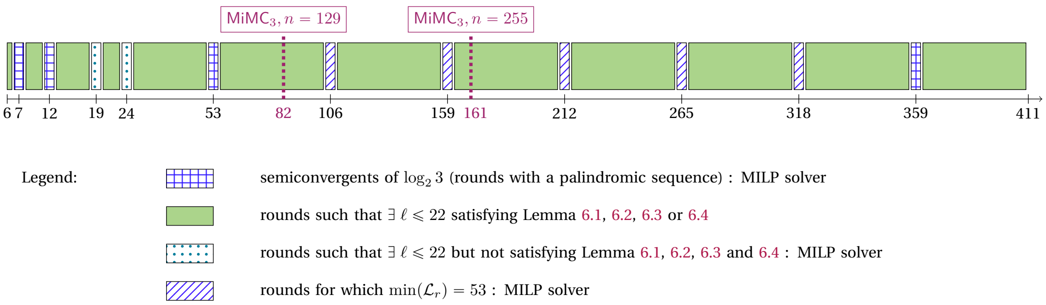


Figure 6.30: *Rounds for which we can construct more maximum-weight exponents.*

Knowing that all lemmas are satisfied, we can now construct exponents combining our inductive proof and the MILP-based algorithm.

Proposition 6.5. *Let* $6 \leqslant r \leqslant 411$, $k_{3,r} = \lfloor r \log_2 3 \rfloor$, $b_{3,r} = k_{3,r} \bmod 2$. *Then, the maximum-weight exponents in* $\mathcal{E}_{3,r}$ *include the set* $\mathcal{M}_{3,r}$ *defined as follows, where* α *can take any value in* $\{2, 5\}$*:*

- *if* $k_{3,r}$ *is odd:*

$$\mathcal{M}_{3,r} := \{2^{k_{3,r}} - \alpha\} ,$$

- *if* $k_{3,r}$ *is even:*
  - *if* $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (000)$*:*

$$\mathcal{M}_{3,r} := \{2^{k_{3,r}-1} - \alpha, 2^{k_{3,r}} - \alpha - 2\} ,$$

  - *if* $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (100)$*:*

$$\mathcal{M}_{3,r} := \left\{2^{k_{3,r}-1} - \alpha\right\} \cup \left\{2^{k_{3,r}} - 2^{2j_1+1} - \alpha, 0 \leqslant j_1 \leqslant \frac{k_{3,r}}{2} - 2\right\} ,$$

  - *if* $(b_{3,r-1}b_{3,r}) = (10)$*:*

$$\begin{aligned}\mathcal{M}_{3,r} := \{2^{k_{3,r}-1} - \alpha\} &\cup \left\{2^{k_{3,r}} - 2^{2j_1+1} - \alpha, 0 \leqslant j_1 \leqslant \frac{k_{3,r}}{2} - 2\right\} \\ &\cup \left\{2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 2^{2j_2} - \alpha, 2 \leqslant j_2 \leqslant \frac{k_{3,r}}{2} - 1\right\} \\ &\cup \{2^{k_{3,r}+1} - 2^{k_{3,r}-1} - 6\} .\end{aligned}$$

Moreover, when $(b_{3,r-1}b_{3,r}) = (10)$*, and* $k_{3,r-5}$ *is odd, with* $k_{3,r-5} = k_{3,r} - 7$*,* $\mathcal{E}_{3,r}$ *also includes:*

$$\begin{aligned}&\left\{2^{k_{3,r}+1} - 2^{k_{3,r}-2} - 2^{2j_3+1} - \alpha, 0 \leqslant j_3 \leqslant \frac{k_{3,r}}{2} - 2\right\} \\ \cup &\left\{2^{k_{3,r}+1} - 2^{k_{3,r}-3} - 2^{2j_4} - \alpha, 2 \leqslant j_4 \leqslant \frac{k_{3,r}}{2} - 2\right\} ,\end{aligned}$$

Proof. First, let us recall that for all $r \leqslant 411$, $\omega_{3,r} = 2^{k_{3,r}} - \alpha_{b_{3,r}} \in \mathcal{E}_{3,r}$ because of Theorem 6.1.

Then, we prove the presence of other exponents by induction on r. Let $(\mathcal{H}_r)$ be the following hypothesis:

$$(\mathcal{H}_r) : \forall\, 6 \leqslant i < r,\ \mathcal{M}_{3,i} \subseteq \mathcal{E}_{3,i}\ .$$

- **For $r = 7$:**

  $$(\mathcal{H}_7) : \forall\, 6 \leqslant i < 7,\ \mathcal{M}_{3,i} \subseteq \mathcal{E}_{3,i}$$

  is satisfied since $b_6 = 1$ and:

  $$\mathcal{M}_{3,6} = \{2^{k_6} - 5, 2^{k_6} - 2\} = \{507, 510\} \subseteq \mathcal{E}_{3,6}\ .$$

- **Induction step.** We assume that $(\mathcal{H}_r)$ is satisfied, then we will show that $(\mathcal{H}_{r+1})$ is also satisfied. If $(s_1, \dots, s_r)$ is a palindrome, or if there is no ℓ that satisfies the conditions of Lemma 6.1 and 6.4, then $\omega_{3,r} \in \mathcal{E}_{3,r}$ as summarized in Table 6.7 and Table 6.8.
  Otherwise, according to Proposition 6.3, we know that there exists $\ell \in \mathcal{L}_r$. Moreover, we know from Observation 6.4 that there is always a round $r \leqslant 411$ so that we can use one of Lemma 6.1, 6.2, 6.3 or 6.4 and prove that we have $\mathcal{M}_{3,r} \subseteq \mathcal{E}_{3,r}$.

□

In Table 6.9 we compare the number of maximum-weight exponents that appear in the univariate form of the polynomial describing MiMC$_3[r]$ and the number of exponents we obtain from Proposition 6.5 (figures in purple-bold correspond to rounds for which we get the exact number of exponents).

round	6	7	8	9	10	11	12	13	14	15	16	17	18
observed	2	2	21	14	4	2	2	37	22	2	2	94	32
exhibited in Proposition 6.5	**2**	**2**	**21**	**14**	2	**2**	**2**	**37**	**22**	**2**	**2**	93	28

Table 6.9: *Number of maximum-weight exponents.*

6.3 Some directions for other permutations

In this section we give some ideas and suggestions to replicate the same procedure for other round permutations, i.e. for MiMC$_d$ with $d > 3$. In Sections 5.3.1 and 5.3.2 we have exhibited bounds on the algebraic degree of MiMC$_d$ for $d = 2^j + 1$ and $d = 2^j - 1$ respectively. In what follows our aim is then to study the existence of trails to construct exponents of Hamming-weight reaching this bound. As we have seen in previous sections, exponent construction is a fairly complicated process. Furthermore, it seems difficult to generalize the results since the trails found depend on the power function used in MiMC$_d$.

6.3.1 For MiMC$_d$, where $d = 2^j + 1$

We first focus on adapting the process for MiMC$_d$, where d is a Gold function different than the cube, i.e. $d = 2^j + 1$ with $j > 1$.

6.3.1.1 Tracing exponents for MiMC$_5$

Let $d = 5$ and $(k_{5,r})_{r\geqslant 1}$ and $(b_{5,r})_{r\geqslant 1}$ be the sequences respectively defined by $k_{5,r} = \lfloor r \log_2 5 \rfloor$ and $b_{5,r} = k_{5,r} \mod 4$. We recall that B_5^r is the maximal algebraic degree reached for at least one sequence of constants for MiMC$_5$. In Table 6.10 we derived B_5^r for the first rounds using the C implementation of Corollary 5.1.

r	4	5	6	7	8	9	10	11	12
$k_{5,r}$	9	11	13	16	18	20	23	25	27
$b_{5,r}$	1	3	1	0	2	0	3	1	3
B_5^r	7	10	12	14	16	19	22	23	26
$B_5^r - k_{5,r}$	2	1	1	2	2	1	1	2	1

Table 6.10: *Comparison between B_5^r and $k_{5,r}$.*

We observe the following:

- if $b_{5,r} \in \{0, 1\}$ then $B_5^r \in \{k_{5,r} - 1, k_{5,r} - 2\}$,
- if $b_{5,r} = 2$ then $B_5^r = k_{5,r} - 2$,
- if $b_{5,r} = 3$ then $B_5^r = k_{5,r} - 1$.

Let us recall that in Proposition 5.8, we found that B_5^r satisfies

$$B_d^r \leqslant \begin{cases} k_{5,r} - 1 & \text{if } b_{5,r} \in \{0, 1, 3\}\ , \\ k_{5,r} - 2 & \text{if } b_{5,r} = 2\ , \end{cases}$$

implying that the bound can be improved.

In what follows our aim is to construct exponents of maximum-weight, i.e. exponents whose Hamming weight reaches B_5^r, as given in Table 6.10. We conjecture that depending on the value $b_{5,r}$ and the expected algebraic degree, some specific exponents appear at each round.

Conjecture 6.4. *Let $k_{5,r} = \lfloor r \log_2 5 \rfloor$, $b_{5,r} = k_{5,r} \mod 4$ and $\mathcal{E}_{5,r}$ be the set of exponents appearing in round r. We have:*

(i) *if $b_{5,r} = 0$ then $2^{k_{5,r}+1} - 2^{k_{5,r}-2} - 3 \in \mathcal{E}_{5,r}$ or $2^{k_{5,r}} - 2^{k_{5,r}-1} - 3 \in \mathcal{E}_{5,r}$,*

(ii) *if $b_{5,r} = 1$ then $2^{k_{5,r}+1} - 2^{k_{5,r}-1} - 3 \in \mathcal{E}_{5,r}$ or $2^{k_{5,r}} - 2^{k_{5,r}-3} - 3 \in \mathcal{E}_{5,r}$,*

(iii) *if $b_{5,r} = 2$ then $2^{k_{5,r}} - 2^{k_{5,r}-2} - 3 \in \mathcal{E}_{5,r}$,*

(iv) *if $b_{5,r} = 3$ then $2^{k_{5,r}} - 3 \in \mathcal{E}_{5,r}$.*

To prove such a property in light of what has been proved for MiMC$_3$, two steps are required:

1. finding some trails to construct maximum-weight exponents with those of the previous rounds, and
2. initializing the induction for some sporadic cases.

For the first point, we can already observe the following.

- Let $k_{5,r} = 1 \bmod 4$ and $k_{5,r-1} = k_{5,r} - 2 = 3 \bmod 4$, implying that $B_5^{r-1} = k_{5,r-1} - 1$. Let $e_{r-1} = 2^{k_{5,r}-2} - 3$. By hypothesis $e_{r-1} \in \mathcal{E}_{5,r-1}$.

  Let $e_r = 2^{k_{5,r}} - 2^{k_{5,r}-3} - 3$. We observe that

$$5 \times \left(\sum_{j=1}^{\lfloor k_{5,r}/4 \rfloor - 1} \left(2^{4j-1} + 2^{4j}\right) + 2^{k_{5,r}-3} \right) = \sum_{j=1}^{\lfloor k_{5,r}/4 \rfloor - 1} \left(\sum_{i=-1}^{2} 2^{4j+i} \right) + 2^{k_{5,r}-3} + 2^{k_{5,r}-1}$$
$$= \sum_{j=3}^{4\lfloor k_{5,r}/4 \rfloor - 2} 2^j + 2^{k_{5,r}-3} + 2^{k_{5,r}-1} ,$$

  where $4\lfloor k_{5,r}/4 \rfloor = k_{5,r} - 1$ since $k_{5,r} = 1 \bmod 4$. We deduce that

$$5 \times \left(\sum_{j=1}^{\lfloor k_{5,r}/4 \rfloor - 1} \left(2^{4j-1} + 2^{4j}\right) + 2^{k_{5,r}-3} \right) = \sum_{j=3}^{k_{5,r}-4} 2^j + 2^{k_{5,r}-2} + 2^{k_{5,r}-1} ,$$

  leading to

$$e_r/5 = 1 + \sum_{j=1}^{\lfloor k_{5,r}/4 \rfloor - 1} \left(2^{4j-1} + 2^{4j}\right) + 2^{k_{5,r}-3} .$$

  We get $e_r/5 \le 2^{k_{5,r}-2} - 3 = e_{r-1}$ implying that $e_r = 2^{k_{5,r}} - 3 \in \mathcal{E}_{5,r}$.

- Let $k_{5,r} = 3 \bmod 4$ and $k_{5,r-1} = k_{5,r} - 3 = 0 \bmod 4$, implying that $B_5^{r-1} = k_{5,r-1} - 1$. Let $e_{r-1} = 2^{k_{5,r}-2} - 2^{k_{5,r}-5} - 3$. By hypothesis $e_{r-1} \in \mathcal{E}_{5,r-1}$.

  Let $e_r = 2^{k_{5,r}} - 3$. We observe that

$$5 \times \left(\sum_{j=1}^{\lfloor k_{5,r}/4 \rfloor} \left(2^{4j-1} + 2^{4j}\right) \right) = \sum_{j=3}^{4\lfloor k_{5,r}/4 \rfloor + 2} 2^j ,$$

  with $4\lfloor k_{5,r}/4 \rfloor = k_{5,r} - 3$, leading to

$$e_r/5 = 1 + \sum_{j=1}^{\lfloor k_{5,r}/4 \rfloor} \left(2^{4j-1} + 2^{4j}\right) .$$

  We get $e_r/5 \le 2^{k_{5,r}-2} - 2^{k_{5,r}-5} - 3 = e_{r-1}$ implying that $2^{k_{5,r}} - 3 \in \mathcal{E}_{5,r}$.

To complete the proof, it would then be necessary to perform the same procedure for each case. At the time of writing, we have not been able to find trails for all the exponents. Several reasons may explain this problem: we might not have started from the right exponent to establish a trail, or we might need to try constructing other families of exponents. As we saw earlier, exponents of maximum weight are not unique, and for some of them trails are more difficult to construct than for others.

6.3.1.2 Tracing exponents for MiMC$_9$

Now, let $d = 9$, and $(k_{9,r})_{r \geqslant 1}$ and $(b_{9,r})_{r \geqslant 1}$ be the sequences respectively defined by $k_{9,r} = \lfloor r \log_2 9 \rfloor$ and $b_{9,r} = k_{9,r} \bmod 6$. Looking at the sequence $(b_{9,r})_{r \geqslant 1}$ we observe some regular

r	4	5	6	7	8	9	10	11	12
$k_{9,r}$	12	15	19	22	25	28	31	34	38
$b_{9,r}$	0	3	1	4	1	4	1	4	2
B_9^r	7	10	15	20	22	26	28	32	34
$B_9^r - k_{9,r}$	5	5	4	2	3	2	3	2	4

Table 6.11: *Comparison between B_9^r and $k_{9,r}$.*

patterns alternating 0 and 3, then 1 and 4, then 2 and 5, then 0 and 3 and so on. Table 6.11 shows the beginning of the pattern. We computed B_9^r from the C implementation of Corollary 5.1.

In particular, we notice that inside each pattern, we can construct easy trails for some specific exponents. Consider r such that $b_{9,r} = k_{9,r} \bmod 6$ and $k_{9,r-1} = k_{9,r} - 3$.

- Let $b_{9,r} = 1$ and $b_{9,r-1} = 4$. Suppose $e_{r-1} = 2^{k_{9,r}-3} - 7 \in \mathcal{E}_{9,r-1}$, and let $e_r = 2^{k_{9,r}} - 2^8 - 7$. Then we have
$$e_r/9 = 1 + 2^4 + 2^5 + 2^6 + 2^8 + 2^9 + \sum_{j=2}^{\lfloor k_{9,r}/6 \rfloor - 1} \left(2^{6j+1} + 2^{6j+2} + 2^{6j+3}\right) .$$
As $e_r/9 \leq 2^{k_{9,r}-3} - 7$ it implies that $2^{k_{9,r}} - 2^8 - 7 \in \mathcal{E}_{9,r}$.
- Let $b_{9,r} = 4$ and $b_{9,r-1} = 1$. Suppose $e_{r-1} = 2^{k_{9,r}-3} - 2^8 - 7 \in \mathcal{E}_{9,r-1}$, and let $e_r = 2^{k_{9,r}} - 7$. Then we have
$$e_r/9 = 1 + \sum_{j=1}^{\lfloor k_{9,r}/6 \rfloor} \left(2^{6j-2} + 2^{6j-1} + 2^{6j}\right) .$$
As $e_r/9 \leq 2^{k_{9,r}-3} - 2^8 - 7$ it implies that $2^{k_{9,r}} - 7 \in \mathcal{E}_{9,r}$.
- Let $b_{9,r} = 2$ and $b_{9,r-1} = 5$. Suppose $e_{r-1} = 2^{k_{9,r}-4} - 7 \in \mathcal{E}_{9,r-1}$, and let $e_r = 2^{k_{9,r}-1} - 2^8 - 7$. Then we have
$$e_r/9 = 1 + 2^4 + 2^5 + 2^6 + 2^8 + 2^9 + \sum_{j=2}^{\lfloor k_{9,r}/6 \rfloor - 1} \left(2^{6j+1} + 2^{6j+2} + 2^{6j+3}\right) .$$
As $e_r/9 \leq 2^{k_{9,r}-4} - 7$ it implies that $2^{k_{9,r}-1} - 2^8 - 7 \in \mathcal{E}_{9,r}$.
- Let $b_{9,r} = 5$ and $b_{9,r-1} = 2$. Suppose $e_{r-1} = 2^{k_{9,r}-4} - 2^8 - 7 \in \mathcal{E}_{9,r-1}$, and let $e_r = 2^{k_{9,r}-1} - 7$. Then we have
$$e_r/9 = 1 + \sum_{j=1}^{\lfloor k_{9,r}/6 \rfloor} \left(2^{6j-2} + 2^{6j-1} + 2^{6j}\right) .$$
As $e_r/9 \leq 2^{k_{9,r}-4} - 2^8 - 7$ it implies that $2^{k_{9,r}-1} - 7 \in \mathcal{E}_{9,r}$.
- Let $b_{9,r} = 0$ and $b_{9,r-1} = 3$. Suppose $e_{r-1} = 2^{k_{9,r}-3} - 2^6 - 7 \in \mathcal{E}_{9,r-1}$, and let $e_r = 2^{k_{9,r}} - 2^7 - 2^6 - 7$. Then we have
$$e_r/9 = 1 + 2^4 + 2^5 + 2^7 + 2^8 + \sum_{j=2}^{\lfloor k_{9,r}/6 \rfloor - 1} \left(2^{6j} + 2^{6j+1} + 2^{6j+2}\right) .$$

As $e_r/9 \preceq 2^{k_{9,r}-3} - 2^6 - 7$ it implies that $2^{k_{9,r}} - 2^7 - 2^6 - 7 \in \mathcal{E}_{9,r}$.

- Let $b_{9,r} = 3$ and $b_{9,r-1} = 0$. Suppose $e_{r-1} = 2^{k_{9,r}-3} - 2^7 - 2^6 - 7 \in \mathcal{E}_{9,r-1}$, and let $e_r = 2^{k_{9,r}} - 2^6 - 7$. Then we have

$$e_r/9 = 1 + 2^4 + 2^5 + \sum_{j=1}^{\lfloor k_{9,r}/6 \rfloor - 1} \left(2^{6j+3} + 2^{6j+4} + 2^{6j+5}\right) .$$

As $e_r/9 \preceq 2^{k_{9,r}-3} - 2^7 - 2^6 - 7$ it implies that $2^{k_{9,r}} - 2^6 - 7 \in \mathcal{E}_{9,r}$.

This means that inside a pattern $(b_{9,r-4}, \ldots, b_{9,r}) = (4,1,4,1,4)$, the exponent $2^{k_{9,r}-12} - 7$ in round $r-4$ allows to construct the exponent $2^{k_{9,r}-9} - 2^8 - 7$ at round $r-3$, which allows to construct the exponent $2^{k_{9,r}-6} - 7$ at round $r-2$, ... and so on until $2^{k_{9,r}} - 7$ at round r. The same arguments hold for sequences $(b_{9,r-4}, \ldots, b_{9,r}) = (5,2,5,2,5)$ and $(b_{9,r-4}, \ldots, b_{9,r}) = (3,0,3,0,3)$.

We note that we can also link the sequences. For example

- Let $b_{9,r} = 2$ and $b_{9,r-1} = 4$. Let $e_{r-1} = 2^{k_{9,r}-4} - 7$, and assume that $e_{r-1} \in \mathcal{E}_{9,r-1}$. Let $e_r = 2^{k_{9,r}-1} - 2^8 - 7$, then

$$e_r/9 = 1 + 2^4 + 2^5 + 2^6 + 2^8 + 2^9 + \sum_{j=2}^{\lfloor k_{9,r}/6 \rfloor - 1} \sum_{i=1}^{3} 2^{6j+i} \quad \preceq e_{r-1} ,$$

implying that $2^{k_{9,r}-1} - 2^8 - 7 \in \mathcal{E}_{9,r}$.

- Let $b_{9,r} = 5$ and $b_{9,r-1} = 1$. Let $e_{r-1} = 2^{k_{9,r}-4} - 2^8 - 7$, we have $e_{r-1} \in \mathcal{E}_{9,r-1}$. Let $e_r = 2^{k_{9,r}-1} - 7$, then

$$e_r/9 = 1 + \sum_{j=1}^{\lfloor k_{9,r}/6 \rfloor} \sum_{i=0}^{2} 2^{6j-i} \quad \preceq e_{r-1} ,$$

implying that $2^{k_{9,r}-1} - 7 \in \mathcal{E}_{9,r}$.

This exactly means that we can link trails constructed when $(b_{9,r-3}, b_{9,r-2}) = (1,4)$ with trails for $(b_{9,r-1}, b_{9,r}) = (2,5)$. Similarly, we can link trails for $(b_{9,r-3}, b_{9,r-2}) = (4,1)$ and for $(b_{9,r-1}, b_{9,r}) = (5,2)$.

Such trails are easy to find since it is only necessary to go back one round before, for obtaining the exponent at round r. However, it is important to note that such paths allow us to construct exponents at each round, but they do not guarantee that we will reach the maximal algebraic degree B_9^r. We only know that we can construct exponents of Hamming weight

- $k_{9,r} - 2$ when $b_{9,r} = 4$, since
$$\mathrm{wt}\left(2^K - 7\right) = K - 2 ,$$
- $k_{9,r} - 3$ when $b_{9,r} \in \{1,3,5\}$, since
$$\mathrm{wt}\left(2^K - 2^8 - 7\right) = \mathrm{wt}\left(2^K - 2^6 - 7\right) = \mathrm{wt}\left(2^{K-1} - 7\right) = K - 3 ,$$
- $k_{9,r} - 4$ when $b_{9,r} \in \{0,2\}$, since
$$\mathrm{wt}\left(2^K - 2^7 - 2^6 - 7\right) = \mathrm{wt}\left(2^{K-1} - 2^8 - 7\right) = K - 4 .$$

This only provides a lower bound on the algebraic degree of $\mathsf{MiMC}_9[r]$ and further study is required to better identify the maximum-weight exponents at each round.

6.3.1.3 Tracing exponents for MiMC$_{17}$

Finally, let $d = 17$, and $(k_{17,r})_{r\geqslant 1}$ and $(b_{17,r})_{r\geqslant 1}$ be the sequences respectively defined by $k_{17,r} = \lfloor r \log_2 17 \rfloor$ and $b_{17,r} = k_{17,r} \bmod 8$. As for MiMC$_9$, looking at the sequence $(b_{17,r})_{r\geqslant 1}$ we observe some regular patterns alternating 0 and 4, then 1 and 5, then 2 and 6, then 3 and 7, then 0 and 4 and so on. In Table 6.12 we can already see the first pattern. The values B^r_{17} were derived using the C implementation of Corollary 5.1.

r	4	5	6	7	8	9	10	11	12
$k_{17,r}$	16	20	24	28	32	36	40	44	49
$b_{17,r}$	0	4	0	4	0	4	0	4	1
B^r_{17}	7	11	16	22	26	32	35	40	44
$B^r_{17} - k_{17,r}$	9	9	8	6	6	4	5	4	5

Table 6.12: *Comparison between B^r_{17} and $k_{17,r}$.*

For MiMC$_{17}$ we have not pushed the analysis as far as for MiMC$_9$, but we can already observe similar behaviour within the sequences. For example:

- Let $b_{17,r} = 1$ and $b_{17,r-1} = 5$. Let us assume that $e_{r-1} = 2^{k_{17,r}-4} - 15$ belongs to $\mathcal{E}_{17,r-1}$. Let $e_r = 2^{k_{17,r}} - 2^{10} - 15$, then

$$e_r/17 = 1 + 2^5 + 2^6 + 2^7 + 2^8 + 2^{10} + 2^{11} + 2^{12} + \sum_{j=2}^{\lfloor k_{17,r}/8 \rfloor - 1} \sum_{i=1}^{4} 2^{8j+i} \quad \preceq e_{r-1} \,,$$

  implying that $2^{k_{17,r}} - 2^{10} - 15 \in \mathcal{E}_{17,r}$.

- Let $b_{17,r} = 5$ and $b_{17,r-1} = 1$. Let us assume that $e_{r-1} = 2^{k_{17,r}-4} - 2^{10} - 15$ belongs to $\mathcal{E}_{17,r-1}$. Let $e_r = 2^{k_{17,r}} - 15$, then

$$e_r/17 = 1 + \sum_{j=1}^{\lfloor k_{17,r}/8 \rfloor} \sum_{i=0}^{3} 2^{8j-i} \quad \preceq e_{r-1} \,,$$

  implying that $2^{k_{17,r}} - 15 \in \mathcal{E}_{17,r}$.

While the case of MiMC$_5$ seems to be slightly different, trails to construct exponents for MiMC$_9$ and MiMC$_{17}$ seem to suggest a possible generic method.

6.3.2 For MiMC$_d$, where $d = 2^j - 1$

We now focus on adapting the procedure to construct exponents for MiMC$_d$, where $d = 2^j - 1$. In Chapter 5 we have seen that a lot of the results for MiMC$_3$ could be generalized to instances of MiMC$_d$, where $d = 2^j - 1$. For such instances of MiMC$_d$, we use $b_{d,r} = k_{d,r} \bmod j$. In this section we will in particular show that a condition, similar to Observation 6.2 that limited our inductive proof to build exponents for MiMC$_3$, appear for MiMC$_7$ and more generally for any MiMC$_d$, where $d = 2^j - 1$.

6.3.2.1 Tracing exponents for MiMC_7

First, let $d = 7$ and $(k_{7,r})_{r\geqslant 1}$ and $(b_{7,r})_{r\geqslant 1}$ be the sequences respectively defined by $k_{7,r} = \lfloor r\log_2 7\rfloor$ and $b_{7,r} = k_{7,r} \bmod 3$. We also recall that B_7^r is the maximal algebraic degree reached for at least one sequence of constants for MiMC_7. In Table 6.13 we derive B_7^r using the C implementation of Corollary 5.1.

r	4	5	6	7	8	9	10	11	12
$k_{7,r}$	11	14	16	19	22	25	28	30	33
$b_{17,r}$	2	2	1	1	1	1	1	0	0
B_7^r	9	12	15	18	21	24	27	27	30
$B_7^r - k_{7,r}$	2	2	1	1	1	1	1	3	3

Table 6.13: *Comparison between B_7^r and $k_{7,r}$.*

We notice the following:

- if $b_{7,r} = 0$ then $B_7^r = k_{7,r} - 3$,
- if $b_{7,r} = 1$ then $B_7^r = k_{7,r} - 1$,
- if $b_{7,r} = 2$ then $B_7^r = k_{7,r} - 2$.

Let us notice that these observations exactly correspond to the bound found in Corollary 5.3, where we have shown that:

$$B_7^r \leqslant \begin{cases} k_{7,r} - 3 & \text{if } b_{7,r} = 0\,, \\ k_{7,r} - b_{7,r} & \text{otherwise}\,. \end{cases}$$

Our aim is then to construct exponents of maximum-weight, i.e. exponents whose Hamming weight reaches B_7^r. We conjecture that depending on the value of $b_{7,r}$ and the expected algebraic degree, some specific exponents appear in each round.

Conjecture 6.5. *Let $k_{7,r} = \lfloor r\log_2 7\rfloor$, $b_{7,r} = k_{7,r} \bmod 3$ and $\mathcal{E}_{7,r}$ be the set of exponents appearing at round r. We have:*

(i) *if $b_{7,r} = 0$ then $2^{k_{7,r}-2} - 9 \in \mathcal{E}_{7,r}$,*

(ii) *if $b_{7,r} = 1$ then $2^{k_{7,r}} - 9 \in \mathcal{E}_{7,r}$,*

(iii) *if $b_{7,r} = 2$ then $2^{k_{7,r}-1} - 9 \in \mathcal{E}_{7,r}$.*

Let us consider some examples to understand how to construct such exponents. The procedure observed in these examples is always the same. We are first considering an integer e_{r-1} resulting from the addition of $\left(2^{k_{7,r}-2} - 9\right)/7$ and a certain sum S. This sum must be chosen so that $e_{r-1}/7^{r-10-1} \preceq e_{10}$. Then we conclude that $e_r = 2^{k_{7,r}-2} - 9 \in \mathcal{E}_{7,r}$ since $e_r/7 \preceq e_{r-1}$.

Example 6.4. First let us observe that $k_{7,10} = 28$ so $b_{7,10} = 1$. Suppose that $e_{10} = 2^{28} - 9 \in \mathcal{E}_{7,10}$. We will show that starting from this exponent, we can construct maximum-weight exponent at rounds 11, 12, 13 or 14 for example.

- At round 11, we have $k_{7,11} = 30$ so $b_{7,11} = 0$. Then $e_{11} = 2^{28} - 9 = e_{10}$ so that e_{11} belongs to $\mathcal{E}_{7,11}$.

- At round 12, we have $k_{7,12} = 33$ so $b_{7,12} = 0$. Then

$$e_{10} \xrightarrow{\mathsf{Mult}_7 \circ \mathsf{Cover}} 2 + (2^{31} - 9)/7 \xrightarrow{\mathsf{Mult}_7 \circ \mathsf{Cover}} 2^{31} - 9\,,$$

  implies that $e_{12} = 2^{31} - 9 \in \mathcal{E}_{7,12}$.

- At round 13, we have $k_{7,13} = 36$ so $b_{7,13} = 0$. Then

$$e_{10} \xrightarrow{\mathsf{Mult}_{(7^2)} \circ \mathsf{Cover}} 2^2 + 2^6 + 2^8 + 2^9 + (2^{34} - 9)/7 \xrightarrow{\mathsf{Mult}_7 \circ \mathsf{Cover}} 2^{34} - 9\,,$$

  implies that $e_{13} = 2^{34} - 9 \in \mathcal{E}_{7,13}$.

- At round 14, we have $k_{7,14} = 39$ so $b_{7,14} = 0$. Then

$$e_{10} \xrightarrow{\mathsf{Mult}_{(7^3)} \circ \mathsf{Cover}} e_{13} \xrightarrow{\mathsf{Mult}_7 \circ \mathsf{Cover}} 2^{37} - 9\,,$$

  where $e_{13} = 2 + 2^2 + 2^5 + 2^{11} + 2^{14} + 2^{15} + (2^{37} - 9)/7$, implies that $e_{14} = 2^{37} - 9$ belongs to $\mathcal{E}_{7,14}$.

6.3.2.2 Generalization

Let us generalize the procedure for MiMC_d when $d = 2^j - 1$. Let ℓ be an integer such that $b_{d,r-\ell} = 1$. Then, we suppose that $e_{r-\ell} = 2^{k_{d,r-\ell}} - d - 2 \in \mathcal{E}_{d,r-\ell}$. Let e_{r-1} be such that

$$e_{r-1} = \left(2^{k_{d,r}} - d - 2\right)/d + S = 1 + \sum_{i=1}^{\lfloor k_{d,r}/j \rfloor - 1} 2^{j \times i + 1} + S\,.$$

Choosing a sum S such that $e_{r-1}/d^{\ell-1}$ is covered by $e_{r-\ell}$, would imply that $e_{r-1} \in \mathcal{E}_{d,r-1}$. If such a sum exists, then we can conclude that $e_r = 2^{k_{d,r}-2} - d - 2 \in \mathcal{E}_{d,r}$ by observing that

$$(2^{k_{d,r}-2} - d - 2)/d \preceq e_{r-1}\,.$$

Therefore, all the remaining work is to find S. Exhibiting similar conditions as for MiMC_3 (see Observation 6.2), we would need to prove that any element x in $\mathbb{Z}/d^{\ell-1}\mathbb{Z}$ can be written as follows:

$$x = \sum_{i=1}^{j-1} \varepsilon_i 2^i + \sum_{t=0}^{j-2} \left[\sum_{i=2}^{m_\ell} \varepsilon_{j \times i - t} 2^{j \times i - t} \right] \bmod d^{\ell-1}\,,$$

where all the ε_i are in $\{0, 1\}$.

Note that is not yet clear which value to choose for m_t. Although having a large interval might help to solve this conjecture, this could also limit the usefulness of this observation in the inductive proof to derive maximum-weight exponents by increasing the number of sporadic cases.

6.4 Rounds 3 and 4 of MiMC_3^{-1}

In light of Chapter 5, where we first give bounds on the algebraic degree of specific instances of MiMC_d and then investigate the case of the inverse transformation, we are also interested in finding trails to build maximum-weight exponents for MiMC_3^{-1}.

Let us recall that the inverse transformation MiMC_3^{-1} is obtained by reversing the order of the round constants and by replacing the round function by $F^{-1}(x) = x^s$ with

$$s = \frac{2^{n+1}-1}{3} = \sum_{i=0}^{(n-1)/2} 2^{2i} .$$

In Section 5.4 we have proved the existence of a plateau between the first two rounds, and we have also considered an upper bound using a result from [BC13]. We have indeed shown that if r_{n-i} denotes the smallest value of r such that $B_s^r \geqslant n-i$ for $1 \leqslant i \leqslant (n-1)/4$, then

$$r_{n-i} \geqslant \left\lceil \frac{1}{\log_2 3}\left(2\left\lceil \frac{1}{2}\left\lceil \frac{n-1}{i}\right\rceil\right\rceil + 1\right)\right\rceil .$$

In this section, our aim is now to give some trails to construct exponents in order to provide a lower bound on the algebraic degree at rounds 3 (see Section 6.4.1) and 4 (see Section 6.4.2). More precisely, in the following we will show how we came to Figure 6.31.

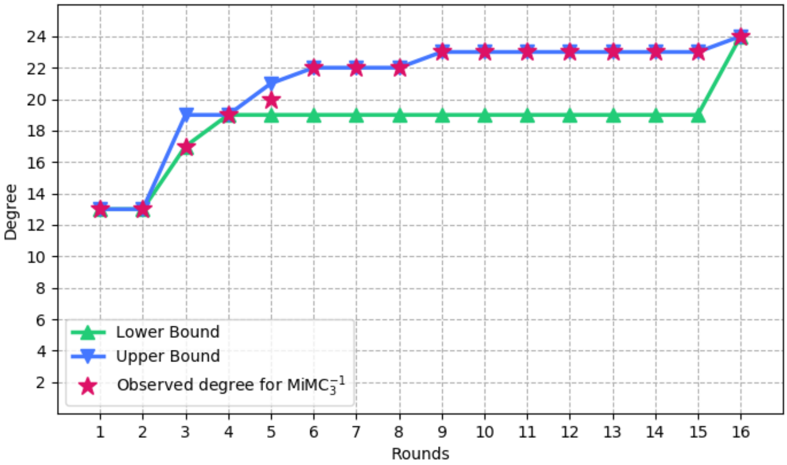


Figure 6.31: *Bounds on the degree of* MiMC_3^{-1} *when* $n = 25$.

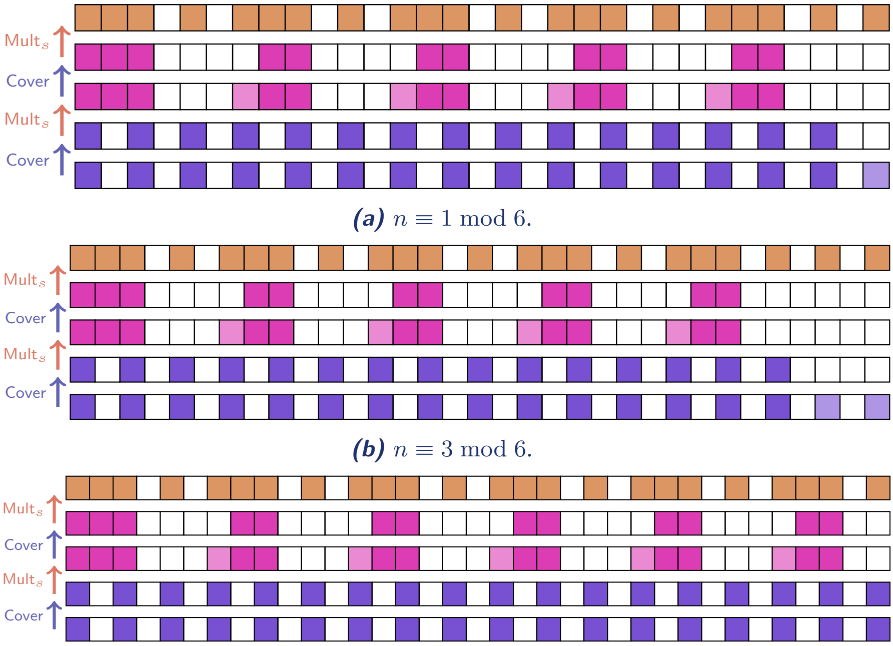
6.4.1 Lower bound for round 3

First, we exhibit a lower bound on the algebraic degree at round 3:

Proposition 6.6. *The algebraic degree at round 3 for* MiMC_3^{-1} *satisfies:*

$$B_s^3 \geqslant \frac{n+1}{2} + \left\lfloor \frac{n+1}{6} \right\rfloor .$$

Before giving the proof, we propose Figure 6.32 to see that the procedure to derive the exponent in round 3 depends on the value of n modulo 6. On the first line the squares 🟧 represent the active bits of e_3, on the second and third lines the squares 🟥 the active bits of e_3/s and e_2 and on the fourth and fifth lines the squares 🟪 the active bits of e_2/s and s.



(a) $n \equiv 1 \bmod 6.$

(b) $n \equiv 3 \bmod 6.$

(c) $n \equiv 5 \bmod 6.$

Figure 6.32: *How to derive exponents for 3 rounds of* MiMC_3^{-1}.

Proof of Proposition 6.6. To prove the result we will exhibit one exponent of Hamming weight $(n+1)/2 + \lfloor (n+1)/6 \rfloor$ that belongs to $\mathcal{E}_{s,3}$. First, let us recall that $s \in \mathcal{E}_{s,1}$ and $\mathcal{E}_{s,2} = \{sj \bmod (2^n - 1)$ where $j \preceq s\}$. Then let

$$e_2 = \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+1} + 2^{6k+2}\right) .$$

We have $e_2/s = 3 \times e_2 \bmod (2^n - 1)$ so

$$\begin{aligned} e_2/s = 3 \times & \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+1} + 2^{6k+2}\right) \\ = & \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+1} + 2^{6k+1} + 2^{6k+2} + 2^{6k+2} + 2^{6k+3}\right) \\ = & \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+2} + 2^{6k+4}\right) . \end{aligned}$$

We deduce that $e_2/s \preceq s$, implying that $e_2 \in \mathcal{E}_{s,2}$. Then let us take

$$e_3 = \begin{cases} \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+1} + 2^{6k+2} + 2^{6k+4}\right) + \sum_{3\lfloor (n+1)/6 \rfloor}^{(n-1)/2} 2^{2k} & \text{if } n \equiv 1, 3 \bmod 6 , \\ \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+1} + 2^{6k+2} + 2^{6k+4}\right) & \text{if } n \equiv 5 \bmod 6 . \end{cases}$$

We have $e_3/s = 3 \times e_3 \bmod (2^n - 1)$. Then if $n \equiv 1, 3 \bmod 6$ we have:

$$\begin{aligned} e_3/s &= 3 \times \left(\sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+1} + 2^{6k+2} + 2^{6k+4}\right) + \sum_{3\lfloor (n+1)/6 \rfloor}^{(n-1)/2} 2^{2k} \right) \\ &= \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2 \cdot 2^{6k+1} + 2 \cdot 2^{6k+2} + 2^{6k+3} + 2^{6k+4} + 2^{6k+5}\right) + \sum_{6\lfloor (n+1)/6 \rfloor}^{n} 2^k \\ &= 1 + 2^2 + \sum_{k=1}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k+1} + 2^{6k+2}\right) + 2^{6\lfloor (n+1)/6 \rfloor} + \sum_{6\lfloor (n+1)/6 \rfloor}^{n} 2^k \\ &= 1 + 2^2 + \sum_{k=1}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k+1} + 2^{6k+2}\right) + 2^{n+1} \\ &\equiv 1 + \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} 2^{6k+1} + 2^{6k+2} \quad \bmod (2^n - 1) . \end{aligned}$$

Similarly, if $n \equiv 5 \bmod 6$, we have:

$$\begin{aligned} e_3/s &= 3 \times \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2^{6k+1} + 2^{6k+2} + 2^{6k+4}\right) \\ &= \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k} + 2 \cdot 2^{6k+1} + 2 \cdot 2^{6k+2} + 2^{6k+3} + 2^{6k+4} + 2^{6k+5}\right) \\ &= 1 + 2^2 + \sum_{k=1}^{\lfloor (n+1)/6 \rfloor - 1} \left(2^{6k+1} + 2^{6k+2}\right) + 2^{n+1} \\ &\equiv 1 + \sum_{k=0}^{\lfloor (n+1)/6 \rfloor - 1} 2^{6k+1} + 2^{6k+2} \quad \bmod (2^n - 1) . \end{aligned}$$

Then $e_3/s \preceq e_2$, implying that $e_3 \in \mathcal{E}_{s,3}$.

Finally, let us notice that if $n \equiv 1, 3 \bmod 6$, we have

$$\mathrm{wt}(e_3) = \left(\left\lfloor \frac{n+1}{6} \right\rfloor - 1 + 1 \right) \times 4 + \left(\frac{n-1}{2} + 3 \left\lfloor \frac{n+1}{6} \right\rfloor + 1 \right) = \frac{n+1}{2} + \left\lfloor \frac{n+1}{6} \right\rfloor ,$$

and if $n \equiv 5 \bmod 6$, we have:

$$\mathrm{wt}(e_3) = \left(\left\lfloor \frac{n+1}{6} \right\rfloor - 1 + 1 \right) \times 4 = \left(\left\lfloor \frac{n+1}{6} \right\rfloor \right) \times 3 + \left\lfloor \frac{n+1}{6} \right\rfloor = \frac{n+1}{2} + \left\lfloor \frac{n+1}{6} \right\rfloor ,$$

Therefore, the algebraic degree at round 3 for MiMC_3^{-1} is at least $(n+1)/2 + \lfloor (n+1)/6 \rfloor$. □

More precisely, the algebraic degree in round 3 for the inverse seems to exactly correspond to $(n+1)/2 + \lfloor (n+1)/6 \rfloor$. However the proposition only gives a lower bound, while the upper bound found in Section 5.4.2 is $\frac{n+1}{2} + \left\lfloor \frac{n}{4} \right\rfloor$ which is not tight.

6.4.2 Exact degree for round 4

In this section, we investigate the case of round 4. More precisely we will show that the algebraic degree of MiMC_3^{-1} after 4 rounds is exactly $(n+1)/2 + \lfloor n/4 \rfloor$.

Remark 6.5. Let us notice that in Corollary 5.5 we have shown that the last round satisfying this condition is:

$$\left\lfloor \frac{1}{\log_2 3} \left(2 \left\lceil \left\lceil \frac{n-1}{i} \right\rceil /2 - 1 \right\rceil + 3 \right) \right\rfloor \quad \text{where } i = \left(\frac{n}{4} - \frac{1}{2} \right) .$$

This exactly means that the bound on the algebraic degree satisfies $B_s^r \leqslant (n+1)/2 + \lfloor n/4 \rfloor$ for $r = \lfloor 7/\log_2 3 \rfloor = 4$.

Now let us prove that this upper bound is also a lower bound. We will use the same procedure as for round 3 to construct some specific exponents appearing in round 4.

Proposition 6.7. *The algebraic degree at round 4 for* MiMC_3^{-1} *satisfies:*

$$B_s^4 \geqslant \frac{n+1}{2} + \left\lfloor \frac{n}{4} \right\rfloor .$$

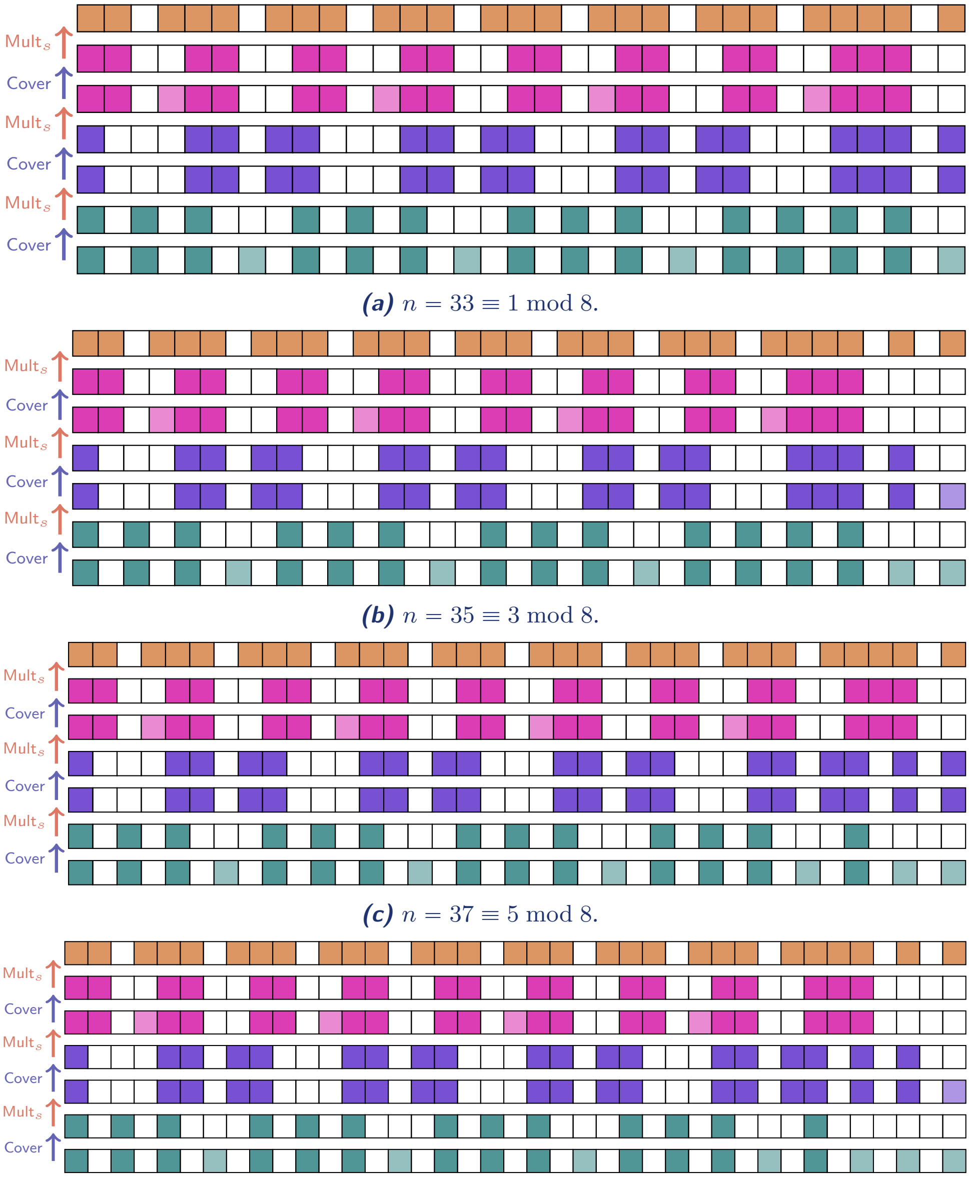
Before giving the proof, we propose Figure 6.33 to see that the procedure to derive the exponents at round 4 depends on the value of n modulo 8. On the first line the squares 🟧 represent the active bits of e_4, on the second and third lines the squares 🟥 the active bits of e_4/s and e_3, on the fourth and fifth lines the squares 🟪 the active bits of e_3/s and e_2 and on the sixth and seventh lines the squares 🟦 the active bits of e_2/s and s.

Proof of Proposition 6.7. We prove that there exists $e_4 \in \mathcal{E}_{s,4}$ such that $wt(e) = (n+1)/2 + \lfloor n/4 \rfloor$. Let

$$e_2 = \begin{cases} 1 + \displaystyle\sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{1,3,4,5\}} 2^{n-i} & \text{if } n \equiv 1 \bmod 8 , \\ 1 + \displaystyle\sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{1,3,5,6,7\}} 2^{n-i} & \text{if } n \equiv 3 \bmod 8 , \\ 1 + \displaystyle\sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{1,3\}} 2^{n-i} & \text{if } n \equiv 5 \bmod 8 , \\ 1 + \displaystyle\sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{1,3,5\}} 2^{n-i} & \text{if } n \equiv 7 \bmod 8 . \end{cases}$$

We have $e_2/s = 3 \times e_2 \bmod (2^n - 1)$. Then if $n \equiv 1 \bmod 8$, we have:

$$e_2/s = 3 \times \left(1 + \sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{1,3,4,5\}} 2^{n-i} \right) ,$$



(a) $n = 33 \equiv 1 \bmod 8$.

(b) $n = 35 \equiv 3 \bmod 8$.

(c) $n = 37 \equiv 5 \bmod 8$.

(d) $n = 39 \equiv 7 \bmod 8$.

Figure 6.33: *How to derive exponents for 4 rounds of* MiMC_3^{-1}.

so that

$$\begin{aligned} e_2/s &= 3 + \sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(2^{8k+4} + 2 \cdot 2^{8k+5} + 2^{8k+6} + 2^{8k+7} + 2 \cdot 2^{8k+8} + 2^{8k+9}\right) \\ &\quad + 2^{n-5} + 2 \cdot 2^{n-4} + 2 \cdot 2^{n-3} + 2^{n-2} + 2^{n-1} + 2^{n} \\ &= 3 + \sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(2^{8k+4} + 2^{8k+8} + 2^{8k+10}\right) + 2^{n-5} + 2^{n-3} + 2^{n+1} \,. \end{aligned}$$

It follows that

$$e_2/s \equiv \sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(2^{8k} + 2^{8k+2} + 2^{8k+4}\right) + 2^{8\lfloor n/8 \rfloor - 2} \mod (2^n - 1)\,.$$

Similarly, if $n \equiv 3 \bmod 8$ we have:

$$\begin{aligned}
e_2/s &= 3 \times \left(1 + \sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i}\right) + \sum_{i \in \{1,3,5,6,7\}} 2^{n-i}\right) \\
&= 3 + \sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(2^{8k+4} + 2 \cdot 2^{8k+5} + 2^{8k+6} + 2^{8k+7} + 2 \cdot 2^{8k+8} + 2^{8k+9}\right) \\
&\quad + 2^{n-7} + 2 \cdot 2^{n-6} + 2 \cdot 2^{n-5} + 2^{n-4} + 2^{n-3} + 2^{n-2} + 2^{n-1} + 2^n \\
&= 3 + \sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(2^{8k+4} + 2^{8k+8} + 2^{8k+10}\right) + 2^{n-7} + 2^{n-5} + 2^{n+1}\,,
\end{aligned}$$

implying that

$$e_2/s \equiv \sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(2^{8k} + 2^{8k+2} + 2^{8k+4}\right) + 2^{8\lfloor n/8 \rfloor - 2} \mod (2^n - 1)\,.$$

If $n \equiv 5 \bmod 8$ we have:

$$\begin{aligned}
e_2/s &= 3 \times \left(1 + \sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i}\right) + \sum_{i \in \{1,3\}} 2^{n-i}\right) \\
&= 3 + \sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(2^{8k+4} + 2 \cdot 2^{8k+5} + 2^{8k+6} + 2^{8k+7} + 2 \cdot 2^{8k+8} + 2^{8k+9}\right) \\
&\quad + 2^{n-3} + 2^{n-2} + 2^{n-1} + 2^n \\
&= 3 + \sum_{k=0}^{\lfloor n/8 \rfloor - 2} \left(2^{8k+4} + 2^{8k+8} + 2^{8k+10}\right) + 2^{8\lfloor n/8 \rfloor - 4} + 2^{8\lfloor n/8 \rfloor} + 2^{n+1}\,,
\end{aligned}$$

so that

$$e_2/s \equiv \sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(2^{8k} + 2^{8k+2} + 2^{8k+4}\right) + 2^{8\lfloor n/8 \rfloor} \mod (2^n - 1)\,.$$

Finally, if $n \equiv 7 \bmod 8$ we have:

$$\begin{aligned}
e_2/s &= 3 \times \left(1 + \sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i}\right) + \sum_{i \in \{1,3,5\}} 2^{n-i}\right) \\
&= 3 + \sum_{k=0}^{\lfloor n/8 \rfloor - 1} \left(2^{8k+4} + 2 \cdot 2^{8k+5} + 2^{8k+6} + 2^{8k+7} + 2 \cdot 2^{8k+8} + 2^{8k+9}\right) \\
&\quad + 2^{n-5} + 2^{n-4} + 2^{n-3} + 2^{n-2} + 2^{n-1} + 2^n\,,
\end{aligned}$$

leading to

$$e_2/s = 3 + \sum_{k=0}^{\lfloor n/8\rfloor-2} \left(2^{8k+4} + 2^{8k+8} + 2^{8k+10}\right) + 2^{8\lfloor n/8\rfloor-4} + 2^{8\lfloor n/8\rfloor} + 2^{n+1}\,.$$

Then, we have

$$e_2/s \equiv \sum_{k=0}^{\lfloor n/8\rfloor-1} \left(2^{8k} + 2^{8k+2} + 2^{8k+4}\right) + 2^{8\lfloor n/8\rfloor} \mod (2^n-1)\,.$$

So we have

$$e_2/s = \begin{cases} \sum_{k=0}^{\lfloor n/8\rfloor-1} \left(2^{8k} + 2^{8k+2} + 2^{8k+4}\right) + 2^{8\lfloor n/8\rfloor-2} & \text{if } n \equiv 1,3 \bmod 8\,,\\ \sum_{k=0}^{\lfloor n/8\rfloor-1} \left(2^{8k} + 2^{8k+2} + 2^{8k+4}\right) + 2^{8\lfloor n/8\rfloor} & \text{if } n \equiv 5,7 \bmod 8\,. \end{cases}$$

It follows that $(e_2/s) \preceq s$ implying that $e_2 \in \mathcal{E}_{s,2}$. Then let

$$e_3 = \begin{cases} \sum_{k=0}^{\lfloor n/8\rfloor-1} \left(\sum_{i\in\{0,1,3,4,5\}} 2^{8k+i}\right) + 2^{8\lfloor n/8\rfloor-2} & \text{if } n \equiv 1,3 \bmod 8\,,\\ \sum_{k=0}^{\lfloor n/8\rfloor-1} \left(\sum_{i\in\{0,1,3,4,5\}} 2^{8k+i}\right) + \sum_{i\in\{0,1,2\}} 2^{8\lfloor n/8\rfloor+i} & \text{if } n \equiv 5,7 \bmod 8\,. \end{cases}$$

We have $e_3/s = 3 \times e_3 \bmod (2^n-1)$. Then if $n \equiv 1,3 \bmod 8$ we have:

$$\begin{aligned} e_3/s &= 3 \times \left(\sum_{k=0}^{\lfloor n/8\rfloor-1} \left(\sum_{i\in\{0,1,3,4,5\}} 2^{8k+i}\right) + 2^{8\lfloor n/8\rfloor-2}\right)\\ &= \sum_{k=0}^{\lfloor n/8\rfloor-1} \left(2^{8k} + 2\cdot 2^{8k+1} + 2^{8k+2} + 2^{8k+3} + 2\cdot 2^{8k+4} + 2\cdot 2^{8k+5} + 2^{8k+6}\right)\\ &\quad + 2^{8\lfloor n/8\rfloor-2} + 2^{8\lfloor n/8\rfloor-1}\\ &= \sum_{k=0}^{\lfloor n/8\rfloor-1} \left(2^{8k} + 2^{8k+4} + 2^{8k+5} + 2^{8k+7}\right) + 2^{8\lfloor n/8\rfloor-2} + 2^{8\lfloor n/8\rfloor-1}\\ &= 1 + \sum_{k=0}^{\lfloor n/8\rfloor-2} \left(2^{8k+4} + 2^{8k+5} + 2^{8k+7} + 2^{8k+8}\right)\\ &\quad + 2^{8\lfloor n/8\rfloor-4} + 2^{8\lfloor n/8\rfloor-3} + 2^{8\lfloor n/8\rfloor-1} + 2^{8\lfloor n/8\rfloor-2} + 2^{8\lfloor n/8\rfloor-1}\\ &\equiv 1 + \sum_{k=0}^{\lfloor n/8\rfloor-2} \left(\sum_{i\in\{4,5,7,8\}} 2^{8k+i}\right) + \sum_{i\in\{0,2,3,4\}} 2^{8\lfloor n/8\rfloor-i} \mod (2^n-1)\,. \end{aligned}$$

Similarly, if $n \equiv 5, 7 \bmod 8$ we have:

$$\begin{aligned}
e_3/s &= 3 \times \left(\sum_{k=0}^{\lfloor n/8 \rfloor -1} \left(\sum_{i \in \{0,1,3,4,5\}} 2^{8k+i} \right) + \sum_{i \in \{0,1,2\}} 2^{8\lfloor n/8 \rfloor +i} \right) \\
&= \sum_{k=0}^{\lfloor n/8 \rfloor -1} \left(2^{8k} + 2 \cdot 2^{8k+1} + 2^{8k+2} + 2^{8k+3} + 2 \cdot 2^{8k+4} + 2 \cdot 2^{8k+5} + 2^{8k+6} \right) \\
&\quad + 2^{8\lfloor n/8 \rfloor} + 2 \cdot 2^{8\lfloor n/8 \rfloor +1} + 2 \cdot 2^{8\lfloor n/8 \rfloor +2} + 2^{8\lfloor n/8 \rfloor +3} \\
&= \sum_{k=0}^{\lfloor n/8 \rfloor -1} \left(2^{8k} + 2^{8k+4} + 2^{8k+5} + 2^{8k+7} \right) + 2^{8\lfloor n/8 \rfloor} + 2^{8\lfloor n/8 \rfloor +2} + 2^{8\lfloor n/8 \rfloor +4} \\
&\equiv 1 + \sum_{k=0}^{\lfloor n/8 \rfloor -1} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{2,4\}} 2^{8\lfloor n/8 \rfloor +i} \mod (2^n - 1)\,.
\end{aligned}$$

So we have

$$e_3/s = \begin{cases} 1 + \displaystyle\sum_{k=0}^{\lfloor n/8 \rfloor -2} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{0,2,3,4\}} 2^{8\lfloor n/8 \rfloor -i} & \text{if } n \equiv 1, 3 \bmod 8\,, \\ 1 + \displaystyle\sum_{k=0}^{\lfloor n/8 \rfloor -1} \left(\sum_{i \in \{4,5,7,8\}} 2^{8k+i} \right) + \sum_{i \in \{2,4\}} 2^{8\lfloor n/8 \rfloor +i} & \text{if } n \equiv 5, 7 \bmod 8\,. \end{cases}$$

It follows that $(e_3/s) \preceq e_2$, implying that $e_3 \in \mathcal{E}_{s,3}$. Finally, let

$$e_4 = 3 + \sum_{k=1}^{\lfloor n/4 \rfloor -1} \left(2^{4k-1} + 2^{4k} + 2^{4k+1} \right) + \sum_{k=2\lfloor n/4 \rfloor -1}^{(n-1)/2} 2^{2k}\,.$$

We have $e_4/s = 3 \times e_4 \bmod (2^n - 1)$ so

$$\begin{aligned}
e_4/s &= 3 \times \left(3 + \sum_{k=1}^{\lfloor n/4 \rfloor -1} \left(2^{4k-1} + 2^{4k} + 2^{4k+1} \right) + \sum_{k=2\lfloor n/4 \rfloor -1}^{(n-1)/2} 2^{2k} \right) \\
&= 9 + \sum_{k=1}^{\lfloor n/4 \rfloor -1} \left(2^{4k-1} + 2 \cdot 2^{4k} + 2 \cdot 2^{4k+1} + 2^{4k+2} \right) + \sum_{k=4\lfloor n/4 \rfloor -2}^{n} 2^{k} \\
&= 9 + \sum_{k=1}^{\lfloor n/4 \rfloor -1} \left(2^{4k-1} + 2^{4k+1} + 2^{4k+3} \right) + \sum_{k=4\lfloor n/4 \rfloor -2}^{n} 2^{k} \\
&= 1 + 2^4 + \sum_{k=1}^{\lfloor n/4 \rfloor -2} \left(2^{4k+1} + 2^{4k+4} \right) + 2^{4\lfloor n/4 \rfloor -3} + 2^{4\lfloor n/4 \rfloor -1} + \sum_{k=4\lfloor n/4 \rfloor -2}^{n} 2^{k} \\
&\equiv 1 + 2 + 2^4 + \sum_{k=1}^{\lfloor n/4 \rfloor -2} \left(2^{4k+1} + 2^{4k+4} \right) + 2^{4\lfloor n/4 \rfloor -3} + 2^{4\lfloor n/4 \rfloor -2} \\
&\equiv \sum_{k=0}^{\lfloor n/4 \rfloor -1} \left(2^{4k} + 2^{4k+1} \right) + 2^{4\lfloor n/4 \rfloor -2} \mod (2n - 1)\,.
\end{aligned}$$

As $(e_4/s) \preceq e_3$, we deduce that $e_4 \in \mathcal{E}_{s,4}$.

Finally, we have

$$\mathrm{wt}(e_4) = 2 + \left(\left\lfloor \frac{n}{4} \right\rfloor - 1\right) \times 3 + \left(\frac{n-1}{2} - 2\left\lfloor \frac{n}{4} \right\rfloor + 2\right) = \frac{n+1}{2} + \left\lfloor \frac{n}{4} \right\rfloor ,$$

implying that the algebraic degree of MiMC_3^{-1} at round 4 is at least $(n+1)/2 + \lfloor n/4 \rfloor$. □

Corollary 6.4. *The algebraic degree at round 4 for* MiMC_3^{-1} *satisfies:*

$$B_s^4 = \frac{n+1}{2} + \left\lfloor \frac{n}{4} \right\rfloor .$$

Proof. In Remark 6.5 we have seen that $\frac{n+1}{2} + \lfloor \frac{n}{4} \rfloor$ is an upper bound on the algebraic degree at round 4. Then, we have proved that there exists at least one exponent reaching this bound in Proposition 6.7. □

We have already seen in Section 5.4.1 that $B_s^1 = B_s^2 = (n+1)/2$. In this section we have also proved that

$$\begin{aligned} B_s^3 &\geqslant \frac{n+1}{2} + \left\lfloor \frac{n+1}{6} \right\rfloor = \left\lfloor \frac{2n+2}{3} \right\rfloor \\ B_s^4 &= \frac{n+1}{2} + \left\lfloor \frac{n-1}{4} \right\rfloor = \left\lfloor \frac{3n+1}{4} \right\rfloor \end{aligned}$$

However, as shown in Figure 6.31 this is not sufficient to provide precise guarantees on the algebraic degree. Experiments seem to indicate that the algebraic degree for the following rounds is close to

$$\begin{aligned} B_s^5 &\approx \frac{n+1}{2} + \left\lfloor \frac{5n-2}{16} \right\rfloor = \left\lfloor \frac{13n+6}{16} \right\rfloor \\ B_s^6 &\approx \frac{n+1}{2} + \left\lfloor \frac{6n-3}{16} \right\rfloor = \left\lfloor \frac{14n+5}{16} \right\rfloor \\ B_s^7 &\approx \frac{n+1}{2} + \left\lfloor \frac{7n-3}{18} \right\rfloor = \left\lfloor \frac{8n+3}{9} \right\rfloor \\ B_s^8 &\approx \frac{n+1}{2} + \left\lfloor \frac{7n-3}{18} \right\rfloor = \left\lfloor \frac{8n+3}{9} \right\rfloor \end{aligned}$$

but it seems difficult to find a pattern for such values.

As in the case of MiMC_3, it would also be interesting to determine all the maximum-weight exponents that are likely to appear. Figure 6.34 gives an overview of the number of maximum-weight exponents for different instances of MiMC_3^{-1}. It is worth noting that the behaviour differs with the size of the field.

6.5 Higher-Order Differential Attacks

In this section, we focus on attacks based on some algebraic properties of the cipher, most notably on higher-order differential attacks exploiting the algebraic degree of the primitive as explained in Section 1.3.2 of Chapter 1. MiMC_3 is the most studied instance and also the one for which we are able to give exact trails for a large number of rounds. Therefore, in this section, we will focus on higher-order differential attacks in the case of MiMC_3. Let $\mathcal{R} = \lceil \log_3 2^n \rceil$.

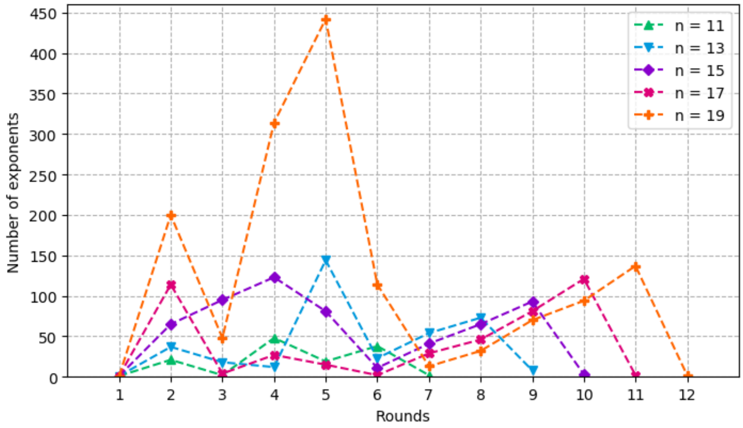


Figure 6.34: *Number of maximum-weight exponents of* MiMC_3^{-1}.

6.5.1 Secret-Key Zero-Sum Distinguisher

In Figure 6.35 we compare our upper bound on the algebraic degree computed in Proposition 5.10 with the bound by [Eic+20]. We see that we have a difference of one or two for the algebraic degree but more importantly we have seen in Section 6.1 that our bound is in fact the exact degree.

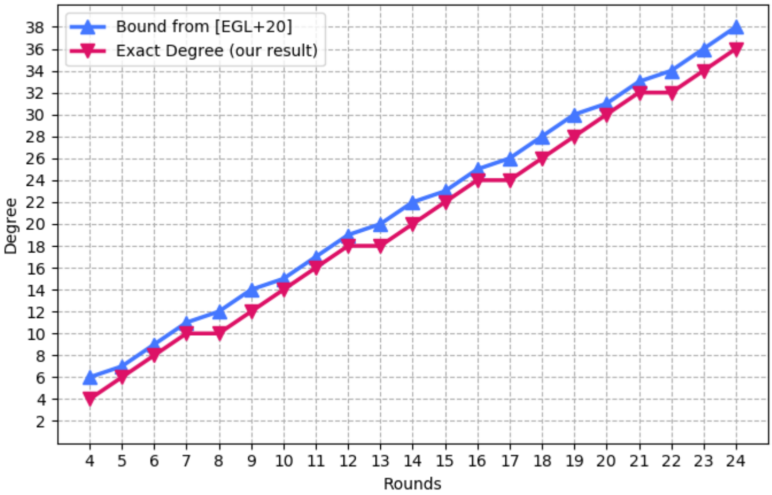


Figure 6.35: *Comparison with previous bound.*

It has been shown in [Eic+20, Prop. 2] that the maximal algebraic degree, which is $(n-1)$, can be reached for MiMC_3 and for its inverse MiMC_3^{-1} when $r \geqslant \lceil \log_3(2^{n-1}+1) \rceil$. In Proposition 6.8 we show that we can slightly improve this bound.

Proposition 6.8. *For any* $r < \mathcal{R} = \lceil \log_3 2^n \rceil$*, the algebraic degree of* MiMC_3 *is at most* $(n-3)$ *and the algebraic degree of* MiMC_3^{-1} *is at most* $(n-2)$.

Proof. We know from Proposition 5.10 that if the degree of r rounds of MiMC_3 is $(n-1)$ for some round constants, then

$$B_3^r = 2\left\lceil \frac{k_{3,r}}{2} - 1 \right\rceil \geqslant n - 1\,.$$

Then we have

$$\left\lceil \frac{k_{3,r}}{2} \right\rceil \geqslant \frac{n+1}{2}\,,$$

which implies that $k_{3,r} \geqslant n$, i.e., $\log_2 3^r \geqslant n$. It follows that, for $r < \lceil \log_3 2^n \rceil$, we have $\deg^a \mathsf{MiMC}_3[r] \leqslant (n-2)$. Using that the value of B_3^r, i.e. $2\lceil k_{3,r}/2 - 1\rceil$, is always even, we derive that

$$\forall\, r < \lceil \log_3 2^n \rceil, \quad \deg^a \mathsf{MiMC}_3[r] \leqslant (n-3)\,.$$

Moreover, as already observed in [BC13; Eic+20], a permutation of $\mathbb{F}_2^n$ has degree $(n-1)$ if and only if its inverse has degree $(n-1)$. Thus,

$$\forall\, r < \lceil \log_3 2^n \rceil, \quad \deg^a \mathsf{MiMC}_3^{-1}[r] \leqslant (n-2)\,.$$

□

Therefore, the number of rounds covered by a zero-sum distinguisher against MiMC_3 or MiMC_3^{-1} is slightly higher than predicted in [Eic+20]. Moreover, this distinguisher against MiMC_3 has data complexity at most 2^{n-2}, instead of 2^{n-1}. However this result only holds for MiMC_3 since for decryption there may be a plateau that is equal to $n-2$ in the last rounds (see Section 5.4.2). This corresponds to the following property. Let $f^r(x,k)$ be the function corresponding to r rounds of $\mathsf{MiMC}_3[r]$, and $\mathcal{V}$ be a subspace of $\mathbb{F}_{2^n}$, then:

$$\bigoplus_{x\in\mathcal{V},\dim(\mathcal{V})=n-2} f^{\mathcal{R}-1}(x,k) = 0\,, \quad \text{and} \quad \bigoplus_{x\in\mathcal{V},\dim(\mathcal{V})=n-1} f^{-(\mathcal{R}-1)}(x,k)\,.$$

As noted in [Eic+20], such a zero-sum distinguisher for $(r-1)$ rounds of MiMC_3^{-1} can be extended to a key-recovery attack over r rounds as described in Section 6.5.2

Another observation is that, in many cases, the data complexity of the distinguisher can be reduced to 2^{n-4} by removing the last round, as stated in the following proposition.

Proposition 6.9. *Let $\mathcal{R} = \lceil \log_3 2^n \rceil$. For any $r < \mathcal{R} - 1$, the algebraic degree of MiMC_3 is at most $(n-5)$, unless $k_{3,\mathcal{R}} = k_{3,\mathcal{R}-1}$ is even and $k_{3,\mathcal{R}-2}$ is odd (which equivalently means that there is a plateau between rounds $(\mathcal{R}-2)$ and $(\mathcal{R}-1)$).*

Proof. Let $b_{3,r} = k_{3,r} \bmod 2$. We recall that a plateau between rounds i and $(i+1)$ corresponds to the situation where $k_{3,i-1}$ is odd and $k_{3,i}$ even, i.e. $(b_{3,i-1}b_{3,i}) = (10)$ (see Corollary 6.3).

Let us investigate three situations.

(i) $(b_{3,\mathcal{R}-1}b_{3,\mathcal{R}}) = (10)$. In this case, there is a plateau between rounds $(\mathcal{R}-1)$ and $\mathcal{R}$ implying

$$B_3^{\mathcal{R}-1} = B_3^{\mathcal{R}} = n-1\,,$$

while we proved in Proposition 6.8 that $B_3^{\mathcal{R}-1} \leqslant n-3$.

(ii) $(b_{3,\mathcal{R}-1}b_{3,\mathcal{R}}) = (00)$. In this case, there is a plateau between rounds $(\mathcal{R}-2)$ and $(\mathcal{R}-1)$ if and only if $(b_{3,\mathcal{R}-2}b_{3,\mathcal{R}-1}) = (10)$.

(iii) $(b_{3,\mathcal{R}-1}b_{3,\mathcal{R}}) \in \{(01),(11)\}$. The only possibility corresponding to a plateau between rounds $(\mathcal{R}-2)$ and $(\mathcal{R}-1)$ is then $(b_{3,\mathcal{R}-2}b_{3,\mathcal{R}-1}b_{3,\mathcal{R}}) = (101)$, which is impossible because it would imply the existence of two consecutive switches in $(b_{3,r})_{r>0}$. i.e. $(s_{\mathcal{R}-1}s_{\mathcal{R}}) = (11)$, while we known from Proposition 6.2 that

$$s_{\mathcal{R}-1} + s_{\mathcal{R}} \in \{3 - k_{3,2}, 4 - k_{3,2}\} = \{0,1\} \; .$$

Therefore, Case (ii) is the only situation where we may have $B_3^{\mathcal{R}-2} = n-3$. In all other cases, $B_3^{\mathcal{R}-2} \leqslant n-5$. □

The complexity then depends on the position of the last plateau for encryption.

Example 6.5. For $n = 127$, we have $\mathcal{R} = 81$, and we can check from Table 6.14 that we are in a case where $B_3^{\mathcal{R}-2} = B_3^{\mathcal{R}-1} = n-3$. While [Eic+20] exhibits a distinguisher with data complexity 2^{125} for 78 rounds, we show that it actually covers 80 rounds. For $n = 129$, we have $\mathcal{R} = 82$, we can check from Table 6.14 that we are in a case where $B_3^{\mathcal{R}-3} = B_3^{\mathcal{R}-2} = n-5$. So we have a distinguisher of data complexity 2^{127} for 81 rounds (instead of 80 in [Eic+20]), and of data complexity 2^{125} for 80 rounds.

	r	77	78	79	80	81	82
[Eic+20]	$\lfloor \log_2(3^r+1) \rfloor$	122	123	125	126	128	129
our result	B_3^r	120	122	124	124	126	128

Table 6.14: *Bounds on the algebraic degree of* MiMC$_3$.

For $n = 129$, we compare our results with those of Eichlseder *et al.* [Eic+20] in Table 6.15, where we use the same notation: "KR" for Key-Recovery, "KK" for Known-Key distinguisher, and "SK" for Secret-Key distinguisher. We mark by a ⋆ the rows for which the complexity given are only valid for the encryption direction since we can use our precise bound to derive the complexity, while for the decryption direction, the bound remains too high, with a large plateau at $n-2$ in the last rounds. Overall, our careful study of the algebraic degree allows us to improve their attacks.

6.5.2 Key-recovery

Let us explain how the previously mentioned distinguisher can be used to attack $\mathcal{R}$ rounds of MiMC$_3$. This key-recovery attack was already proposed in [Eic+20], in this section we show how we can improve it using our results on the algebraic degree.

The idea is to recover the key with a chosen ciphertext attack. Let us consider ciphertexts in an $(n-1)$-dimensional subspace $\mathcal{V}+v$ of $\mathbb{F}_{2^n}$ and $\mathcal{W}$ the corresponding plaintexts, i.e. $\mathcal{W} = \text{MiMC}_3^{-1}(\mathcal{V}+v)$. From Proposition 6.8, we know that

$$F(k) = \bigoplus_{x \in \mathcal{W}} f(x,k) = 0 \; ,$$

where f denotes MiMC$_3$ round function, i.e.:

$$f(x) = (x \oplus k)^3 = k^3 \oplus k^2 \cdot x \oplus k \cdot x^2 \oplus x^3 \; .$$

Type	n	Rounds	Time	Data	Source
SK	129	80	2^{128}XOR	2^{128}	[Eic+20]
	n	$\lceil\log_3(2^{n-1}-1)\rceil-1$	2^{n-1}XOR	2^{n-1}	
	129	81	2^{128}XOR	2^{128}	Proposition 6.8
	n	$\lceil\log_3 2^n\rceil-1$	2^{n-1}XOR	2^{n-1}	
	129	81 $\star$	2^{127}XOR	2^{127}	Proposition 6.8
	n	$\lceil\log_3 2^n\rceil-1$ $\star$	2^{n-2}XOR	2^{n-2}	
	129	80 $\star$	2^{125}XOR	2^{125}	Proposition 6.9
	n	$\lceil\log_3 2^n\rceil-2$ $\star$	2^{n-2} or 2^{n-4}XOR	2^{n-2} or 2^{n-4}	
KK	129	160	-	2^{128}	[Eic+20]
	n	$2\cdot\lceil\log_3(2^{n-1}-1)\rceil-2$	-	2^{n-1}	
	129	162	-	2^{128}	Section 6.5.3
	n	$2\cdot\lceil\log_3 2^n\rceil-2$	-	2^{n-1}	
KR	129	82	$2^{122.64}$	2^{128}	[Eic+20]
	n	$\lceil n\cdot\log_3 2\rceil$	$2^{n-1-(\log_2\lceil n\log_3 2\rceil)}$ or $2^{n-(\log_2\lceil n\log_3 2\rceil)}$	2^{n-1}	
	129	82	$2^{121.64}$	2^{128}	Section 6.5.2
	n	$\lceil n\cdot\log_3 2\rceil$	$2^{n-1-(\log_2\lceil n\log_3 2\rceil)}$	2^{n-1}	

Table 6.15: Complexity of attacks on MiMC$_3$.

Then the key k can be recovered by solving this equation, i.e.:

$$\begin{aligned} F(k) &= \bigoplus_{x\in\mathcal{W}} (k^3 \oplus k^2\cdot x \oplus k\cdot x^2 \oplus x^3) \\ &= \left(k^2\cdot\bigoplus_{x\in\mathcal{W}} x\right) \oplus \left(k\cdot\bigoplus_{x\in\mathcal{W}} x^2\right) \oplus \left(\bigoplus_{x\in\mathcal{W}} x^3\right) \\ &= 0\,. \end{aligned}$$

This step is negligible because the polynomial has a low univariate degree in k.

6.5.3 Known-Key Zero-Sum Distinguisher

Using a subspace of dimension $n-1$, the number of rounds we can distinguish is $\mathcal{R}-1$ for both MiMC$_3$, and MiMC$_3^{-1}$. As a consequence, there is a known-key zero-sum distinguisher as defined in [AM09] on almost twice the number of rounds, starting from the middle of the primitive.

Such a known-key distinguisher can be applied to the hash function proposed in [Alb+16], based on the use of MiMC$_3$ within the sponge framework. We recall the construction of MiMCHash in Figure 6.36, where r is the rate and c the capacity.

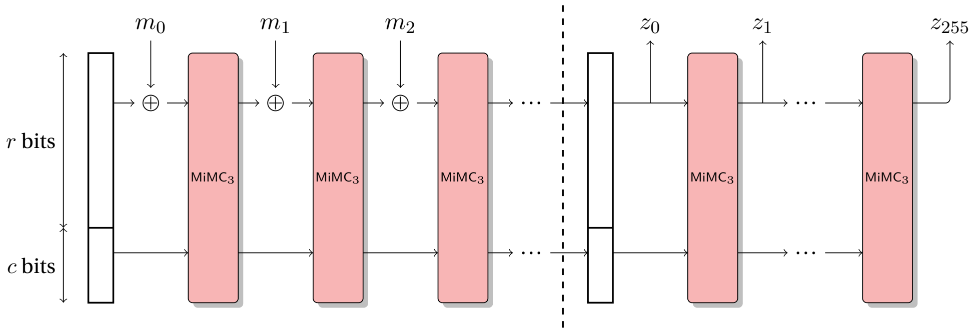


Figure 6.36: MiMC$_3$ *hash function in sponge framework.*

While there is a 0-sum distinguisher on $2\mathcal{R} - 2$ rounds when the dimension of the subspace $\mathcal{V}$ is $n - 1$, we are also interested in reducing the size of the subspace, in order to decrease the data complexity.

Example 6.6. First, let us consider the hash function using MiMC$_3$ with an extension degree $n = 1025$, which has $\mathcal{R} = 647$ rounds according to the designers' choice. In this case, the last plateau for MiMC$_3$ is between rounds $\mathcal{R} - 4$ and $\mathcal{R} - 3$, where the degree is equal to $n - 7$. Furthermore, for MiMC$_3^{-1}$, we know from Corollary 5.5 that $r_{n-2} \geqslant 324$, where r_{n-2} is the first round where the degree reaches $n - 2$. It follows that, if we operate on a subspace $\mathcal{V}$ of dimension $n - 2$, we would reduce by a quarter the number of rounds for which we can set up a distinguisher, as seen in Figure 6.37.

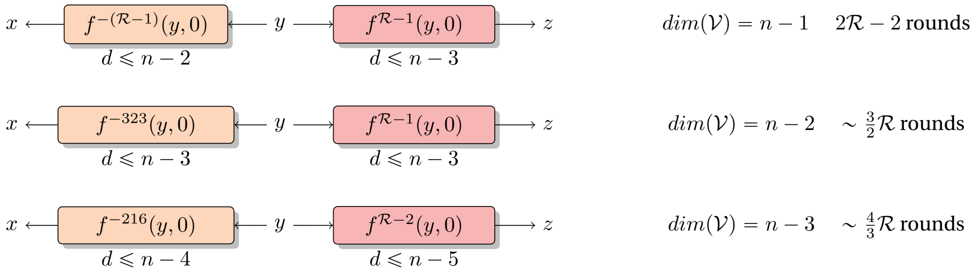


Figure 6.37: *0-sum against keyless permutation (with $n = 1025$).*

The other hash function uses MiMC$_3$ with an extension degree $n = 769$, and has 486 rounds. In this case, the first round where the degree reaches $n - 2$ is $r_{n-2} \geqslant 243$. However, the main difference is that the last plateau for MiMC$_3$ is between rounds $\mathcal{R} - 2$ and $\mathcal{R} - 1$, where the degree is equal to $n - 3$. But this has no impact on the fact that the attack covers much fewer rounds when we try to reduce the size of the subspace (see Figure 6.38).

Conclusion

In this chapter we have seen that the bound given in Chapter 5 on the algebraic degree of MiMC$_3$ is tight. Indeed, we managed to evaluate the exact algebraic degree of up to more than 16000 rounds by finding some families of exponents whose Hamming weight reaches the bound. While

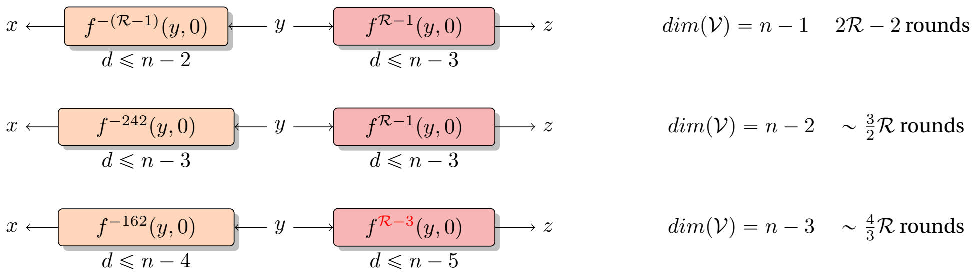


Figure 6.38: *0-sum against keyless permutation (with $n = 769$).*

finding only one maximum-weight exponent is sufficient to prove that the bound is tight, we aimed at exhibiting all of them for MiMC$_3$. Although we miss some of them for the general case, we managed to build large families of exponents for more than 400 rounds. Our procedure allowed us to give explicit trails to construct maximum-weight exponents by combining an inductive proof and a MILP-based algorithm to cover some few sporadic cases.

We also investigated other instances of MiMC$_d$ and gave some directions to find trails to construct maximum-weight exponents reaching the bounds given in Chapter 5. Moreover, we have found some trails allowing us to derive lower bounds for the algebraic degree at rounds 3 and 4 of the inverse transformation.

Finally, the tracing of exponents proposed in this chapter enables us to slightly improve the bound given in [Eic+20], so that we can save one or two rounds for the higher-order differential attacks proposed in their paper. Overall, we provide some precise guarantees on the minimal complexity for a higher-order differential attack for MiMC$_3$ and its inverse. Although our results focus on MiMC$_3$, we have also shown, in the previous chapter, that other natural exponents appear to have security risks.

CHAPTER 7

Other perspectives for the algebraic degree

In this chapter we push further the analysis of the algebraic degree of MiMC and we investigate different directions. More precisely, we aim at answering various open problems that are raised by the previous study of the algebraic degree in Chapters 5 and 6. Some of these questions have been answered and published at Crypto 2023 [Liu+23b], while other are still open, at the time of writing. However, we believe that it is worth proposing them as an invitation for future work in these different directions.

In Section 7.1 we study the growth of the algebraic degree in SPN constructions with an affine transformation. In particular, we use the so-called coefficient grouping strategy to study the algebraic degree of schemes like CHAGHRI or MiMC. We also provide another view of the sequence $(\lfloor r \log_2 d \rfloor)_{r>0}$ in Section 7.2. In particular, we try to better understand the link between the algebraic degree of MiMC$_d$ and the denominators of semi-convergents of $\log_2 d$. Finally, in Section 7.3, by seeing MiMC as a bivariate polynomial in the plaintext and the key, we suggest some directions to investigate the influence of the coefficients of the polynomials obtained by fixing either the plaintext or the key.

The results presented in this chapter, on the algebraic degree of SPN constructions with an affine transformation, have been obtained with Fukang Liu, Lorenzo Grassi, Willi Meier, and Takanori Isobe, and published in the proceedings of the conference *CRYPTO* in 2023 [Liu+23b].

Contents

7.1 Coefficient grouping for complex affine layer

In Chapters 5 and 6 we have studied the algebraic degree of iterated power functions, with a specific focus on MiMC$_3$. Now let us imagine that we have several of them in parallel in the nonlinear layer of an SPN construction. Then, the existence of families of missing exponents seems unlikely, or at least very difficult, to exhibit, because of the linear layer that creates diffusion. Indeed, this is what can be observed by constructing toy examples of SPN constructions composed of a multiplication by a matrix as a linear layer and of the cube as the non-linear layer. In this section, we will investigate, more generally, upper bounds on the algebraic degree of such SPN constructions. We will in particular study schemes inspired by the design of Chaghri and MiMC.

7.1.1 Definition and Main Theorem

First, let us give some notation and definitions of the coefficient grouping strategy.

7.1.1.1 Objectives

In this section, we consider SPN ciphers over $\mathbb{F}_{2^n}^m$ for $n \geqslant 3$ and $m \geqslant 1$ as illustrated in Figure 7.1. The SPN construction is composed of:

- an invertible S-box defined as the composition of a Gold function $S(x) = x^d$ where $d = 2^j + 1$, and of an $\mathbb{F}_2$-linearized affine polynomial $B(x) = c_0 + \sum_{i=1}^{w} c_i x^{2^{h_i}}$ where $c_1, \ldots, c_w \neq 0$. In the following, we will call B the affine layer and w its *density*,
- a linear transformation defined by a multiplication with an arbitrary invertible matrix $M \in \mathbb{F}_{2^n}^{m \times m}$, and
- the addition of a key and round constants that we represented by AddK and AddC on Figure 7.1.

Note also that, for the sake of consistency with Chapters 5 and 6, the notation we use differs from the original paper [Liu+23b].

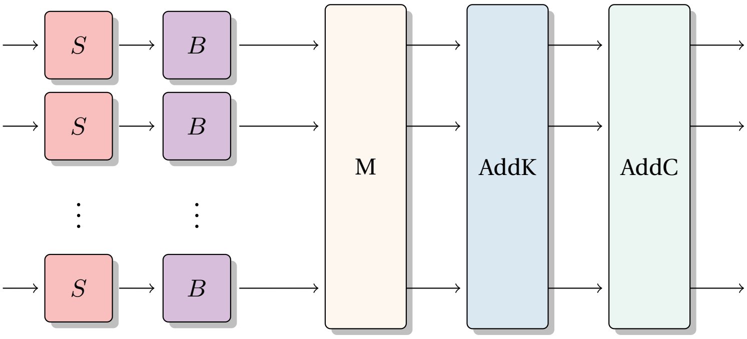


Figure 7.1: *The round function of SPN ciphers over* $\mathbb{F}_{2^n}^m$

Chaghri [AMT22] and MiMC [Alb+16], introduced in Chapter 1, are two examples of such a construction. MiMC is a special case where $m = 1$, $B(x) = x$ is the identity function and M is the identity matrix of size 1×1, i.e. $M = (1)$. The original version of Chaghri is a case where $m = 3$ and $B(x) = c_0 + c_1 x^{2^{h_1}}$. As already mentioned in Chapter 1, the version has been changed and B has been replaced by $B(x) = c_0 + \sum_{i=1}^{w} c_i 2^{h_i}$ with $w = 3$, but for convenience, in the following, Chaghri will always refer to the first version.

In this section we will investigate the algebraic degree of this construction, relying on the coefficient grouping strategy. As we will not give details of all the proofs, interested readers are invited to refer to the paper [Liu+23b]. Instead, we propose a discussion of the obtained results.

In particular, we will also study some tweaked version of MiMC_3 (see Figure 7.2) with an affine layer whose density is larger than one. Then we will be able to compare the results presented in this section with those given in Chapters 5 and 6 to analyze the influence of the affine layer on the growth of the algebraic degree.

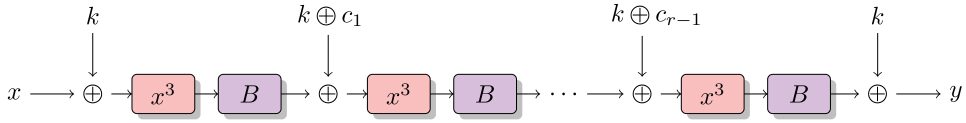


***Figure 7.2:** Tweaked version of* MiMC_3 *with an affine layer.*

The coefficient grouping technique was first introduced in [Liu+23a] and was particularly effective to break CHAGHRI. While this strategy is quite efficient when the density of the affine layer is $w = 1$, its performance and accuracy decrease when w increases.

The objective of this section is to answer various questions related to the study of the algebraic degree of SPN constructions with a complex affine layer. The general idea is to use a more efficient coefficient grouping technique to deeply analyze the set of all monomials that might appear in the polynomial representation of the internal state after any round. We will see that such a set is well-structured, and allows us to obtain the following results.

1. First, we will suggest some necessary conditions on the density w of the affine layer to ensure an exponential growth of the algebraic degree. In particular, we will prove that for $w = 1$ the algebraic degree never increases exponentially, and that for $w > 1$, the algebraic degree never increases exponentially after a certain number of rounds. This point will be addressed in Section 7.1.2.

2. Then, in Section 7.1.3, we will derive some equivalent affine layers, reducing the number of cases to study when searching for one that can achieve an exponential growth of the algebraic degree.

3. Finally, we will see, in Section 7.1.4, how the new modelisation allows us to determine concrete affine layers that can achieve the exponential growth, and provides an upper bound on the algebraic degree.

7.1.1.2 The coefficient grouping strategy

Let us introduce the original coefficient grouping technique proposed in [Liu+23a]. Suppose that $w = 1$, so that

$$B(x) = c_0 + c_1 x^{2^{h_1}} .$$

The coefficient grouping technique consists in finding a specific representation of the exponents in order to transform the problem of upper bounding the algebraic degree into an optimization problem that can be solved efficiently. Every exponent e is represented by:

$$e = \sum_{i=0}^{n-1} 2^i a_i, \quad \text{where } 0 \leqslant a_i \leqslant \nu_{r,i}, \text{ for } i \in [\![0, n-1]\!] ,$$

where the parameter $\nu_r = (\nu_{r,n-1}, \ldots, \nu_{r,0}) \in \mathbb{N}^n$ is computed with the following recursive relation:

$$\begin{cases} \nu_{0,0} = 1, \nu_{0,i} = 0, & \text{for } i \in [\![1, n-1]\!], \\ \nu_{j,i} = \nu_{j-1,(i-d-h_1) \bmod n} + \nu_{j-1,(i-h_1) \bmod n}, & \text{for } j \in [\![0, n-1]\!] . \end{cases}$$

It is proved in [Liu+23a] that computing an upper bound on the algebraic degree after r rounds is reduced to solving the following optimization problem:

$$\begin{aligned}
&\text{maximize wt}\left(M_n\left(\sum_{i=0}^{n-1} 2^i a_i\right)\right),\\
&\text{subject to } 0 \leqslant a_i \leqslant \nu_{r,i}, \text{ for } i \in [\![0, n-1]\!],
\end{aligned}$$

where M_n is defined as follows:

$$M_n = \begin{cases} 2^n - 1 & \text{if } (2^n-1)|x, \text{ and } x \geqslant 2^n - 1,\\ x \bmod (2^n - 1) & \text{otherwise.}\end{cases}$$

Based on this idea, we will introduce a new coefficient grouping technique for more complex affine layer. We will focus on the univariate case, but similar results can be obtained for the multivariate case.

In Chapters 5 and 6, we denoted by $\mathcal{E}_r$ the set of exponents likely to appear in the polynomial. Here the aim is also to give a representation of such a set. Since they are not computed with the same procedure, we will use a different but similar notation: $\mathscr{E}_r$. Note that in [Liu+23b] we use the notation $\mathcal{W}_r$. This set allows to compute the algebraic degree. Indeed, the algebraic degree is then the maximal Hamming weight of an integer in this set.

$$\deg^a = \max\left\{\text{wt}(M_n(e)), e \in \mathscr{E}_r\right\} \ .$$

Let us recall that some of the exponents in $\mathscr{E}_r$ might not necessarily appear for some particular values of the key and/or of the linear layer M. However, if an exponent is missing in this set, then we know that it does not appear in the polynomial, independently of the values of the key or of the linear layer M. This is sufficient to set up an upper bound on the algebraic degree, which is tight up to cancellations due to the key or to the linear layer M.

Let us denote by $\mathcal{P}_r$ the polynomial describing the transformation after each round. In particular, it would also help to have an intermediate representation of the polynomial. So we use $\mathcal{P}_r^S$ to denote the polynomial after the S-box layer. As a consequence $\mathscr{E}_r$ will represent the exponents in $\mathcal{P}_r$, and $\mathscr{E}_r^S$ the exponents in $\mathcal{P}_r^S$.

Based on such considerations, we have

$$\mathcal{P}_r(x) = (B \circ S)^r(\mathcal{P}_0(x)), \qquad \text{and} \qquad \mathcal{P}_r^S(x) = S(\mathcal{P}_{r-1}(x)).$$

Since CHAGHRI starts with the addition of a whitening key, let us consider $\mathcal{P}_0(x) = x + 1$. Then for the first round, after the S-box, the polynomial is:

$$\mathcal{P}_1^S(x) = (x+1)^{2^j+1} = x^{2^j+1} + x^{2^j} + x + 1\,,$$

implying that the only exponents that might appear in $\mathcal{P}_1^S$ are: $\left\{2^j + 1, 2^j, 1, 0\right\}$. Let us observe that we can represent this set by

$$\mathscr{E}_1^S = \left\{a_{1,1}2^j + a_{1,2} \mid 0 \leqslant a_{1,1}, a_{1,2} \leqslant 1\right\} \ .$$

Then after applying the affine layer, we get:

$$\mathcal{P}_1(x) = 1 + \sum_{i=1}^{w} \left(\mathcal{P}_1^S(x)\right)^{2^{h_i}} = 1 + \sum_{i=1}^{w}\left(x^{2^{j+h_i}} + x^{2^{j+h_i}+2^{h_i}} + x^{2^{h_i}}\right)\,,$$

implying that the exponents that might appear in $\mathcal{P}_1$ are of the form:

$$\begin{aligned}\mathscr{E}_1 &= \left\{2^{j+h_i}+2^{h_i}, 2^{j+h_i}, 2^{h_i}, 0\,,\ \text{where } 1 \leqslant i \leqslant w\right\}\\ &= \left\{a_{1,1}2^{j+h_i}+a_{1,2}2^{h_i}\ ,\ \text{where } 1 \leqslant i \leqslant w,\ \text{and } a_{1,1}, a_{1,2} \in \{0,1\}\right\}\end{aligned}$$

Now let us investigate the second round. After the S-box, we have:

$$\begin{aligned}\mathcal{P}_2^S(x) &= (\mathcal{P}_1(x))^{2^j+1}\\ &= \left(1+\sum_{i=1}^{w}\left(x^{2^{2j+h_i}}+x^{2^{2j+h_i}+2^{j+h_i}}+x^{2^{j+h_i}}\right)\right)\\ &\quad\times\left(1+\sum_{i=1}^{w}\left(x^{2^{j+h_i}}+x^{2^{j+h_i}+2^{h_i}}+x^{2^{h_i}}\right)\right)\,,\end{aligned}$$

implying that the exponents are of the form

$$\mathscr{E}_2^S = \left\{a_{2,1}2^{2j+h_{i_0}}+a_{2,2}2^{j+h_{i_0}}+a_{2,3}2^{j+h_{i_1}}+a_{2,4}2^{h_{i_1}}\right\}\,,$$

where $1 \leqslant i_0, i_1 \leqslant w$ and for all $i \in \{1,\dots,4\}$, $a_{2,i} \in \{0,1\}$. Then after the affine layer we get

$$\begin{aligned}\mathcal{P}_2(x) &= 1+\sum_{i=1}^{w}\left(\mathcal{P}_2^S(x)\right)^{2^{h_i}}\\ &= 1+\sum_{i_2=1}^{w}\left(\sum_{i_1=1}^{w}\sum_{i_0=1}^{w}x^{a_{2,1}2^{2j+h_{i_0}}+a_{2,2}2^{j+h_{i_0}}+a_{2,3}2^{j+h_{i_1}}+a_{2,4}2^{h_{i_1}}}\right)^{2^{h_{i_2}}}\,,\end{aligned}$$

implying that the exponents are of the form

$$\mathscr{E}_2 = \left\{a_{2,1}2^{2j+h_{i_0}+h_{i_2}}+a_{2,2}2^{j+h_{i_0}+h_{i_2}}+a_{2,3}2^{j+h_{i_1}+h_{i_2}}+a_{2,4}2^{h_{i_1}+h_{i_2}}\right\}\,,$$

where we have $1 \leqslant i_0, i_1, i_2 \leqslant w$ and for all $i \in \{1,\dots,4\}$, $a_{2,i} \in \{0,1\}$.

Working iteratively, our goal is to find similar sets of possible exponents that can appear in $\mathcal{P}_r^S(x)$. In the following, for $a \geqslant b$, we will use the notation:

$$\binom{a}{\leqslant b} = \begin{cases}\binom{a}{0}+\ldots+\binom{a}{b} & \text{if } b \geqslant 0\,,\\ 0 & \text{otherwise.}\end{cases}$$

Hence, we can deduce the following theorem.

Theorem 7.1. *For each $r \geqslant 1$, let $\mathcal{V}_{r,w}$ be the set defined as*

$$\mathcal{V}_{r,w} = \left\{e \in \mathbb{N} \mid e = \sum_{i=1}^{w} b_i h_i, \sum_{i=1}^{w} b_i = r-1, b_i \geqslant 0\right\}, \tag{7.1}$$

which represents all possible values by summing up $r-1$ elements from the set $\{h_1,\dots,h_w\}$. The set $\mathscr{E}_r^S$ can be described as follows:

$$\mathscr{E}_r^S = \left\{\sum_{i_0=0}^{r}\sum_{i_1=1}^{\binom{r}{i_0}} a_{r,v}2^{(r-i_0)d+f_v}, v = i_1+\binom{r}{\leqslant i_0-1}, 0 \leqslant a_{r,v} \leqslant 1, f_v \in \mathcal{V}_{r,w}\right\},$$

where

$$f_{\binom{r}{\leqslant i}+\ell} = f_{\binom{r}{\leqslant i}-\binom{r-1}{i}+\ell} \text{ for } 0 \leqslant i \leqslant r-1, 1 \leqslant \ell \leqslant \binom{r-1}{i}. \tag{7.2}$$

As already mentioned, in this thesis, we are interested in discussing the result we presented in [Liu+23b] and we do not aim at giving all details of the proof. Thus, in the following we will mainly discuss the consequences of using this representation of the exponents.

Remark 7.1. Based on Theorem 7.1, we can give a well-structured description of the monomials that will possibly appear after r rounds. Especially, from its current form, we immediately observe that the exponent of each possible monomial is a linear combination of $\sum_{i=0}^{r}\binom{r}{i} = 2^r$ numbers satisfying certain properties:

$$\begin{array}{ll}
i = 0 & 2^{rj+f_1}, \\
i = 1 & 2^{(r-1)j+f_{1+1}}, \dots, 2^{(r-1)j+f_{1+r}}, \\
 & \vdots \\
 & 2^{(r-i)j+f_{\binom{r}{\leqslant i-1}+1}}, \dots, 2^{(r-i)j+f_{\binom{r}{\leqslant i-1}+\binom{r}{i}}}, \\
 & \vdots \\
i = r & 2^{f_{2^r}}.
\end{array}$$

In the following, we show how to use this well-structured description to achieve our objectives, i.e. giving necessary conditions on the density of the affine layer to ensure an exponential growth of the algebraic degree, finding equivalent affine layers, determining concrete affine layers that achieve an exponential growth, and deriving an upper bound on the algebraic degree for any instance of an SPN construction with an affine layer.

In particular, we will capture the condition on the f_i by introducing a vector ν_r so that the exponents can be represented as:

$$\left\{ M_n(e), e = \sum_{i=0}^{n-1} 2^i a_i,\ 0 \leqslant a_i \leqslant \nu_{r,i}, \text{ for } 0 \leqslant i \leqslant n-1 \right\},$$

where M_n is defined by:

$$M_n = \begin{cases} 2^n - 1 & \text{if } (2^n-1)|x, \text{ and } x \geqslant 2^n - 1, \\ x \bmod (2^n - 1) & \text{otherwise.} \end{cases}$$

As in the previous coefficient grouping technique, proposed in [Liu+23a], those ν_r are the integers used in the modelisation of the optimization problem.

Theorem 7.2. *For each valid assignment of* $(f_1, \dots, f_{2^r})$*, the corresponding vector* $\nu_r = (\nu_{r,n-1}, \dots, \nu_{r,0})$ *satisfies the following property:*

$$\sum_{i=0}^{n-1} \nu_{r,i} = 2^r.$$

Especially, if there exist (i_1, v_1) *and* (i_2, v_2) *where* $i_1, i_2 \in [\![0, r]\!]$ *and* $v_1, v_2 \in [\![1, 2^r]\!]$ *such that* $(r - i_1) \times d + f_{v_1} = (r - i_2) \times d + f_{v_2}$*, there are at most* $2^r - 1$ *nonzero coordinates in the vector* ν_r*.*

Based on this property we will deduce some necessary conditions for the exponential growth of the algebraic degree.

7.1.2 Condition for the exponential growth of the degree

The first consequence of Theorem 7.1 is that it allows us to define necessary conditions for the exponential growth of the algebraic degree.

Theorem 7.3. *To ensure that the algebraic degree 2^r can be reached after r rounds, one necessary condition is that there exists a valid assignment of $(f_1, \ldots, f_{2^r})$ such that the following 2^r elements are all different:*

$$\begin{array}{ll} i=0 & (rj+f_1) \bmod n, \\ i=1 & ((r-1)j+f_{1+1}) \bmod n, \ldots, ((r-1)j+f_{1+r}) \bmod n, \\ \quad\vdots & \\ & \left((r-i)j+f_{\binom{r}{\leqslant i-1}+1}\right) \bmod n, \ldots, \left((r-i)j+f_{\binom{r}{\leqslant i-1}+\binom{r}{i}}\right) \bmod n, \\ \quad\vdots & \\ i=r & f_{2^r} \bmod n\,. \end{array}$$

This theorem implies, in particular, that for $i = \lceil r/2 \rceil$, the following $\binom{r}{i}$ integers must be distinct:

$$\left((r-i)j+f_{\binom{r}{\leqslant i-1}+1}\right) \bmod n, \ldots, \left((r-i)j+f_{\binom{r}{\leqslant i-1}+\binom{r}{i}}\right) \bmod n\,,$$

implying that the integers

$$\left(f_{\binom{r}{\leqslant i-1}+1}\right) \bmod n, \ldots, \left(f_{\binom{r}{\leqslant i-1}+\binom{r}{i}}\right) \bmod n$$

must be different. This observation leads to Corollary 7.1.

Corollary 7.1. *For a given $(h_1, \ldots, h_w)$, a necessary condition to ensure a possible exponential degree is*

$$|\mathcal{V}^R_{r,w}| \geqslant \binom{r}{\lceil \frac{r}{2} \rceil}$$

where

$$\mathcal{V}^R_{r,w} = \{e \bmod n, e \in \mathcal{V}_{r,w}\} = \left\{ e \bmod n, e = \sum_{i=1}^{w} b_i h_i, \sum_{i=1}^{w} b_i = r-1, b_i \geqslant 0 \right\}.$$

Let us observe that the set $\mathcal{V}^R_{r,w}$ involved in this corollary satisfies $|\mathcal{V}^R_{r,w}| \leqslant |\mathcal{V}_{r,w}|$ since some integers of $\mathcal{V}_{r,w}$ might have the same reduction modulo n.

In the following, it will be easier to develop reasoning in terms of partitions, so let us introduce a new set. We let $\mathcal{B}_{r,w}$ be the set of tuples $(b_1, \ldots, b_w)$ such that:

$$\mathcal{B}_{r,w} = \left\{ (b_1, \ldots, b_w), \sum_{i=1}^{w} b_i = r, b_i \geqslant 0 \right\}.$$

Noting that

$$|\mathcal{B}_{r-1,w}| \geqslant |\mathcal{V}_{r,w}| \geqslant |\mathcal{V}^R_{r,w}|\,,$$

the set $\mathcal{B}_{r,w}$ must also satisfy some condition in order to achieve an exponential growth.

Corollary 7.2. *A necessary condition for an exponential growth of the degree in the first r rounds is that*

$$|\mathcal{B}_{r-1,w}| \geqslant \binom{r}{\lceil \frac{r}{2} \rceil}.$$

Let us investigate the consequences of this corollary. First, let us notice that by definition of $\mathcal{B}_{r,w}$ we have

$$|\mathcal{B}_{1,w}| = |\,\{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots(0,\ldots,0,1)\}\,| = w\,.$$

Then, for the case $w = 1$, we have

$$|\mathcal{B}_{1,1}| = 1 < 2 = \binom{2}{1},$$

implying that it is impossible to achieve an exponential growth in that case.

Let us consider the case $w = 2$. First, we check that

$$|\mathcal{B}_{1,2}| = 2 \geqslant 2 = \binom{2}{1}.$$

For the second round, we have

$$|\mathcal{B}_{2,2}| = |\{(b_1,b_2) \mid b_1 + b_2 = 2\}| = |\{(0,2),(1,1),(2,0)\}| = 3 \geqslant 3 = \binom{3}{2}.$$

Then, for the third round, we have

$$|\mathcal{B}_{3,2}| = |\{(b_1,b_2) \mid b_1 + b_2 = 3\}| = |\{(0,3),(1,2),(2,1),(3,0)\}| = 4 < 6 = \binom{4}{2}.$$

This inequality implies that it is impossible to achieve an exponential algebraic degree at round 4 when $w = 2$.

In Table 7.1 we store all the values $|\mathcal{B}_{r,w}|$ for $w \in \{2,3,4\}$. Then we can also deduce that it is impossible to achieve an exponential algebraic degree at round 7 when $w = 3$ since, when computing the values $|\mathcal{B}_{r,3}|$, we observe the following

$$\begin{aligned}\forall i \leqslant 5, \quad & |\mathcal{B}_{i,3}| \geqslant \binom{i+1}{\lceil (i+1)/2 \rceil},\\ \text{but} \quad & |\mathcal{B}_{6,3}| < \binom{7}{4}.\end{aligned}$$

Similarly, when computing the values $|\mathcal{B}_{r,4}|$, we observe the following

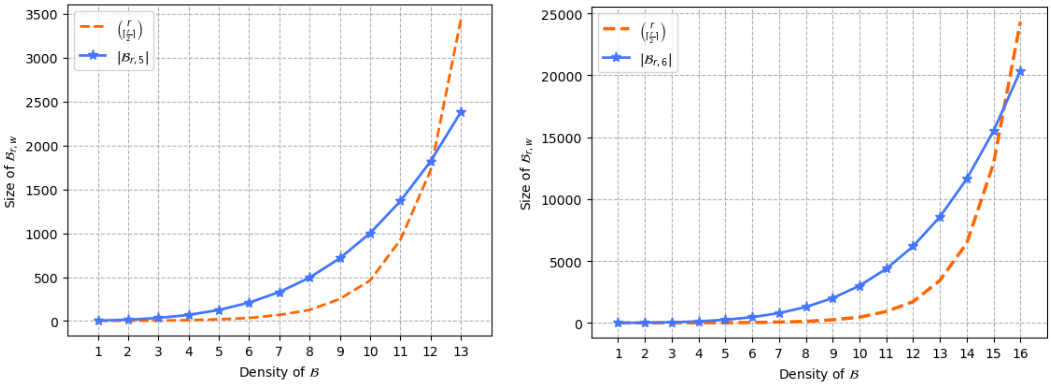
$$\begin{aligned}\forall i \leqslant 8, \quad & |\mathcal{B}_{i,4}| \geqslant \binom{i+1}{\lceil (i+1)/2 \rceil},\\ \text{but} \quad & |\mathcal{B}_{9,4}| < \binom{10}{5},\end{aligned}$$

implying that it is impossible to achieve an exponential algebraic degree at round 10 when $w = 4$.

While in [Liu+23b] we only suggest the implications of Corollary 7.2 for $w = 2, 3, 4$, we push the analysis a little further to investigate the situation for $w > 4$. These cases might be less relevant

r	1	2	3	4	5	6	7	8	9
$\binom{r+1}{\lceil (r+1)/2\rceil}$	2	3	6	10	20	35	70	126	252
$w = 2$	2	3	4	-	-	-	-	-	-
$w = 3$	3	6	10	15	21	28	-	-	-
$w = 4$	4	10	20	35	56	84	120	165	220

Table 7.1: *Comparison between the size of $\mathcal{B}_{r,w}$ and binomial coefficients.*



(a) *When $w = 5$.*

(b) *When $w = 6$*

Figure 7.3: *Evolution of the size of $\mathcal{B}_{r,w}$ compared to the one of binomial coefficients.*

as this implies a higher degree for the affine layer and for the SPN construction, and that the overall construction is maybe less efficient. However it is worth mentioning what happens for these cases. For the cases $w = 5$, and $w = 6$ we compare the evolution of $|\mathcal{B}_{r,w}|$ and $\binom{r+1}{\lceil (r+1)/2\rceil}$ in Figure 7.3a and 7.3b respectively. We observe that the first round for which it is impossible to achieve an exponential algebraic degree is round 13 when $w = 5$, and round 16 when $w = 6$.

We can also observe on these figures that for rounds 12 and 15, for the case $w = 5$ and $w = 6$, (respectively), the two lines are close, suggesting that although the necessary condition implies that an exponential degree is not impossible, it might still be unlikely to happen. Indeed, this is only a necessary but not sufficient condition.

While we did not consider the concrete values of the powers $h_1, \ldots, h_w$ in the affine layer, the above observations show that the density w of the affine layer has some influence on the growth of the algebraic degree. More precisely we saw that we are likely to achieve an exponential growth for at most the first 3, 6, 9, 12 and 15 rounds when w is equal to 2, 3, 4, 5 and 6 respectively.

7.1.3 Equivalent affine layer

In this section we see that there exist some equivalent affine layers that have the same influence on the algebraic degree. We suggest such equivalences in Corollary 7.3 and 7.4, and then study some examples.

Corollary 7.3. *Given an integer $\varepsilon \geqslant 0$, the following two affine layers have the same effect on the growth of the algebraic degree:*

$$B(x) = c_0 + \sum_{i=1}^{w} c_i x^{2^{h_i}}, \quad \text{and} \quad B'(x) = c'_0 + \sum_{i=1}^{w} c'_i x^{2^{h'_i}},$$

where $h'_i \equiv (h_i + \varepsilon) \bmod n$ for $i \in [\![1, w]\!]$.

Corollary 7.4. *The following two affine layers have the same effect on the growth of the algebraic degree:*

$$B(x) = c_0 + \sum_{i=1}^{w} c_i x^{2^{h_i}}, \quad \text{and} \quad B'(x) = c'_0 + \sum_{i=1}^{w} c'_i x^{2^{h'_i}},$$

where $(h_{i+1} - h_i) \equiv (h'_{i+1} - h'_i) \bmod n$ for $i \in [\![1, w-1]\!]$.

As, in this thesis, we mainly discussed on the algebraic degree of the MiMC bloc cipher, let us see some examples of such an equivalence for tweaked version of MiMC when the density of the affine layer is $w = 2$ or $w = 3$.

Example 7.1 (when $w = 2$). We let $B^{(i_0,i_1)}$ be some affine layers such that

$$\begin{aligned}
B^{(0,1)}(x) &= c_0^{(0,1)} + c_1^{(0,1)} x + c_2^{(0,1)} x^2 , \\
B^{(0,2)}(x) &= c_0^{(0,2)} + c_1^{(0,2)} x + c_2^{(0,2)} x^4 , \\
B^{(0,3)}(x) &= c_0^{(0,3)} + c_1^{(0,3)} x + c_2^{(0,3)} x^8 , \\
B^{(1,2)}(x) &= c_0^{(1,2)} + c_1^{(1,2)} x^2 + c_2^{(1,2)} x^4 .
\end{aligned}$$

Then, we denote by $\mathsf{MiMC}_3^{(0,1)}$, $\mathsf{MiMC}_3^{(0,2)}$, $\mathsf{MiMC}_3^{(0,3)}$ and $\mathsf{MiMC}_3^{(1,2)}$ the tweaked MiMC_3 instances with the affine layers $B^{(0,1)}$, $B^{(0,2)}$, $B^{(0,3)}$ and $B^{(1,2)}$ respectively. In Table 7.2 we compare the degrees that we obtained with the different instances. Our experiments consist in constructing explicitly the polynomial using a Sage implementation. We note that $B^{(0,1)}$ and $B^{(1,2)}$ are equivalent according to Corollary 7.4 and so have the same influence on the algebraic degree.

r	1	2	3	4
MiMC_3 (original)	2	2	4	4
$\mathsf{MiMC}_3^{(0,1)}$ / $\mathsf{MiMC}_3^{(1,2)}$	2	4	6	8
$\mathsf{MiMC}_3^{(0,2)}$	2	4	6	10
$\mathsf{MiMC}_3^{(0,3)}$	2	4	8	12

Table 7.2: *Degrees of tweaked instances of MiMC_3 when $w = 2$.*

We notice that the algebraic degree in exponential in the first two rounds only, for all instances, except $\mathsf{MiMC}_3^{(0,3)}$ that can achieve it until round 3. Let us recall that, since $w = 2$, the exponential increase cannot be achieved for more than three rounds.

Example 7.2 (when $w = 3$)**.** We let $B^{(i_0,i_1,i_2)}$ be some affine layers such that

$$\begin{aligned}
B^{(0,1,2)}(x) &= c_0^{(0,1,2)} + c_1^{(0,1,2)}x + c_2^{(0,1,2)}x^2 + c_3^{(0,1,2)}x^4 \,, \\
B^{(0,1,3)}(x) &= c_0^{(0,1,3)} + c_1^{(0,1,3)}x + c_2^{(0,1,3)}x^2 + c_3^{(0,1,3)}x^4 \,, \\
B^{(1,2,3)}(x) &= c_0^{(1,2,3)} + c_1^{(1,2,3)}x + c_2^{(1,2,3)}x^2 + c_3^{(1,2,3)}x^4 \,.
\end{aligned}$$

As in the previous example, $\mathsf{MiMC}_3^{(0,1,2)}$, $\mathsf{MiMC}_3^{(0,1,3)}$ and $\mathsf{MiMC}_3^{(1,2,3)}$ are the tweaked MiMC_3 instances with the affine layers $B^{(0,1,2)}$, $B^{(0,1,3)}$ and $B^{(1,2,3)}$ respectively. In Table 7.3 we compare the degrees that we obtained with the different instances. We also note that $B^{(0,1,2)}$ and $B^{(1,2,3)}$ lead to the same algebraic degree since they are equivalent according to Corollary 7.4.

r	1	2	3	4
MiMC_3 (original)	2	2	4	4
$\mathsf{MiMC}_3^{(0,1,2)}$ / $\mathsf{MiMC}_3^{(1,2,3)}$	2	4	8	10
$\mathsf{MiMC}_3^{(0,1,3)}$	2	4	8	14

Table 7.3: Degrees of tweaked instances of MiMC_3 *when* $w = 3$.

Let us observe that, for all the examples, the exponential growth is achieved only for the first three rounds, while the previous necessary conditions suggest that it may happen until round 6.

7.1.4 Practical tests

In this section, we discuss the results obtained by our new coefficient grouping technique to determine bound on the algebraic degree and which consists in solving the following optimization problem:

$$\begin{aligned}
&\text{maximize } \mathrm{wt}\left(M_n\left(\sum_{i=0}^{n-1} 2^i a_i\right)\right), \\
&\text{subject to } 0 \leqslant \nu_{r,i};\ \sum_{i=0}^{n-1} \nu_{r,i} = 2^r;\ |\{i \mid \nu_{r,i} \neq 0\}| \leqslant \pi;\ \{i \mid \nu_{r,i} \neq 0\} \subseteq \mathcal{Z}\,.
\end{aligned}$$

where π has to hold to ensure an exponential algebraic degree, the set $\mathcal{Z}$ stores all possible numbers that can be chosen for the 2^r elements in the $r+1$ classes as defined in Remark 7.1, and M_n is defined as follows:

$$M_n = \begin{cases} 2^n - 1 & \text{if } (2^n-1)|x, \ \text{ and } x \geqslant 2^n - 1, \\ x \bmod (2^n - 1) & \text{otherwise.} \end{cases}$$

We do not describe the precise modeling of this technique since this is not the scope of this thesis, but more details on the construction of π and $\mathcal{Z}$ can be found in our paper [Liu+23b].

Our aim is to find proper $(h_1, \ldots, h_w)$ such that an SPN construction can achieve an exponential growth for the algebraic degree, for any specified (n, j) with small w. Then we are also interested in upper bounding the algebraic degree for any given instance.

7.1.4.1 Finding good affine layers

The modelisation to find good affine layers consists in efficiently checking the condition of Theorem 7.3.

The case $(n, j) = (63, 32)$, with $m = 3$.

For instance, when $(n, j) = (63, 32)$, which is the parameter used in Chaghri, according to Corollary 7.2, $w \geqslant 3$ has to hold to ensure the exponential growth. Indeed $62 \approx 2^6$, implying that the smallest density w that satisfies the necessary condition for an exponential growth in the first six rounds is $w = 3$. With our new technique, we found 80 solutions of (h_1, h_2, h_3) up to equivalence relations that can achieve an exponential degree at round 6. We list them in Table 7.4.

h_2	(h_1, h_2, h_3)
2	$(0,2,9), (0,2,14), (0,2,20), (0,2,22), (0,2,24), (0,2,25), (0,2,26), (0,2,27),$ $(0,2,38), (0,2,39), (0,2,40), (0,2,41), (0,2,43), (0,2,45), (0,2,51), (0,2,56)$
3	$(0,3,27), (0,3,39)$
4	$(0,4,10), (0,4,17), (0,4,26), (0,4,29), (0,4,38), (0,4,41), (0,4,50), (0,4,57)$
5	$(0,5,19), (0,5,24), (0,5,28), (0,5,40), (0,5,44), (0,5,49)$
6	$(0,6,14), (0,6,15), (0,6,54), (0,6,55)$
7	$(0,7,22), (0,7,27), (0,7,34), (0,7,36), (0,7,43), (0,7,48)$
8	$(0,8,18), (0,8,26), (0,8,45), (0,8,53)$
9	$(0,9,26), (0,9,28), (0,9,34), (0,9,35), (0,9,37), (0,9,38), (0,9,44), (0,9,46)$
10	$(0,10,23), (0,10,25), (0,10,27), (0,10,28), (0,10,29), (0,10,44), (0,10,45),$ $(0,10,46), (0,10,48), (0,10,50)$
11	$(0,11,29), (0,11,34), (0,11,36), (0,11,38), (0,11,40), (0,11,45)$
12	$(0,12,26), (0,12,30)$

Table 7.4: *List of choices of (h_1, h_2, h_3) for $(n, j) = (63, 32)$.*

It is worth noting that the recommended parameters $(h_1, h_2, h_3) = (0, 2, 8)$ chosen to patch Chaghri in [AMT22] is not included, raising the question of the relevance of this choice. Indeed, with the technique that will be described in Section 7.1.4.2, although the upper bound for the algebraic degree in round 6 is 62 for $(n, j, h_1, h_2, h_3) = (63, 32, 0, 2, 8)$, this bound is possibly a loose one and we cannot conclude for sure whether the maximal algebraic degree will be reached at round 6.

The case $(n, j) = (129, 1)$, with $m = 3$.

Let us now consider the case $(n, j) = (129, 1)$, which corresponds to the parameters used in MiMC$_3$. According to Corollary 7.2, to ensure the exponential growth, $w \geqslant 4$ has to hold, since $128 = 2^7$ and the smallest density w that satisfies the necessary condition for an exponential degree in the first seven rounds is $w = 4$.

There are lots of solutions (h_1, h_2, h_3, h_4) that may reach this goal. We list some of them in Table 7.5.

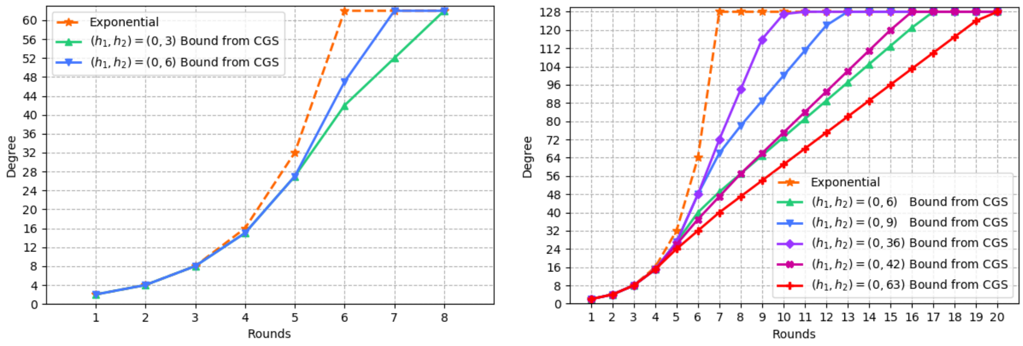
h_3	(h_1, h_2, h_3, h_4)
6	$(0,1,6,54), (0,1,6,55), (0,1,6,56), (0,1,6,79), (0,1,6,80), (0,1,6,81)$
7	$(0,1,7,27), (0,1,7,28), (0,1,7,29), (0,1,7,34), (0,1,7,35), (0,1,7,36),$ $(0,1,7,40), (0,1,7,41), (0,1,7,54), (0,1,7,55), (0,1,7,56), (0,1,7,57),$ $(0,1,7,79), (0,1,7,80), (0,1,7,81), (0,1,7,82), (0,1,7,95), (0,1,7,100),$ $(0,1,7,101), (0,1,7,102), (0,1,7,103), (0,1,7,107), (0,1,7,108), (0,1,7,109)$
8	$(0,1,8,28), (0,1,8,29)$

Table 7.5: *List of some choices of* (h_1, h_2, h_3, h_4) *for* $(n, j) = (129, 1)$.

7.1.4.2 Upper bound on the algebraic degree

Upper-bounding the algebraic degree requires to enumerate all $(f_1, \dots f_{2^r})$ and the corresponding $\nu_r = (\nu_{r,n-1}, \dots, \nu_{r,0})$. Such an enumeration is time-costly. Therefore, some properties can be captured from ν_r to reduce the optimization problem into an equivalent one. For instance, one property is that the sum of all $\nu_{r,i}$ must be equal to 2^r. Although this relaxes the original condition (since more ν_r can be found satisfying this property than those found by an exhaustive enumeration) this reduction simplifies computations.

One interesting experiment consists in studying how the algebraic degree increases in the univariate setting when $w = 2$. We tried some (h_1, h_2) for some fixed parameters (n, j). In the previous sections we saw that such instances of the SPN construction do not allow the algebraic degree to achieve an exponential increase for more than three rounds. However it is worth observing how far the upper bound is from the exponential increase. Figure 7.4a shows the results obtained when $(n, j) = (63, 32)$, that can also be seen as a tweaked version of Chaghri, and Figure 7.4b shows the results obtained when $(n, j) = (129, 1)$, that can also be seen as a tweaked version of MiMC for different values of (h_1, h_2). In the figures we denote the Coefficient Grouping Strategy by "CGS".

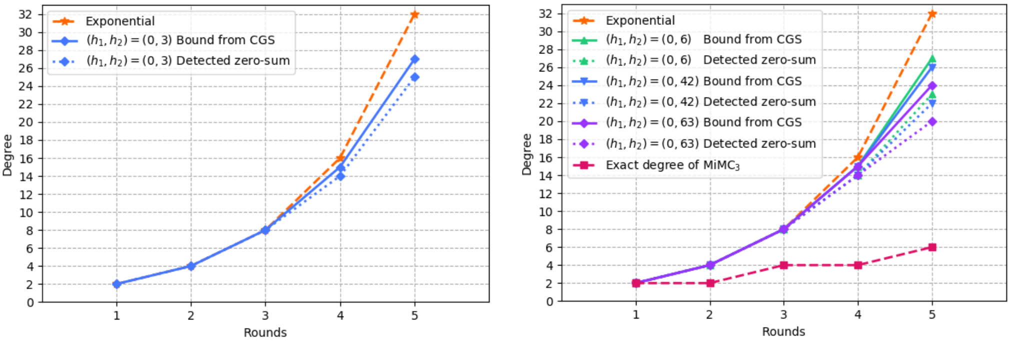


(a) *When* $(n, j) = (63, 32)$ *and* $m = 3$. ***(b)*** *When* $(n, j) = (129, 1)$ *and* $m = 3$.

Figure 7.4: *Upper-bounds on the algebraic degree.*

It is quite surprising to see, for example, that for $(h_1, h_2) = (0, 63)$ when $(n, j) = (129, 1)$, the algebraic degree increases linearly. Thus, a more fine grained interpretation should be developed to understand this behaviour. We leave it as an interesting problem.

The reduced well-structured optimization problems are solved via blackbox solvers. To investigate the efficiency of the technique we compare, in Figure 7.5, the bound given with the coefficient grouping technique and the estimation given by zero-sum. The strategy of zero-sum consists in choosing subspaces of dimension $\dim$, and then test whether the corresponding sums of the outputs are zero. We thus deduce that the algebraic degree is likely to be $\dim - 1$ for the smallest $\dim$ that can make the sums of the outputs equal to zero. Computing such zero-sums is expensive so we only compare the two results for the first five rounds of some instances. We observe that our upper bound is tight in the first three rounds and becomes less accurate in rounds 4 and 5, which is expected due to the relaxed conditions. Then, it is meaningful to develop efficient algorithms to further understand the efficiency of the new technique.



(a) *When $(n, j) = (63, 32)$ and $m = 3$.*

(b) *When $(n, j) = (129, 1)$ and $m = 3$.*

Figure 7.5: *Comparison with estimated degree estimated with zero-sums.*

In Figure 7.5b, we also added a comparison with the exact degree found for MiMC$_3$, operating on $(3n)$ bits, in Chapter 6. This clearly reveals the influence of the addition of an affine layer in the construction.

Overall, we observe that the model used to evaluate the upper bound on the algebraic degree for arbitrary B is not perfect since we use relaxed constraints. It would be interesting to see if it is possible to take into account more precise properties to get a finest bound without too much affecting the efficiency of the model.

7.2 Open problems on the sequences $k_{3,r}$

This section focuses on another unrelated open problem on the algebraic degree. When studying the algebraic degree of MiMC$_d$ in Chapters 5 and 6, the sequences $k_{d,r} = \lfloor r \log_2 d \rfloor$ played a crucial role. In this section, we propose to study them from a different point of view. Indeed, a better understanding of the behaviour of these sequences might enable us to obtain proofs for some observations from previous chapters. Let us recall that the sequence $(k_{d,r})_{r \geqslant 1}$ is highly related to the sequence $(b_{d,r})_{r \geqslant 1}$ where, if $d = 2^j + 1$ then $b_{d,r} = k_{d,r} \bmod 2j$, and if $d = 2^j - 1$ then $b_{d,r} = k_{d,r} \bmod j$.

Throughout this section, our method will be the same and will consist in starting from a round r for which $b_{d,r}$ is given by b, and then going back some rounds before to find out which sub-sequences of $(b_{d,r-i})_{1\leqslant i<r}$ made it possible to get $b_{d,r}$ at round r.

7.2.1 Sequences $b_{3,r}$

In this section, we first investigate the behaviours of sequences $(k_{3,r})_{r\geqslant 1}$ and $(b_{3,r})_{r\geqslant 1}$. In particular, we try to better understand the link with the denominators of semi-convergents of $\log_2 3$ that we briefly mentioned in Chapter 6. To this end, we will trace the precise evolution of the sequence $(b_{3,r})_{r\geqslant 1}$.

Let us suppose that round r is such that $b_{3,r} = 0$, then going back one round before, we have either $b_{3,r-1} = 1$ or $b_{3,r-1} = 0$. However, going back two rounds before, we can identify an impossible sequence. Indeed, if $b_{3,r-1} = 1$ we necessarily have $b_{3,r-2} = 1$, meaning that it is not possible to find r such that $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (010)$. The same holds for the sequence $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (101)$. Such an impossible sequence is precisely what we will be looking at in this section.

We will use the following notation.

- We will use the overline to denote the complementary of a binary value
- $\mathcal{B}_2 = (\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b}^3\overline{\mathsf{b}}^2\mathsf{b}^3)$ will denote sequences with two patterns b^3,
- $\mathcal{B}_3 = (\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b}^3\overline{\mathsf{b}}^2\mathsf{b}^3\overline{\mathsf{b}}^2\mathsf{b}^3) = \left(\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b}\mathcal{B}_2\right)$, sequences with three patterns b^3,
- $\mathscr{B}_2 = (\mathcal{B}_2\overline{\mathcal{B}_2}\mathcal{B}_3)$, sequences with two patterns $\mathcal{B}_2$, and
- $\mathscr{B}_3 = (\overline{\mathcal{B}_2}\mathcal{B}_2\overline{\mathcal{B}_2}\mathcal{B}_3) = \left(\overline{\mathcal{B}_2}\mathscr{B}_2\right)$, sequences with three patterns $\mathcal{B}_2$.

The sequences $\mathcal{B}_2, \mathcal{B}_3, \mathscr{B}_2$ and $\mathscr{B}_2$ are constructed such that there exist some particular properties for the sequences $(k_{3,r})_{r\geqslant 1}$.

Lemma 7.1. *Let $(k_{3,r})_{r\geqslant 1}$ and $(b_{3,r})_{r\geqslant 1}$ be the sequences defined by $k_{3,r} = \lfloor r\log_2 3\rfloor$ and $b_{3,r} = k_{3,r} \bmod 2$.*

(i) *If $(b_{3,r-11}\dots b_{3,r}) = \mathcal{B}_2$ then $k_{3,r} = k_{3,r-11} + 18$.*

(ii) *If $(b_{3,r-16}\dots b_{3,r}) = \mathcal{B}_3$ then $k_{3,r} = k_{3,r-16} + 26$.*

(iii) *If $(b_{3,r-40}\dots b_{3,r}) = \mathscr{B}_2$ then $k_{3,r} = k_{3,r-40} + 64$.*

(iv) *If $(b_{3,r-52}\dots b_{3,r}) = \mathscr{B}_3$ then $k_{3,r} = k_{3,r-52} + 83$.*

Proof. In the proof we rely on the fact that, as proved in Proposition 6.1, if $(b_{3,r-1}b_{3,r}) = (\overline{\mathsf{b}}\mathsf{b})$ then $k_{3,r-1} = k_{3,r} + 1$, while if $(b_{3,r-1}b_{3,r}) = (\mathsf{b}^2)$ then $k_{3,r-1} = k_{3,r} + 2$. It follows that if $(b_{3,r-\ell+1}\dots b_{3,r})$ corresponds to a sequence of the form $(\mathsf{b}^{\ell_0}\overline{\mathsf{b}^{\ell_1}}\mathsf{b}^{\ell_2}\dots\overline{\mathsf{b}^{\ell_{K-2}}}\mathsf{b}^{\ell_{K-1}})$ then

$$k_{3,r} - k_{3,r-\ell+1} = \sum_{i=0}^{K-1}(2\ell_i - 1) - 1 = 2\ell - K - 1\,.$$

(i) If $(b_{3,r-11}\dots b_{3,r}) = \mathcal{B}_2 = (\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b}^3\overline{\mathsf{b}}^2\mathsf{b}^3)$, then since $\mathcal{B}_2$ is a sequence of length 12 with 5 blocks, we have:

$$k_{3,r} = k_{3,r-11} + 2\times 12 - 5 - 1 = k_{3,r-11} + 18\,.$$

(ii) If $(b_{3,r-16}\dots b_{3,r}) = \mathcal{B}_3 = \left(\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b}\mathcal{B}_2\right)$, then we can check that

$$k_{3,r} = k_{3,r-16} + 6 + 2 + 18 = k_{3,r-16} + 26\,.$$

(iii) If $(b_{3,r-40}\dots b_{3,r}) = \mathscr{B}_2 = (\mathcal{B}_2\overline{\mathcal{B}_2}\mathcal{B}_3)$, then we can check that

$$k_{3,r} = k_{3,r-40} + 18 + 1 + 18 + 26 = k_{3,r-40} + 64\,.$$

(iv) If $(b_{3,r-52}\dots b_{3,r}) = \mathscr{B}_3 = \left(\overline{\mathcal{B}_2}\mathscr{B}_2\right)$, then we can check that

$$k_{3,r} = k_{3,r-52} + 18 + 1 + 64 = k_{3,r-52} + 83\,.$$

□

Then, using this lemma we now establish that some sub-sequences cannot appear in $\{b_{3,r}\}_{r\geqslant 0}$.

Lemma 7.2. *Let* $(k_{3,r})_{r>0}$ *and* $(b_{3,r})_{r>0}$ *be the sequences defined by* $k_{3,r} = \lfloor r\log_2 3\rfloor$ *and* $b_{3,r} = k_{3,r} \bmod 2$. *Then, for any* $r \geqslant 1$, *and* $\mathsf{b} \in \mathbb{F}_2$ *none of the following situations can occur:*

(i) $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (\mathsf{b}\overline{\mathsf{b}}\mathsf{b})$,

(ii) $(b_{3,r-3}\dots b_{3,r}) = (\mathsf{b}^4)$,

(iii) $(b_{3,r-5}\dots b_{3,r}) = (\overline{\mathsf{b}}^3\mathsf{b}^3)$,

(iv) $(b_{3,r-7}\dots b_{3,r}) = (\mathsf{b}\overline{\mathsf{b}}^2\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$,

(v) $(b_{3,r-17}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_3)$,

(vi) $(b_{3,r-29}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathcal{B}_3})$,

(vii) $(b_{3,r-41}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathcal{B}_2}\mathcal{B}_3)$,

(viii) $(b_{3,r-53}\dots b_{3,r}) = (\overline{\mathsf{b}}\mathcal{B}_2\overline{\mathcal{B}_2}\mathcal{B}_2\overline{\mathcal{B}_2}\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$,

(ix) $(b_{3,r-94}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathscr{B}_2}\mathscr{B}_2)$,

(x) $(b_{3,r-306}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathscr{B}_2\mathscr{B}_3^4}\mathscr{B}_2)$,

(xi) $(b_{3,r-359}\dots b_{3,r}) = (\mathsf{b}\mathscr{B}_3^6\overline{\mathcal{B}_2}\mathcal{B}_2\overline{\mathcal{B}_2}\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$,

(xii) $(b_{3,r-665}\dots b_{3,r}) = (\overline{\mathsf{b}}\overline{\mathscr{B}_3^6}\mathscr{B}_2\mathscr{B}_3^5\overline{\mathcal{B}_2}\mathcal{B}_2\overline{\mathcal{B}_2}\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$,

(xiii) $(b_{3,r-971}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathscr{B}_2\mathscr{B}_3^5}\mathscr{B}_2\mathscr{B}_3^5\overline{\mathscr{B}_2\mathscr{B}_3^5}\mathscr{B}_2)$.

Proof. In this proof, we will use that:

$$\forall r, i, \quad k_{3,r-i} + \lfloor i\log_2 3\rfloor \leqslant k_{3,r} \leqslant k_{3,r-i} + \lfloor i\log_2 3\rfloor + 1\,.$$

Recall that $\log_2 3 \approx 1.585$, then we can derive the following contradictions:

(i) $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (\mathsf{b}\overline{\mathsf{b}}\mathsf{b})$ implies

$$k_{3,r} = k_{3,r-2} + 1 + 1 = k_{3,r-2} + 2\,,$$

so that

$$k_{3,r} \geqslant k_{3,r-2} + \lfloor 2\log_2 3 \rfloor = k_{3,r-2} + 3 > k_{3,r-2} + 2\,.$$

(ii) $(b_{3,r-3}\dots b_{3,r}) = (\mathsf{b}^4)$ implies

$$k_{3,r} = k_{3,r-3} + 2 \times 3 = k_{3,r-3} + 6\,,$$

so that

$$k_{3,r} \leqslant k_{3,r-3} + \lfloor 3\log_2 3 \rfloor + 1 = k_{3,r-3} + 5 < k_{3,r-3} + 6\,.$$

(iii) $(b_{3,r-5}\dots b_{3,r}) = (\overline{\mathsf{b}}^3\mathsf{b}^3)$ implies

$$k_{3,r} = k_{3,r-5} + 2 \times 2 + 1 + 2 \times 2 = k_{3,r-5} + 9\,,$$

so that

$$k_{3,r} \leqslant k_{3,r-5} + \lfloor 5\log_2 3 \rfloor + 1 = k_{3,r-5} + 8 < k_{3,r-9} + 9\,.$$

(iv) $(b_{3,r-7}\dots b_{3,r}) = (\mathsf{b}\overline{\mathsf{b}}^2\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$ implies

$$k_{3,r} = k_{3,r-7} + 1 + (2+1) \times 3 = k_{3,r-7} + 10\,,$$

so that

$$k_{3,r} \geqslant k_{3,r-7} + \lfloor 7\log_2 3 \rfloor = k_{3,r-7} + 11 > k_{3,r-7} + 10\,.$$

(v) $(b_{3,r-17}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_3)$ implies

$$k_{3,r} = k_{3,r-17} + 2 + 26 = k_{3,r-17} + 28\,,$$

so that

$$k_{3,r} \leqslant k_{3,r-17} + \lfloor 17\log_2 3 \rfloor + 1 = k_{3,r-3} + 27 < k_{3,r-3} + 28\,.$$

(vi) $(b_{3,r-29}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathcal{B}_3})$ implies

$$k_{3,r} = k_{3,r-29} + 2 + 18 + 1 + 26 = k_{3,r-29} + 47\,,$$

so that

$$k_{3,r} \leqslant k_{3,r-29} + \lfloor 29\log_2 3 \rfloor + 1 = k_{3,r-29} + 46 < k_{3,r-29} + 47\,.$$

(vii) $(b_{3,r-41}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathcal{B}_2}\mathcal{B}_3)$ implies

$$k_{3,r} = k_{3,r-41} + 2 + (18+1) \times 2 + 26 = k_{3,r-41} + 66\,,$$

so that

$$k_{3,r} \leqslant k_{3,r-41} + \lfloor 41\log_2 3 \rfloor + 1 = k_{3,r-41} + 65 < k_{3,r-41} + 66\,.$$

(viii) $(b_{3,r-53}\dots b_{3,r}) = (\overline{\mathsf{b}}\mathcal{B}_2\overline{\mathcal{B}_2}\mathcal{B}_2\overline{\mathcal{B}_2}\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$ implies

$$k_{3,r} = k_{3,r-53} + 1 + (18+1) \times 4 + (2+1) \times 2 = k_{3,r-53} + 83\,,$$

so that

$$k_{3,r} \geqslant k_{3,r-53} + \lfloor 53\log_2 3 \rfloor = k_{3,r-53} + 84 > k_{3,r-53} + 83\,.$$

(ix) $(b_{3,r-94}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathscr{B}_2}\mathscr{B}_2)$ implies

$$k_{3,r} = k_{3,r-94} + 2 + 18 + (1+64)\times 2 = k_{3,r-94} + 150\,,$$

so that

$$k_{3,r} \leqslant k_{3,r-94} + \lfloor 94\log_2 3\rfloor + 1 = k_{3,r-94} + 149 < k_{3,r-29} + 150\,.$$

(x) $(b_{3,r-306}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathscr{B}_2\mathscr{B}_3^4}\mathscr{B}_2)$ implies

$$k_{3,r} = k_{3,r-306} + 2 + 18 + 1 + 64 + (1+83)\times 4 + 1 + 64 = k_{3,r-306} + 486\,,$$

so that

$$k_{3,r} \leqslant k_{3,r-306} + \lfloor 306\log_2 3\rfloor + 1 = k_{3,r-306} + 485 < k_{3,r-29} + 486\,.$$

(xi) $(b_{3,r-359}\dots b_{3,r}) = (\mathsf{b}\mathscr{B}_3^6\overline{\mathcal{B}_2}\mathcal{B}_2\overline{\mathcal{B}_2}\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$ implies

$$\begin{aligned} k_{3,r} &= k_{3,r-359} + (1+83)\times 6 + (1+18)\times 3 + (1+2)\times 2 + 1 \\ &= k_{3,r-359} + 568\,, \end{aligned}$$

so that

$$k_{3,r} \geqslant k_{3,r-359} + \lfloor 359\log_2 3\rfloor = k_{3,r-359} + 569 > k_{3,r-359} + 568\,.$$

(xii) $(b_{3,r-665}\dots b_{3,r}) = (\overline{\mathsf{b}}\overline{\mathscr{B}_3^6}\mathscr{B}_2\mathscr{B}_3^5\overline{\mathcal{B}_2}\mathcal{B}_2\overline{\mathcal{B}_2}\mathsf{b}^2\overline{\mathsf{b}}^2\mathsf{b})$ implies

$$\begin{aligned} k_{3,r} &= k_{3,r-665} + (1+83)\times 6 + 1 + 64 + (1+83)\times 5 + (1+18)\times 3 \\ &\quad + (1+2)\times 2 + 1 \\ &= k_{3,r-665} + 1053\,, \end{aligned}$$

so that

$$k_{3,r} \geqslant k_{3,r-665} + \lfloor 665\log_2 3\rfloor = k_{3,r-665} + 1054 > k_{3,r-665} + 1053\,.$$

(xiii) $(b_{3,r-971}\dots b_{3,r}) = (\mathsf{b}\mathcal{B}_2\overline{\mathscr{B}_2\mathscr{B}_3^5}\mathscr{B}_2\mathscr{B}_3^5\overline{\mathscr{B}_2\mathscr{B}_3^5}\mathscr{B}_2)$ implies

$$\begin{aligned} k_{3,r} &= k_{3,r-971} + 2 + 18 + 1 + 64 + ((1+83)\times 5 + 1 + 64)\times 3 \\ &= k_{3,r-971} + 1540\,, \end{aligned}$$

so that

$$k_{3,r} \leqslant k_{3,r-971} + \lfloor 971\log_2 3\rfloor + 1 = k_{3,r-971} + 1539 < k_{3,r-971} + 1540\,.$$

□

We have chosen to consider the impossible sequences up to round $r-971$ because these are the only sequences that can be observed over the first 16265 rounds (let us remember that this corresponds to the number of rounds for which we were able to prove in Chapter 6 that the bound on the algebraic degree is tight).

The previous situations can also be written as follows, where each affirmation holds for any value of b in $\mathbb{F}_2$:

(i) there are at least two consecutive b ,

(ii) there are at most three consecutive b ,

(iii) there is at most one consecutive pattern b^3 ,

(iv) there are at most two consecutive patterns b^2 ,

(v) there are at most three consecutive patterns $\overline{\mathsf{b}}^2\mathsf{b}^3$,

(vi) there is at most 1 consecutive $\mathcal{B}_3$,

(vii) there are at least 2 consecutive $\mathcal{B}_2$,

(viii) there are at most 3 consecutive $\mathcal{B}_2$,

(ix) there is at most 1 consecutive $\mathscr{B}_2$,

(x) there are at least 5 consecutive $\mathscr{B}_3$,

(xi) there are at most 6 consecutive $\mathscr{B}_3$,

(xii) there is at most 1 consecutive series of 6 $\mathscr{B}_3$,

(xiii) there are at most 2 consecutive series of 5 $\mathscr{B}_3$.

Consequently, we deduce that the pattern of the parity of $k_{3,r}$ is a sequence of 5 or 6 $\mathscr{B}_3$, separated by a single $\mathscr{B}_2$.

In Figure 7.6 we use a tree to represent the sequences that might appear in the sequence $(b_{3,r})_{r>0}$, where a red dotted arrow means that the transition is impossible because of a case in Lemma 7.2.

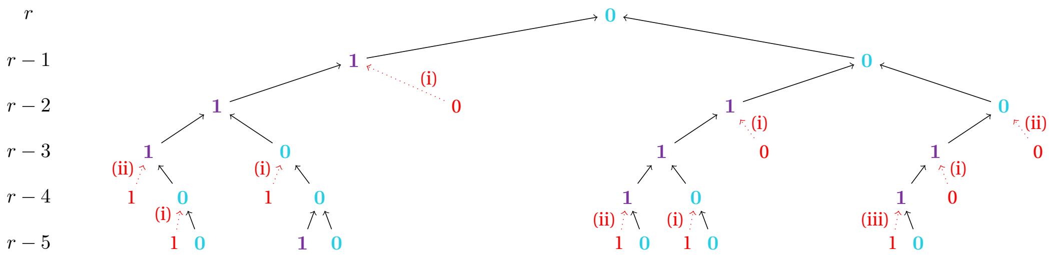


Figure 7.6: *Impossible subsequences in the sequence* $(b_{3,r})_{r>0}$.

As representing each of the impossible arrows makes the figure less compact when increasing the number of rounds. We choose to omit them to represent only the possible sequences in Figure 7.7. Based on Lemma 7.2, we prove that the sequence $\{b_{3,r}\}_{r>0}$ can be obtained by concatenating five different sub-sequences. The tree of Figure 7.7 will then help us to visualize the different cases. We note that we are considering possible sequences on the right of the graph, meaning that for each node with a branching (identified with a square on the figure), the left branch represents the end of a possible sub-sequence. We also choose to stop at round $r-12$ since the next node, at the far right, with two branchings is much further away and it would be difficult to visualize it on the tree.

Proposition 7.1. *Let $(k_{3,r})_{r>0}$ and $(b_{3,r})_{r>0}$ be the sequences defined in Lemma 7.2. Then, for any $r \geqslant 1$, there exists $\mathsf{b} \in \mathbb{F}_2$ such that one of the following situations occurs:*

(i) $(b_{3,r-1}b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b})$,

(ii) $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b}^2)$,

(iii) $(b_{3,r-7}\dots b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b}^2\bar{\mathsf{b}}^2\mathsf{b}^3)$,

(iv) $(b_{3,r-12}\dots b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b}^2(\bar{\mathsf{b}}^2\mathsf{b}^3)^2)$,

(v) $(b_{3,r-12}\dots b_{3,r}) = (\mathsf{b}^3(\bar{\mathsf{b}}^2\mathsf{b}^3)^2)$.

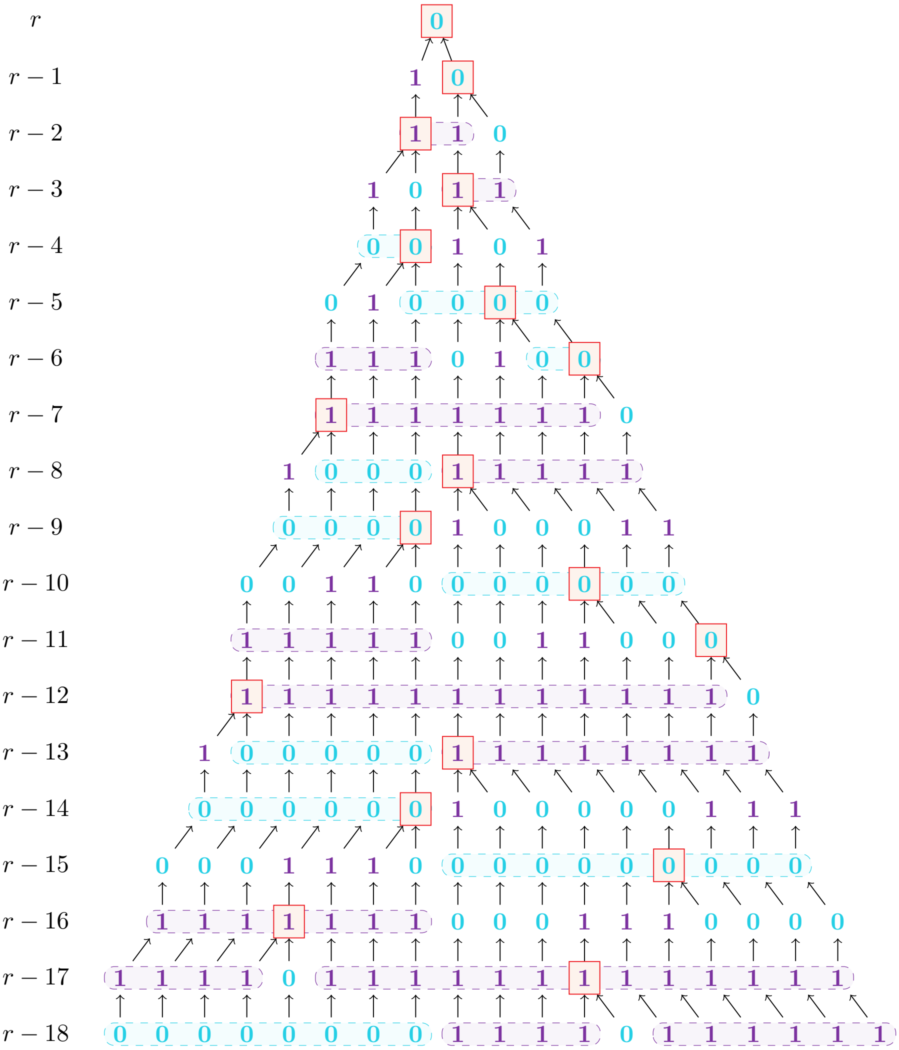
Proof. Let $b_{3,r} = \mathsf{b}$, then we will look at the $b_{3,r-i}$ according to Lemma 7.2. For a better understanding of the steps involved in this proof, we will refer to Figure 7.7. We start with the first node at the top. This node has 2 branches, either $b_{3,r-1} = \bar{\mathsf{b}}$ or $b_{3,r-1} = \mathsf{b}$.

- **If $\boldsymbol{b_{3,r-1}} = \bar{\mathsf{b}}$:** this is a left child, so we stop the process. We have $(b_{3,r-1}b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b})$, which corresponds to the first sequence **(i)**.
- **If $\boldsymbol{b_{3,r-1}} = \mathsf{b}$:** we know from Lemma 7.2-**(i)** and **(ii)** that we have either 2 or 3 consecutive b. In Figure 7.7, we can indeed see that the node 0 in round $(r-1)$ has two branches, either $b_{3,r-2} = \bar{\mathsf{b}}$ or $b_{3,r-2} = \mathsf{b}$.
- **If $\boldsymbol{b_{3,r-2}} = \bar{\mathsf{b}}$:** this is a left child leading to the second sequence **(ii)** since we have $(b_{3,r-2}b_{3,r-1}b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b}^2)$.
- **If $\boldsymbol{b_{3,r-2}} = \mathsf{b}$:** we have necessarily $(b_{3,r-6}\dots b_{3,r}) = (\mathsf{b}^2\bar{\mathsf{b}}^2\mathsf{b}^3)$, because we know from Lemma 7.2-**(iii)** that we cannot have $(\bar{\mathsf{b}}^3\mathsf{b}^3)$. In Figure 7.7, this observation corresponds to a sequence of nodes with only one branching until round $(r-6)$. Then, in round $(r-6)$, the node 0 has two branches, either $b_{3,r-7} = \bar{\mathsf{b}}$ or $b_{3,r-7} = \mathsf{b}$.
- **If $\boldsymbol{b_{3,r-7}} = \bar{\mathsf{b}}$:** we have a left child, so we stop at this node. We get $(b_{3,r-7}\dots b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b}^2\bar{\mathsf{b}}^2\mathsf{b}^3)$, which is the third case **(iii)**.
- **If $\boldsymbol{b_{3,r-7}} = \mathsf{b}$:** we have necessarily $(b_{3,r-11}\dots b_{3,r}) = (\mathsf{b}^2\bar{\mathsf{b}}^2\mathsf{b}^3\bar{\mathsf{b}}^2\mathsf{b}^3) = (\mathcal{B}_2)$, using the same argument as before. In Figure 7.7, this is again translated by a sequence of nodes with only one branching until round $(r-11)$. Then, in round $(r-11)$, the node 0 has two branches, either $b_{3,r-12} = \bar{\mathsf{b}}$ or $b_{3,r-12} = \mathsf{b}$.
- **If $\boldsymbol{b_{3,r-12}} = \bar{\mathsf{b}}$:** we have $(b_{3,r-12}\dots b_{3,r}) = (\bar{\mathsf{b}}\mathsf{b}^2(\bar{\mathsf{b}}^2\mathsf{b}^3)^2)$, so this is the sequence **(iv)**.
- **If $\boldsymbol{b_{3,r-12}} = \mathsf{b}$:** we have $(b_{3,r-12}\dots b_{3,r}) = (\mathsf{b}^3(\bar{\mathsf{b}}^2\mathsf{b}^3)^2)$, which corresponds to the last sequence **(v)**.

□

We interestingly notice that the integers $i \in \{1, 2, 7, 12\}$ corresponding to the sequences $(b_{3,r-i}\dots b_{3,r})$ involved in the proposition are exactly the one such that $(s_1 \dots s_i)$ is a palindrome, where the sequence $(s_r)_{r>0}$ introduced in Chapter 6 is the sequence of switches from one parity to another, i.e.

$$s_1 = 0 \quad \text{and} \quad s_r = b_{3,r} \oplus b_{3,r-1}\,.$$



r 0
r − 1 1 0
r − 2 1 1 0
r − 3 1 0 1 1
r − 4 0 0 1 0 1
r − 5 0 1 0 0 0 0
r − 6 1 1 1 0 1 0 0
r − 7 1 1 1 1 1 1 1 0
r − 8 1 0 0 0 1 1 1 1 1
r − 9 0 0 0 0 1 0 0 0 1 1
r − 10 0 0 1 1 0 0 0 0 0 0 0
r − 11 1 1 1 1 1 0 0 1 1 0 0 0
r − 12 1 1 1 1 1 1 1 1 1 1 1 1 0
r − 13 1 0 0 0 0 0 1 1 1 1 1 1 1 1
r − 14 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1
r − 15 0 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0
r − 16 1 1 1 1 1 1 1 0 0 0 1 1 1 0 0 0 0
r − 17 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1
r − 18 0 0 0 0 0 0 0 0 1 1 1 1 0 1 1 1 1 1 1

Figure 7.7: *The different sub-sequences that could occur in the sequence* $(b_{3,r})_{r>0}$.

7.2.2 Link with music theory

It is interesting to observe the link with denominators of the semi-convergents of $\log_2 3$, that we quickly mentioned in Section 6.1.1. First, let us introduce the notion of *convergents* and *semi-convergents* of a real number.

Definition 7.1. Let $[a_0, a_1, a_2, a_3, \ldots]$ be the continued fraction representation of a real number a:

$$a = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}}.$$

Then the *convergents* of a are given by the fractions:

$$\frac{h_n}{k_n} = [a_0, a_1, a_2, \ldots, a_n] \,.$$

Besides, if the fractions

$$\frac{h_{n-1}}{k_{n-1}} \quad \text{and} \quad \frac{h_n}{k_n}$$

are consecutive convergents, then any fraction

$$\frac{h_{n-1} + m \times h_n}{k_{n-1} + m \times k_n} \quad \text{where} \quad 0 \leqslant m < a_{n+1}$$

is a *semi-convergent*.

More particularly, in the case of $\log_2 3$, it is worth observing that the denominators of semi-convergents are also divisions of the octave that give a good approximation of perfect fifths in music theory. Indeed, let us notice that a perfect octave is the musical interval corresponding to a pair of pitches with a frequency ratio of $(2 : 1)$, while the frequency ratio is $(3 : 2)$ for a perfect fifth. Let us take an example of one fraction representing $\log_2(3)$, we have that

$$\log_2(3) \simeq \frac{11}{7} \quad \text{or equivalently} \quad 2^{11} \simeq 3^7 \,.$$

Then, we deduce that

$$\left(\frac{2}{1}\right)^4 \simeq \left(\frac{3}{2}\right)^7 ,$$

implying that 4 octaves is a good approximation of 7 fifths.

For a deeper understanding of this observation, let us explain a few important points of music theory. The *notes*, in ascending succession of tones, from low to high, are called `C`, `D`, `E`, `F`, `G`, `A`, `B`. We usually start with `C`, since the `C` major scale is used as a reference. A *tone* is the interval between all the notes of the `C` major scale, except between `E` and `F`, and `B` and `C`, in which case it is a *semitone* (half a tone).

The *alterations* are signs that higher or lower the sound of the notes to which they are assigned. The sharp $\sharp$ is higher in pitch by one semitone, a flat $\flat$ is lower by one semitone. This implies that the `C` major scale decomposed in semitones is:

$$\texttt{C - C}\sharp\texttt{/D}\flat\texttt{ - D - D}\sharp\texttt{/E}\flat\texttt{ - E - F - F}\sharp\texttt{/G}\flat\texttt{ - G - G}\sharp\texttt{/A}\flat\texttt{ - A - A}\sharp\texttt{/B}\flat\texttt{ - B}\,.$$

A perfect fifth is composed of 7 semitones, while a perfect octave is composed of 12. It follows that, starting from `C`, a perfect fifth corresponds to

$$\texttt{C - C}\sharp\texttt{/D}\flat\texttt{ - D - D}\sharp\texttt{/E}\flat\texttt{ - E - F - F}\sharp\texttt{/G}\flat\texttt{ - G}\,,$$

and a perfect octave to

$$\texttt{C - C}\sharp\texttt{/D}\flat\texttt{ - D - D}\sharp\texttt{/E}\flat\texttt{ - E - F - F}\sharp\texttt{/G}\flat\texttt{ - G - G}\sharp\texttt{/A}\flat\texttt{ - A - A}\sharp\texttt{/B}\flat\texttt{ - B - C}\,.$$

In Figure 7.8 we compare the construction of 4 octaves and 7 fifths. Starting from `C` we end in `C` for the 4 octaves, while we end in `C`$\sharp$`/D`$\flat$ for 7 fifths, meaning that those two intervals are close up to one semitone.

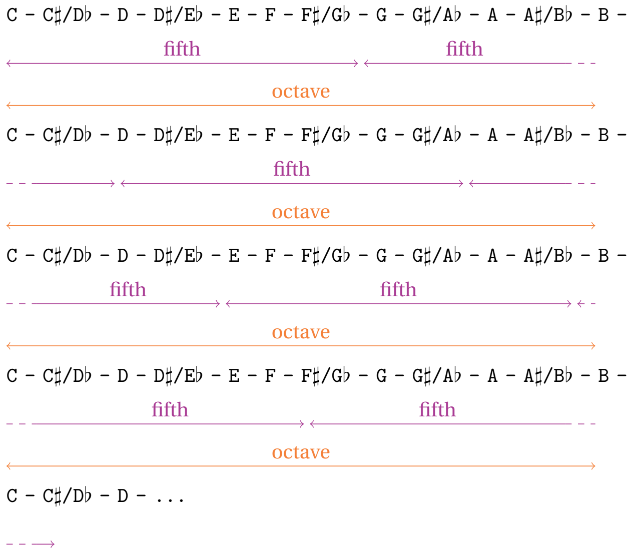

C - C♯/D♭ - D - D♯/E♭ - E - F - F♯/G♭ - G - G♯/A♭ - A - A♯/B♭ - B -
fifth
fifth
octave
C - C♯/D♭ - D - D♯/E♭ - E - F - F♯/G♭ - G - G♯/A♭ - A - A♯/B♭ - B -
fifth
octave
C - C♯/D♭ - D - D♯/E♭ - E - F - F♯/G♭ - G - G♯/A♭ - A - A♯/B♭ - B -
fifth
fifth
octave
C - C♯/D♭ - D - D♯/E♭ - E - F - F♯/G♭ - G - G♯/A♭ - A - A♯/B♭ - B -
fifth
fifth
octave
C - C♯/D♭ - D - ...

Figure 7.8: *Comparison between 4 octaves and 7 fifths.*

Let $\mathfrak{D}_3$ be the set of denominators of the semi-convergents of $\log_2 3$. We have

$$\mathfrak{D}_3 = \{1, 2, 3, 5, 7, 12, 17, 29, 41, 53, 94, 147, 200, 253, 306, 359, 665, 971, \ldots\} .$$

Therefore, it is relevant to notice that the integers i such that there is an impossible subsequence $(b_{3,r-i} \ldots b_{3,r})$ in Lemma 7.2 or a possible sequence in Proposition 7.1 seem to correspond to a subset of $\mathfrak{D}_3$.

Moreover, let us observe that Figure 7.7 raises the following open problems.

1. For each round, there is only one node with branching.

2. If i is a denominator of the semi-convergents of $\log_2 3$, then, at round $r - i$, nodes are either all $\overline{\mathsf{b}}$ or all b (except the node resulting from the branching).

In Appendix B, we will go further by investigating the sequences $(b_{d,r})_{r\geqslant 1}$ for $d > 3$. In particular, we will prove Proposition 7.2, where we identify the possible subsequences for MiMC_d for $d \in \{7, 15, 31, 63\}$.

Proposition 7.2. *Let $d = 2^j - 1$ with $j \in \{3, 4, 5, 6\}$. Let $(k_{d,r})_{r>0}$ and $(b_{d,r})_{r>0}$ be the sequences defined by $k_{d,r} = \lfloor r \log_2 d \rfloor$ and $b_{d,r} = k_{d,r} \mod j$ We defined γ_d as follows:*

$$\gamma_7 = 6 , \qquad \gamma_{15} = 11 , \qquad \gamma_{31} = 22 , \qquad \textit{and} \qquad \gamma_{63} = 45 .$$

Then, for any $r \geqslant 1$, there exists $\mathsf{b} \in \{0, \ldots, j\}$ such that one of the following situations occurs:

(i) $(b_{d,r-i} \ldots b_{d,r}) = (\mathsf{b} \ldots \mathsf{b}) + (10^i)$*, for all $i = 1, \ldots, \gamma_d - 1$,*

(ii) $(b_{d,r-\gamma_d-1} \ldots b_{d,r}) = (\mathsf{b} \ldots \mathsf{b}) + (0^{\gamma_d})$.

Interestingly, the value γ_d is the last integer i in the set $\mathfrak{D}_d$ of the denominators of semi-convergents of $\log_2 d$ such that if $(i-1)$ is in $\mathfrak{D}_d$, then i is also in $\mathfrak{D}_d$. Indeed, let us observe that the first elements in $\mathfrak{D}_d$ for $d \in \{7, 15, 31, 63\}$ are:

$$\begin{aligned}
\mathfrak{D}_7 &= \{1, 2, 3, 4, 5, \mathbf{6}, 11, 16, \ldots\}\,,\\
\mathfrak{D}_{15} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \mathbf{11}, 21, 32, \ldots\}\,,\\
\mathfrak{D}_{31} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, \mathbf{22}, 43, 65, \ldots\}\,,\\
\mathfrak{D}_{63} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26,\\
&\quad 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, \mathbf{45}, 89, 133, \ldots\}\,.
\end{aligned}$$

Although the link between the denominators of the semi-convergents of $\log_2 d$ and the growth of the algebraic degree remains unclear at the time of writing, we will observe, in Appendix B, that for instances of MiMC_d, where d is a Gold function, these numbers seem to only be involved in the lengths of possible sub-sequences of $(b_{d,r})_{r>0}$ while for MiMC_d, where $d \equiv 2^j - 1 \bmod 2^{j+1}$, it appears that they are involved in the lengths of both impossible and possible sub-sequences of $(b_{d,r})_{r>0}$.

7.3 Form of coefficients

In this section, our aim is to better understand the form of the coefficients of the monomials of the univariate polynomials representing MiMC_d. In particular, we will be interested in the study of the univariate representation of MiMC_d as polynomials in the variable x, corresponding to the plaintext and in the key k. A more detailed analysis of the form of the coefficients could help to identify the reasons for some cancellations of coefficients, which could cause the degree to fall. Therefore, in Section 7.3.1, we will see how to detect cancellations of coefficients for MiMC_d by investigating the form of the coefficients for $\mathsf{MiMC}_{d^\lambda}$. Then, in Section 7.3.2, we will also investigate cancellations of coefficients for the MiMC transformation seen as a univariate polynomial in the key k.

7.3.1 Link between $\mathsf{MiMC}_{d^\lambda}$ and MiMC_d.

First, we will look at the form of the coefficients for polynomials in the variable x. One particular line of thought is to study the form of the coefficients of monomials with a maximum-weight exponent. We will, more precisely, focus on the link with the univariate representation of $\mathsf{MiMC}_{d^\lambda}$ that can help to understand the one of MiMC_d.

7.3.1.1 First observations with $\mathsf{MiMC}_{3^\lambda}$ and MiMC_3.

As a first observation, let us notice that the list of monomial exponents given by $\mathcal{E}_{d,r}$ is not minimal since the coefficients of some monomials may cancel for certain choices of round constants. This could cause the degree to fall significantly in certain rounds.

We can then iteratively determine the coefficients of the monomials at each round. Let us recall that in Proposition 5.1 we used that: if $\mathcal{P}_{r-1}(x) = \sum_{i \in \mathcal{E}_{d,r-1}} \alpha_i x^i$ then, we have

$$\mathcal{P}_r(x) = \mathcal{P}'_{r-1}(x^d + c_1) = \sum_{i \in \mathcal{E}_{3,r-1}} \alpha'_i (x^d + c_1)^i\,,$$

where the polynomial $\mathcal{P}'_{r-1}$ corresponds to the polynomial $\mathcal{P}_{r-1}$ with a shift of round constants, i.e. each c_k in α_i is replaced by c_{k+1} in α'_i. Noticing that

$$(x^d + c_1)^i = \prod_{\ell \in I} (x^d + c_1)^{2^\ell} = \prod_{\ell \in I} (x^{d2^\ell} + c_1^{2^\ell}) \quad \text{where} \quad I = Supp(i) \, ,$$

we get, by expanding the product:

$$\left(x^{d \sum_{\ell \in J} 2^\ell} \right) \left(c_1^{\sum_{\ell \in I \setminus J} 2^\ell} \right) \quad \text{where} \quad J \subseteq I \, .$$

Finally, we have that the multi-set $\mathcal{C}_r$ of coefficients of the monomials at round r is:

$$\mathcal{C}_r = \left\{ \alpha'_i \left(c_1^{\sum_{\ell \in I \setminus J} 2^\ell} \right), i \in \mathcal{E}_{d,r-1}, J \subseteq Supp(i) \right\} \, .$$

In the univariate polynomial $\mathcal{P}_r$, the monomials $x^{d \sum_{\ell \in J} 2^\ell}$ are not distinct. Then, when considering the polynomial with only distinct monomials, the coefficients correspond to a sum of elements of $\mathcal{C}_r$, which might be equal to zero.

For a better understanding of the influence of the form of the coefficients, it is also interesting to compare the algebraic degree of MiMC$_9[r]$ with that of MiMC$_3[2r]$. Indeed, the transformation describing MiMC using x^9 as a permutation is equivalent to the transformation describing MiMC using x^3 where every constant of odd index is zero, as described in Figure 7.9.

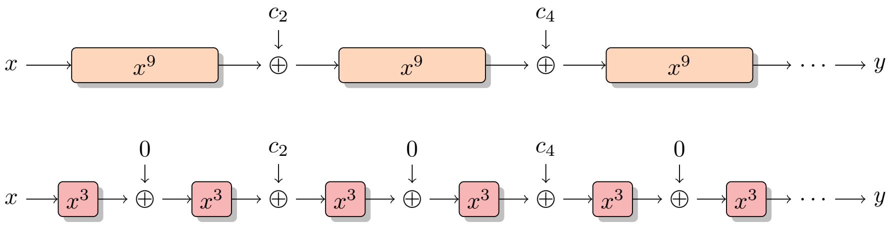


Figure 7.9: *Construction of* MiMC$_9$.

In Figure 7.10a, we can see that the algebraic degree at round r for MiMC$_9$ is not always the same as the algebraic degree at round $2r$ for MiMC$_3$. For example, studying MiMC$_9[r]$ shows that some coefficients cancel when the constants c_i for odd i are zero. If we consider the polynomial representing MiMC$_3[4]$, the observed algebraic degree is 4, but the algebraic degree for MiMC$_9[2]$ is 3. This difference is directly explained by the form of the coefficients of the monomials of maximum-weight exponents at round 4 for MiMC$_3$. We can indeed check, by generating the polynomial representation after each round with a simple Sage implementation, that all of them depend only on the odd index constants c_1 and c_3:

$$27 : c_1^{18} + c_3^2 \, , \quad 30 : c_1^{17} \, , \quad 51 : c_1^{10} \, , \quad 54 : c_1^9 + c_3 \, , \quad 57 : c_1^8 \, , \quad 75 : c_1^2 \, , \quad \text{and} \quad 78 : c_1 \, .$$

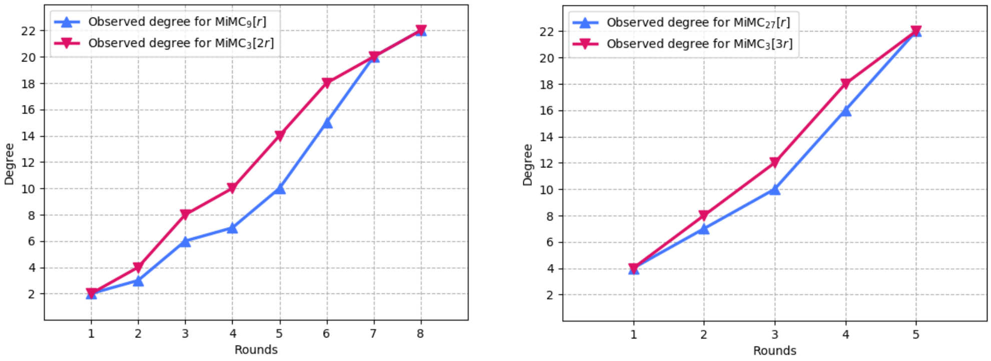
Similarly, the algebraic degree for MiMC$_9[3]$ cannot be 8 since the coefficients of the monomials of maximum-weight exponent at round 6 for MiMC$_3$ are:

$$507 : c_1^2 c_3^8 \, , \quad \text{and} \quad 510 : c_1^{64} c_3 + c_1 c_3^8 \, .$$

In addition, there is only one exponent of degree 7 at round 6, for which the corresponding coefficient also depends on odd index constants.

$$702 : c_3 \ .$$

More generally, the coefficients of monomials with exponents not divisible by 9 can be factored by a linear combination of constants with odd indices.



(a) *When* $\lambda = 2$.

(b) *When* $\lambda = 3$.

Figure 7.10: *Comparison of the degrees of* r *rounds of* MiMC *with* x^{3^λ} *and of* λr *rounds with* x^3.

To compare the algebraic degree of MiMC$_3$ with the algebraic degree of MiMC$_{27}$ we now need to consider MiMC$_3$ with the round constants c_i equal to zero when $i \bmod 3 \in \{1, 2\}$. The construction of MiMC$_{27}$ is depicted in Figure 7.11.

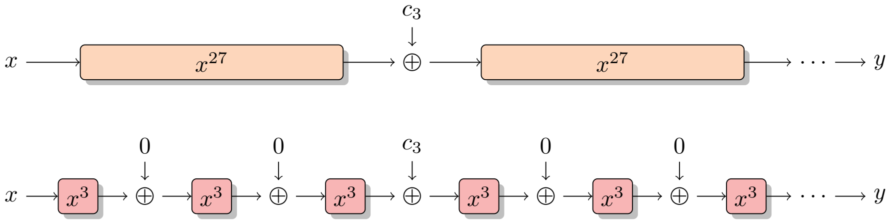
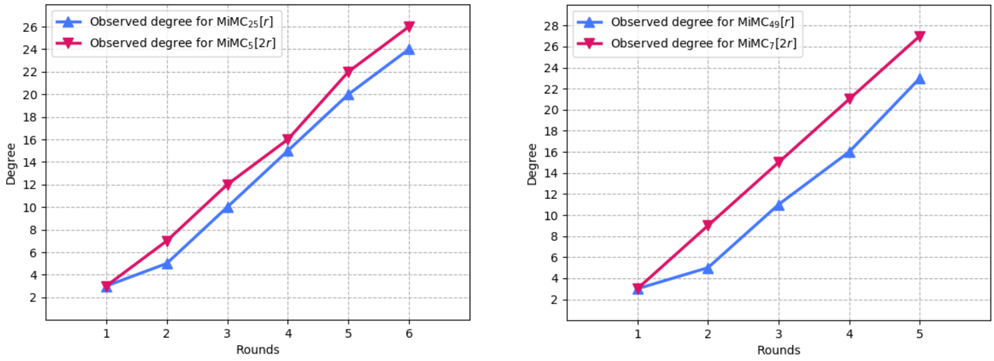


Figure 7.11: *Construction of* MiMC$_{27}$.

As we have seen previously, at round 6 of MiMC$_3$ the algebraic degree is 8. There are two exponents of Hamming weight 8: 507 and 510, which cannot appear in MiMC$_{27}$ since they are divisible by c_1. The only exponent of Hamming weight 7 is 702 but its coefficient equals c_3, so it is likely to appear. Then, the algebraic degree is reduced from 8 to 7 at round 2 of MiMC$_{27}$.

7.3.1.2 Other examples

We choose to compare others instances of MiMC: MiMC$_{5^\lambda}$ and MiMC$_5$, as an example of MiMC$_d$ with a Gold function, and MiMC$_{7^\lambda}$ and MiMC$_7$, as an example of MiMC$_d$, where $d = 2^j - 1$. We focus in particular on the case $\lambda = 2$. It is interesting to notice that we can observe a higher difference between the algebraic degree of MiMC$_{49}[r]$ and MiMC$_7[2r]$ (see Figure 7.12a), than between the algebraic degree of MiMC$_{25}[r]$ and MiMC$_5[2r]$ (see Figure 7.12b).



(a) *When $d = 5$.*

(b) *When $d = 7$.*

Figure 7.12: *Comparison of the degrees of r rounds of* MiMC *with x^{d^2} and of $2r$ rounds with x^d.*

MiMC$_5$

Let us investigate the case of MiMC$_5$. For example at round 4, we have that the exponents of Hamming weight 7 have the following coefficients.

$$445 : c_1^{36}\,, \quad \text{and} \quad 505 : c_1^{24}\,,$$

Both 405 and 505 are divisible by c_1 so they cannot appear at round 2 of MiMC$_{25}$. Then let us also observe that the exponents of Hamming weight 6 are:

$$\begin{array}{llll} 125 : c_1^{100} + c_3^4\,, & 245 : c_1^{76}\,, & 365 : c_1^{52}\,, & 380 : c_1^{49}\,, \\ 485 : c_1^{28}\,, & 500 : c_1^{25} + c_3\,, \text{ and} & 605 : c_1^4\,, & \end{array}$$

implying that they are also missing at round 2 of MiMC$_{25}$. This explains why the algebraic degree drops from 7 to 5.

MiMC$_7$

Let us also study the case of MiMC$_7$. The algebraic degree at round 4 of MiMC$_7$ is 9, but the exponents of maximum weight are

$$\begin{array}{lll} 1015 : c_1^{100}c_3^2 + c_1^2c_3^4\,, & 1022 : c_1c_3^4\,, & 1911 : c_1^{70}\,, \\ 1918 : c_1^{69}\,, & 2030 : c_1^4c_3\,, \text{ and} & 2044 : c_1^2c_3\,, \end{array}$$

implying that they cannot appear at round 2 of MiMC$_{49}$. Then, there is only one exponent of Hamming weight 8:

$$1463 : c_1^{36}c_3^2\,,$$

that is also missing. The coefficients of exponents of Hamming weight 7 have the following form

$$\begin{array}{lll} 1239 : c_1^{68}c_3^2\,, & 1267 : c_1^{64}c_3^2\,, & 1491 : c_1^{32}c_3^2\,, \\ 1687 : c_1^4c_3^2\,, & 1715 : c_3^2\,, & 1939 : c_1^{66}\,, \\ 1946 : c_1^{65}\,, & 2359 : c_1^6\,, \text{ and} & 2366 : c_1^5\,, \end{array}$$

so that they are missing at round 2 of MiMC_{49}. Finally, there are 86 exponents of Hamming weight 6. All are dependent on the constants of odd index. This explains why the algebraic degree is reduced from 9 to 5.

So, although the univariate representation of MiMC_5 (around 50% of missing exponents) is sparser than the one of MiMC_7 (around 25% of missing exponents), more coefficients easily cancelled for MiMC_7, implying that we would expect the algebraic degree to decrease a lot for some weak round constants. This further motivates the need to better understand the exact form of the coefficients.

7.3.2 Missing key monomials

In this section we are interested in studying the MiMC transformation as a univariate polynomial in the key k instead of a univariate polynomial in the plaintext x. Our aim is to investigate cancellations of coefficients to identify missing monomials in the polynomial. We will more particularly focus on the case MiMC_3.

7.3.2.1 First observations

Let us consider the case where the iterated permutation is the cube. We recall that round i of MiMC_3 corresponds to the function:

$$F_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, x \mapsto (x + k + c_{i-1})^3 ,$$

where $(c_0, \ldots, c_{r-1})$ is a sequence of round constants such that $c_0 = 0$.

Let $\mathcal{P}_r(k, x)$ be the bivariate polynomial in k and x describing $\mathsf{MiMC}_3[r]$. So far we were only studying this polynomial with a fixed key. While it was previously denoted by $\mathcal{P}_r(x)$, in this section we will use the notation $\mathcal{P}_r^k(x)$ to easily distinguish it from the polynomial in the key.

Then, in the following, we will use

$$\mathcal{P}_r^x(k) = \sum_{i=0}^{3^r} \alpha_{r,i} k^i$$

to denote the polynomial in k describing $\mathsf{MiMC}_3[r]$, i.e. the polynomial $\mathcal{P}_r(k, x)$ where x is fixed. Then the $\alpha_{r,i}$ are coefficients depending on x.

At the first round, we have

$$\mathcal{P}_1^x(k) = (x + k)^3 = k^3 + x \cdot k^2 + x^2 \cdot k + x^3 .$$

So we have the monomials $\{0, k, k^2, k^3\}$. We note that, when considering the polynomial in the variable x, we also have all the possible monomials $\{0, x, x^2, x^3\}$.

Then, at the second round, we have

$$\begin{aligned}
\mathcal{P}_2^x(k) &= (\mathcal{P}_1^x(k) + k + c_1)^3 \\
&= (k^3 + x \cdot k^2 + (x^2 + 1) \cdot k + x^3 + c_1)^3 \\
&= (k^6 + x^2 \cdot k^4 + (x^4 + 1) \cdot k^2 + x^6 + c_1^2) \\
&\quad \times (k^3 + x \cdot k^2 + (x^2 + 1) \cdot k + x^3 + c_1) .
\end{aligned}$$

After expanding the multiplication we get

$$\begin{aligned}\mathcal{P}_2^x(k) = k^9 &+ x\cdot k^8 + (x^2+1)\cdot k^7 + (x^3+c_1)\cdot k^6\\ &+ x^2\cdot k^7 + x^3\cdot k^6 + (x^4+x^2)\cdot k^5 + (x^5+c_1x^2)\cdot k^4\\ &+ (x^4+1)\cdot k^5 + (x^5+x)\cdot k^4 + (x^6+x^4+x^2+1)\cdot k^3\\ &+ (x^7+c_1x^4+x^3+c_1)\cdot k^2\\ &+ (x^6+c_1^2)\cdot k^3 + (x^7+c_1^2x)\cdot k^2 + (x^8+x^6+c_1^2x^2+c_1^2)\cdot k\\ &+ x^9+c_1x^6+c_1^2x^3+c_1^3\,.\end{aligned}$$

Finally, by re-arranging the monomials we obtain:

$$\begin{aligned}\mathcal{P}_2^x(k) = k^9 &+ x\cdot k^8 + k^7 + c_1\cdot k^6 + (x^2+1)\cdot k^5 + (c_1x^2+x)\cdot k^4\\ &+ (x^4+x^2+1+c_1^2)\cdot k^3 + (c_1x^4+x^3+c_1^2x+c_1)\cdot k^2\\ &+ (x^8+x^6+c_1^2x^2+c_1^2)\cdot k + (x^9+c_1x^6+c_1^2x^3+c_1^3)\,.\end{aligned}$$

So we have again all the monomials in k, namely $\{0,k,k^2,k^3,k^4,k^5,k^6,k^7,k^8,k^9\}$. However, we only have $\{0,x,x^2,x^3,x^4,x^6,x^8,x^9\}$, meaning that while we have specific families of missing exponents for monomials in x, this does not happen similarly for monomials in k. Then, we are also interested in studying the coefficients of monomials in the key. Lemma 7.3 exhibits the recurrence relation expressing these coefficients at round r from the coefficients at round $(r-1)$. As we will see, the study is much more complex than for polynomials in the variable x.

Lemma 7.3. *Let $\mathcal{P}_{r-1}^x(k)$ be the polynomial describing $\mathsf{MiMC}_3[r-1]$ such that*

$$\mathcal{P}_{r-1}^x(k) = \sum_{i=0}^{3^{r-1}} \alpha_{r-1,i}k^i\,.$$

Then, the coefficients $\alpha_{r,i}$ of the monomials in the polynomial $\mathcal{P}_r^x$ describing $\mathsf{MiMC}_3[r]$ are given by:

$$\begin{aligned}\alpha_{r,0} &= (\alpha_{r-1,0}+c_{r-1})^3\\ \alpha_{r,1} &= (\alpha_{r-1,0}^2+c_{r-1}^2)(\alpha_{r-1,1}+1)\\ \alpha_{r,2} &= \alpha_{r-1,2}(\alpha_{r-1,0}^2+c_{r-1}^2)+(\alpha_{r-1,0}+c_{r-1})(\alpha_{r-1,1}^2+1)\\ \alpha_{r,3} &= \alpha_{r-1,3}(\alpha_{r-1,0}^2+c_{r-1}^2)+(\alpha_{r-1,1}+1)^3\\ \alpha_{r,4} &= \alpha_{r-1,4}(\alpha_{r-1,0}^2+c_{r-1}^2)+\alpha_{r-1,2}(\alpha_{r-1,1}^2+1)+\alpha_{r-1,2}^2(\alpha_{r-1,0}+c_{r-1})\\ \alpha_{r,5} &= \alpha_{r-1,5}(\alpha_{r-1,0}^2+c_{r-1}^2)+\alpha_{r-1,3}(\alpha_{r-1,1}^2+1)+\alpha_{r-1,2}^2(\alpha_{r-1,1}+1)\,,\end{aligned}$$

And for i such that $6\leqslant i\leqslant 3^r$, we have the following:

$$\alpha_{r,i} = \mathcal{S} + \sum_{\ell,m\ s.t.\ 2\ell+m=i} \alpha_{r-1,\ell}^2\alpha_{r-1,m}\,,$$

where $\mathcal{S}$ is defined by

$$\mathcal{S} = \begin{cases} \alpha_{r-1,i}(\alpha_{r-1,0}^2 + c_{r-1}^2) & \\ \quad +\alpha_{r-1,i-2}(\alpha_{r-1,1}^2 + 1) & \\ \quad +\alpha_{r-1,i/2}^2(\alpha_{r-1,0} + c_{r-1}) & \textit{if } 6 \leqslant i \leqslant 3^{r-1}, i \equiv 0 \bmod 2\,, \\ \alpha_{r-1,i}(\alpha_{r-1,0}^2 + c_{r-1}^2) & \\ \quad +\alpha_{r-1,i-2}(\alpha_{r-1,1}^2 + 1) & \\ \quad +\alpha_{r-1,(i-1)/2}^2(\alpha_{r-1,1} + 1) & \textit{if } 6 \leqslant i \leqslant 3^{r-1}, i \equiv 1 \bmod 2\,, \\ \alpha_{r-1,i-2}(\alpha_{r-1,1}^2 + 1) & \\ \quad +\alpha_{r-1,i/2}^2(\alpha_{r-1,0} + c_{r-1}) & \textit{if } i = 3^{r-1} + 1\,, \\ \alpha_{r-1,i-2}(\alpha_{r-1,1}^2 + 1) & \\ \quad +\alpha_{r-1,(i-1)/2}^2(\alpha_{r-1,1} + 1) & \textit{if } i = 3^{r-1} + 2\,, \\ \alpha_{r-1,i/2}^2(\alpha_{r-1,0} + c_{r-1}) & \textit{if } 3^{r-1} + 3 \leqslant i \leqslant 2 \cdot 3^{r-1} - 1, i \equiv 0 \bmod 2\,, \\ \alpha_{r-1,(i-1)/2}^2(\alpha_{r-1,1} + 1) & \textit{if } 3^{r-1} + 3 \leqslant i \leqslant 2 \cdot 3^{r-1} - 1, i \equiv 1 \bmod 2\,, \\ 0 & \textit{if } i \geqslant 2 \cdot 3^{r-1}\,. \end{cases}$$

Proof. Using $\mathcal{P}_r^x(k) = \left(\mathcal{P}_{r-1}^x(k) + k + c_{r-1}\right)^3$, we have

$$\begin{aligned} \mathcal{P}_r^x(k) &= \left(\sum_{i=0}^{3^{r-1}} \alpha_{r-1,i} k^i + k + c_{r-1} \right)^3 \\ &= \left((\alpha_{r-1,0} + c_{r-1}) + (\alpha_{r-1,1} + 1)k + \sum_{i=2}^{3^{r-1}} \alpha_{r-1,i} k^i \right)^3 \,, \end{aligned}$$

implying that

$$\begin{aligned} \mathcal{P}_r^x(k) = &\left((\alpha_{r-1,0}^2 + c_{r-1}^2) + (\alpha_{r-1,1}^2 + 1)k^2 + \sum_{i=2}^{3^{r-1}} \alpha_{r-1,i}^2 k^{2i} \right) \\ &\times \left((\alpha_{r-1,0} + c_{r-1}) + (\alpha_{r-1,1} + 1)k + \sum_{i=2}^{3^{r-1}} \alpha_{r-1,i} k^i \right) . \end{aligned}$$

It follows that

$$\begin{aligned}\mathcal{P}_r^x(k) = {} & (\alpha_{r-1,0} + c_{r-1})^3 + (\alpha_{r-1,0}^2 + c_{r-1}^2)(\alpha_{r-1,1} + 1)k \\ & + \sum_{i=2}^{3^{r-1}} \alpha_{r-1,i}(\alpha_{r-1,0}^2 + c_{r-1}^2)k^i + (\alpha_{r-1,0} + c_{r-1})(\alpha_{r-1,1}^2 + 1)k^2 \\ & + (\alpha_{r-1,1} + 1)^3 k^3 + \sum_{i=2}^{3^{r-1}} \alpha_{r-1,i}(\alpha_{r-1,1}^2 + 1)k^{i+2} \\ & + \sum_{i=2}^{3^{r-1}} \alpha_{r-1,i}^2(\alpha_{r-1,0} + c_{r-1})k^{2i} + \sum_{i=2}^{3^{r-1}} \alpha_{r-1,i}^2(\alpha_{r-1,1} + 1)k^{2i+1} \\ & + \sum_{i=2}^{3^{r-1}} \sum_{j=2}^{3^{r-1}} \alpha_{r-1,i}^2 \alpha_{r-1,j} k^{2i+j}\end{aligned}$$

□

Although it is difficult to see a pattern to detect families of missing exponents, these relations allows us to identify some missing exponents close to 3^r.

Proposition 7.3. *Let $\mathcal{P}_r^x(k)$ be the polynomial describing r rounds of MiMC_3 such that*

$$\mathcal{P}_r^x(k) = \sum_{i=0}^{3^r} \alpha_{r,i} k^i \, .$$

If r is odd, then, for $j = 4, 5, 6, 7$, we have $\alpha_{r,3^r-j} = 0$ meaning that monomials k^{3^r-j} are missing in $\mathcal{P}_r^x$.

Proof. To prove that such monomials are missing, we will show by induction on r that the coefficients of the last 8 monomials are given by the following formulas:

if r is even

$$\begin{aligned}\alpha_{r,3^r-7} &= c_1x^4 + x^3 + c_1^2x + c_1 \\ \alpha_{r,3^r-6} &= x^4 + x^2 + c_1^2 + 1 \\ \alpha_{r,3^r-5} &= c_1x^2 + x \\ \alpha_{r,3^r-4} &= x^2 + 1 \\ \alpha_{r,3^r-3} &= c_1 \\ \alpha_{r,3^r-2} &= 1 \\ \alpha_{r,3^r-1} &= x \\ \alpha_{r,3^r} &= 1\,.\end{aligned}$$

if r is odd

$$\begin{aligned}\alpha_{r,3^r-7} &= 0 \\ \alpha_{r,3^r-6} &= 0 \\ \alpha_{r,3^r-5} &= 0 \\ \alpha_{r,3^r-4} &= 0 \\ \alpha_{r,3^r-3} &= x^3 + c_1 \\ \alpha_{r,3^r-2} &= x^2 + 1 \\ \alpha_{r,3^r-1} &= x \\ \alpha_{r,3^r} &= 1\,.\end{aligned}$$

First it holds at round 2 for coefficients of monomials $k^2, \ldots, k^9$. Indeed, we have

$$\begin{aligned}\mathcal{P}_2^x(k) = {} & k^9 + x \cdot k^8 + k^7 + c_1 \cdot k^6 + (x^2+1) \cdot k^5 + (c_1x^2 + x) \cdot k^4 \\ & + (x^4 + x^2 + c_1^2 + 1) \cdot k^3 + (c_1x^4 + x^3 + c_1^2x + c_1) \cdot k^2 \\ & + (x^8 + x^6 + c_1^2x^2 + c_1^2) \cdot k + (x^9 + c_1x^6 + c_1^2x^3 + c_1^3)\,.\end{aligned}$$

Let us now assume that the property holds at round r, i.e. that for $j \in \{0, \ldots 7\}$, $\alpha_{r,3^r-j}$ are given by the above equations.

Then using Lemma 7.3 let us compute the $\alpha_{r+1,3^{r+1}-i}$ for $i \in \{0,\dots 7\}$. For $\alpha_{r+1,3^{r+1}-7}$, we get

$$\alpha_{r+1,3^{r+1}-7} = \alpha^2_{r,3^r-3}\alpha_{r,3^r-1} + \alpha^2_{r,3^r-2}\alpha_{r,3^r-3} + \alpha^2_{r,3^r-1}\alpha_{r,3^r-5} + \alpha^2_{r,3^r}\alpha_{r,3^r-7} .$$

It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-7} &= (x^3+c_1)^2\cdot x + (x^2+1)^2\cdot(x^3+c_1) + x^2\cdot 0 + 1^2\cdot 0\\ &= (x^6+c_1^2)\cdot x + (x^4+1)(x^3+c_1)\\ &= c_1x^4 + x^3 + c_1^2x + c_1 ,\end{aligned}$$

and if $r+1$ is odd, then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-7} &= c_1^2\cdot x + 1^2\cdot c_1 + x^2\cdot(c_1x^2+x) + 1^2\cdot(c_1x^4+x^3+c_1^2x+c_1)\\ &= 0 .\end{aligned}$$

Similarly, for $\alpha_{r+1,3^{r+1}-6}$, we get

$$\alpha_{r+1,3^{r+1}-6} = \alpha^2_{r,3^r-3}\alpha_{r,3^r} + \alpha^3_{r,3^r-2} + \alpha^2_{r,3^r-1}\alpha_{r,3^r-4} + \alpha^2_{r,3^r}\alpha_{r,3^r-6} .$$

It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-6} &= (x^3+c_1)^2\cdot 1 + (x^2+1)^3 + x^2\cdot 0 + 1^2\cdot 0\\ &= (x^6+c_1^2) + (x^6+x^4+x^2+1)\\ &= x^4+x^2+c_1^2+1 ,\end{aligned}$$

and if $r+1$ is odd, then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-6} &= c_1^2\cdot 1 + 1^3 + x^2\cdot(x^2+1) + 1^2\cdot(x^4+x^2+c_1^2+1)\\ &= 0 .\end{aligned}$$

For $\alpha_{r+1,3^{r+1}-5}$, we get

$$\alpha_{r+1,3^{r+1}-5} = \alpha^2_{r,3^r-2}\alpha_{r,3^r-1} + \alpha^2_{r,3^r-1}\alpha_{r,3^r-3} + \alpha^2_{r,3^r}\alpha_{r,3^r-5} .$$

It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-5} &= (x^2+1)^2\cdot x + x^2\cdot(x^3+c_1) + 1^2\cdot 0\\ &= (x^4+1)\cdot x + x^5 + c_1x^2\\ &= c_1x^2 + x ,\end{aligned}$$

and if $r+1$ is odd, then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-5} &= 1^2\cdot x + x^2\cdot c_1 + 1^2\cdot(c_1x^2+x)\\ &= 0 .\end{aligned}$$

For $\alpha_{r+1,3^{r+1}-4}$, we get

$$\alpha_{r+1,3^{r+1}-4} = \alpha^2_{r,3^r-2}\alpha_{r,3^r} + \alpha^2_{r,3^r-1}\alpha_{r,3^r-2} + \alpha^2_{r,3^r}\alpha_{r,3^r-4} .$$

It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-4} &= (x^2+1)^2\cdot 1 + x^2\cdot(x^2+1) + 1^2\cdot 0\\ &= x^2+1\,,\end{aligned}$$

and if $r+1$ is odd, then we have

$$\begin{aligned}\alpha_{r+1,3^{r+1}-4} &= 1^2\cdot 1 + x^2\cdot 1 + 1^2\cdot(x^2+1)\\ &= 0\,.\end{aligned}$$

Then for $\alpha_{r+1,3^{r+1}-3}$, we get

$$\alpha_{r+1,3^{r+1}-3} = \alpha^3_{r,3^r-1} + \alpha^2_{r,3^r}\alpha_{r,3^r-3}\,.$$

It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\alpha_{r+1,3^{r+1}-3} = x^3 + 1^2\cdot(x^3+c_1) = c_1\,,$$

and if $r+1$ is odd, then we have

$$\alpha_{r+1,3^{r+1}-3} = x^3 + 1^2\cdot c_1 = x^3 + c_1\,.$$

For $\alpha_{r+1,3^{r+1}-2}$, we get

$$\alpha_{r+1,3^{r+1}-2} = \alpha^2_{r,3^r-1}\alpha_{r,3^r} + \alpha^2_{r,3^r}\alpha_{r,3^r-2}\,.$$

It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\alpha_{r+1,3^{r+1}-2} = x^2\cdot 1 + 1^2\cdot(x^2+1) = 1\,,$$

and if $r+1$ is odd, then we have

$$\alpha_{r+1,3^{r+1}-2} = x^2\cdot 1 + 1^2\cdot 1 = x^2+1\,.$$

For $\alpha_{r+1,3^{r+1}-1}$, we get

$$\alpha_{r+1,3^{r+1}-1} = \alpha^2_{r,3^r}\alpha_{r,3^r-1}\,.$$

It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\alpha_{r+1,3^{r+1}-1} = 1^2\cdot x = x\,,$$

and if $r+1$ is odd, then we have

$$\alpha_{r+1,3^{r+1}-1} = 1^2\cdot x = x\,.$$

Finally, for $\alpha_{r+1,3^{r+1}}$, we get

$$\alpha_{r+1,3^{r+1}} = \alpha^3_{r,3^r}\,.$$

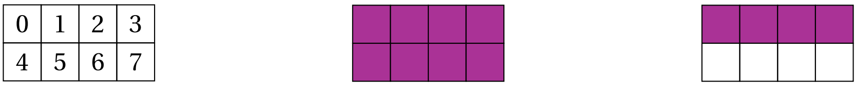
It follows that if $r+1$ is even (i.e. r is odd), then we have

$$\alpha_{r+1,3^{r+1}} = 1^3 = 1\,,$$

and if $r+1$ is odd, then we have

$$\alpha_{r+1,3^{r+1}} = 1^3 = 1\,.$$

□

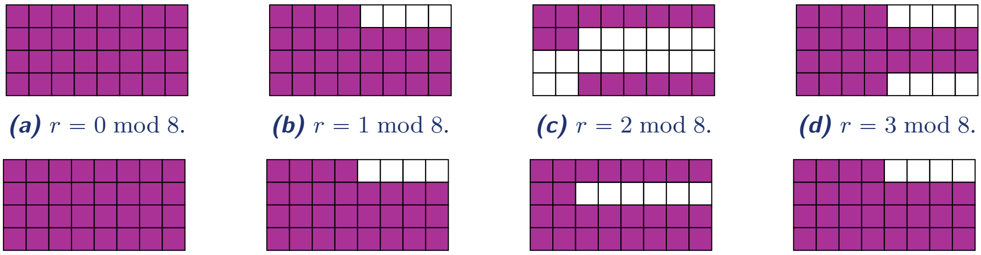


(a) *Representation of* $3^k - i$. ***(b)*** $r = 0 \bmod 2$. ***(c)*** $r = 1 \bmod 2$.

Figure 7.13: *Missing exponents* $3^r - i$ *with* $0 \leqslant i \leqslant 7$.

We can illustrate the previous result with Figure 7.13, where each exponent $3^r - i$ for $i \in \{0, \dots, 7\}$ is represented by a square so that the squares ■ correspond to the exponents that might appear in the polynomial, and the squares □ the missing exponents.

Going further with experiments, we have observed the pattern of Figure 7.14 for exponents $3^r - i$ for $i \in \{0, \dots, 31\}$. However, to prove this result we would need to consider the representation of the coefficients depending on the value of r modulo 8. Given the complexity of the representation of the coefficients, we have not pushed the study to this point.



(a) $r = 0 \bmod 8$. ***(b)*** $r = 1 \bmod 8$. ***(c)*** $r = 2 \bmod 8$. ***(d)*** $r = 3 \bmod 8$.

(e) $r = 4 \bmod 8$. ***(f)*** $r = 5 \bmod 8$. ***(g)*** $r = 6 \bmod 8$. ***(h)*** $r = 7 \bmod 8$.

Figure 7.14: *Missing exponents* $3^k - i$ *with* $0 \leqslant i \leqslant 31$.

We will now show that the situation is different for $\mathcal{P}_r^k$ since the monomials of degree $3^r - i$ for $i \in \{1, \dots 7\}$ that are missing are not the same as in $\mathcal{P}_r^x$. First, let us observe the form of the powers of 3.

Lemma 7.4. *Let* $r \geqslant 1$ *then:*

$$\begin{array}{rcrlrcrl}
3^r &=& 1 \bmod 32 & \textit{if} \quad r \equiv 0 \bmod 8\,, & 3^r &=& 17 \bmod 32 & \textit{if} \quad r \equiv 4 \bmod 8\,, \\
3^r &=& 3 \bmod 32 & \textit{if} \quad r \equiv 1 \bmod 8\,, & 3^r &=& 19 \bmod 32 & \textit{if} \quad r \equiv 5 \bmod 8\,, \\
3^r &=& 9 \bmod 32 & \textit{if} \quad r \equiv 2 \bmod 8\,, & 3^r &=& 25 \bmod 32 & \textit{if} \quad r \equiv 6 \bmod 8\,, \\
3^r &=& 27 \bmod 32 & \textit{if} \quad r \equiv 3 \bmod 8\,, & 3^r &=& 11 \bmod 32 & \textit{if} \quad r \equiv 7 \bmod 8\,.
\end{array}$$

Proof. Let us notice that the property holds for the first eight rounds since we have

$$\begin{array}{rcrlrcrcrl}
3^1 &=& & 3 \bmod 32\,, & 3^5 &=& 243 &=& 19 \bmod 32\,, \\
3^2 &=& & 9 \bmod 32\,, & 3^6 &=& 729 &=& 25 \bmod 32\,, \\
3^3 &=& & 27 \bmod 32\,, & 3^7 &=& 2187 &=& 11 \bmod 32\,, \\
3^4 &=& 81 = & 17 \bmod 32\,, & 3^8 &=& 6561 &=& 1 \bmod 32\,.
\end{array}$$

Then, since $3^8 = 1 \bmod 32$. We have that if 3^r satisfies the property, then $3^{r+8} = 3^r \cdot 3^8 = 3^r \bmod 32$ also satisfies the property. □

This lemma allows us to determine some families of exponents that are missing, or some families of exponents that might appear in the polynomial $\mathcal{P}_r^k(x)$ based on Proposition 5.6. For example, if $r \equiv 0 \bmod 2$ we have $3^r \equiv 1 \bmod 8$, implying that

$$3^r - 2 \equiv 7 \bmod 8 \quad \text{and} \quad 3^r - 4 \equiv 5 \bmod 8\,.$$

We then deduce that the exponents of the form $\{3^r - (2+8i), 3^r - (2+8i),\ \text{with } i \geqslant 0\}$ are missing. Similarly, if $r \equiv 1 \bmod 2$ we have $3^r \equiv 3 \bmod 8$, implying that

$$3^r - 4 \equiv 7 \bmod 8 \quad \text{and} \quad 3^r - 6 \equiv 5 \bmod 8\,.$$

We then deduce that the exponents of the form $\{3^r - (4+8i), 3^r - (6+8i),\ \text{with } i \geqslant 0\}$ are missing.

Moreover, we identify some exponents that are likely to appear at round r since they belong to $\mathcal{E}_{3,r}$. We describe them in Observation 7.1 and 7.2.

Figure 7.15 shows the missing integers that we saw with experiments on the first rounds, implementing the procedure of Corollary 5.1. We also highlight the cases that we have discussed above. The squares ● represent exponents captured with Observation 7.1, the squares ◇ represent exponents captured with Observation 7.2, the squares ■ represent the other exponents appearing, the squares ★ the missing exponents equal to 5 or 7 modulo 8, the squares □ the other missing exponents. Let us notice that the figures are dependent on the value of r modulo 8. In particular the position of the squares ★ depend on the value of r modulo 2.

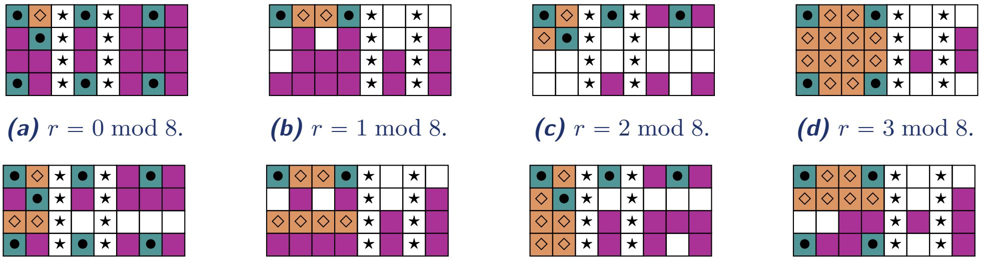

(a) $r = 0 \bmod 8$.
(b) $r = 1 \bmod 8$.
(c) $r = 2 \bmod 8$.
(d) $r = 3 \bmod 8$.
(e) $r = 4 \bmod 8$.
(f) $r = 5 \bmod 8$.
(g) $r = 6 \bmod 8$.
(h) $r = 7 \bmod 8$.

Figure 7.15: *Missing exponents* $3^r - i$*, in* $\mathcal{P}_r^k$*, with* $0 \leqslant i \leqslant 31$.

Observation 7.1. Like for $\mathcal{P}_r^x$, we analyze the monomials of degree greater than or equal to $3^r - 31$. We recall that $\mathcal{E}_{3,r} = \{3j, j \preceq i, i \in \mathcal{E}_{3,r-1}\}$. It follows that, if $i \leqslant 15$ satisfies $i \preceq (3^{r-1} \bmod 16)$, then $(3^{r-1} - i) \preceq 3^{r-1}$, implying that $(3^r - 3i) \in \mathcal{E}_{3,r}$. Then depending on $(r - 1 \bmod 4)$ we deduce the following.

- If $r - 1 \equiv 0 \bmod 4$, we have $3^{r-1} \equiv 1 \bmod 16$ implying that

  $$\{3^r - 3\} \subset \mathcal{E}_{3,r}\,.$$

  Since this allows us to derive exponents that might appear at round r where $r \equiv 1 \bmod 4$, this case corresponds to Figures 7.15b and 7.15f.

- If $r - 1 \equiv 1 \bmod 4$, we have $3^{r-1} \equiv 3 \bmod 16$ implying that

  $$\{3^r - 3, 3^r - 6, 3^r - 9\} \subset \mathcal{E}_{3,r}\,.$$

  This case corresponds to Figures 7.15c and 7.15g.

- If $r-1 \equiv 2 \bmod 4$, we have $3^{r-1} \equiv 9 \bmod 16$ implying that
$$\{3^r-3, 3^r-24, 3^r-27\} \subset \mathcal{E}_{3,r} \ .$$
This case corresponds to Figures 7.15d and 7.15h.
- If $r-1 \equiv 3 \bmod 4$, we have $3^{r-1} \equiv 11 \bmod 16$ implying that
$$\{3^r-3, 3^r-6, 3^r-9, 3^r-24, 3^r-27, 3^r-30\} \subset \mathcal{E}_{3,r} \ .$$
This case corresponds to Figures 7.15a and 7.15e.

Observation 7.2. Let us also recall that for the study of the algebraic degree in Chapters 5 and 6 we focused on a keyless setting. As we are now considering a setting with a whitening key, i.e. $\mathcal{P}_r^k(x) = \mathcal{P}_r(x+k)$, the exponents in $\mathcal{P}_r^k$ are covered by the exponents in $\mathcal{P}_r$. Indeed,
$$\mathcal{P}_r(x) = \sum_{i \in \mathcal{E}_{3,r}} \alpha_i x^i \quad \Rightarrow \mathcal{P}_r(x+k) = \sum_{j, j \preceq i, i \in \mathcal{E}_{3,r}} \alpha'_j x^j \ .$$

It follows that we can capture more exponents that might appear in the $\mathcal{P}_r^k$. Indeed, using that $3^r \in \mathcal{E}_{3,r}$, we deduce that any exponent covered by 3^r is likely to appear in $\mathcal{P}_r^k$. We then derive that:

- If $r \equiv 0 \bmod 8$, we have $3^r \equiv 1 \bmod 32$ so that
$$\{3^r-1\} \subset \mathcal{E}_{3,r} \ .$$
- If $r \equiv 1 \bmod 8$, we have $3^r \equiv 3 \bmod 32$ so that
$$\{3^r-1, 3^r-2, 3^r-3\} \subset \mathcal{E}_{3,r} \ .$$
- If $r \equiv 2 \bmod 8$, we have $3^r \equiv 9 \bmod 32$ so that
$$\{3^r-1, 3^r-8, 3^r-9\} \subset \mathcal{E}_{3,r} \ .$$
- If $r \equiv 3 \bmod 8$, we have $3^r \equiv 27 \bmod 32$ so that
$$\{3^r-i, i \in \{1,2,3,8,9,10,11,16,17,18,19\}\} \subset \mathcal{E}_{3,r} \ .$$
- If $r \equiv 4 \bmod 8$, we have $3^r \equiv 17 \bmod 32$ so that
$$\{3^r-1, 3^r-16, 3^r-17\} \subset \mathcal{E}_{3,r} \ .$$
- If $r \equiv 5 \bmod 8$, we have $3^r \equiv 19 \bmod 32$ so that
$$\{3^r-i, i \in \{1,2,3,16,17,18,19,24,25,26,27\}\} \subset \mathcal{E}_{3,r} \ .$$
- If $r \equiv 6 \bmod 8$, we have $3^r \equiv 25 \bmod 32$ so that
$$\{3^r-i, i \in \{1,8,9,16,17,24,25\}\} \subset \mathcal{E}_{3,r} \ .$$
- If $r \equiv 7 \bmod 8$, we have $3^r \equiv 11 \bmod 32$ so that
$$\{3^r-i, i \in \{1,2,3,8,9,10,11\}\} \subset \mathcal{E}_{3,r} \ .$$

Conclusion

In this chapter we have seen different perspectives to extend the study of the algebraic degree of iterated power functions. We first answered different questions regarding the growth of the algebraic degree for SPN constructions with an affine layer. This analysis is based on the coefficient grouping strategy that allows to efficiently represent the exponents that might appear in the polynomial describing the construction. In particular, we gave some necessary conditions on the density of the affine layer to ensure an exponential growth of the algebraic degree for a certain number of rounds.

We also discussed the impossible sub-sequences of $(b_{d,r})_{r>0}$ for various instances of MiMC_d. While we did not manage to clearly understand the link between these sequences and the algebraic degree of MiMC_d, we believe that there might be more to be done in this direction.

We finally investigated the forms of the coefficients in the two univariate polynomials, the one in the variable x, corresponding to the plaintext, and the one in the key k. Although this chapter does not necessarily provide precise answers to all the questions that have been raised, we believe that these results could encourage further work in these directions.

Conclusions and perspectives

This manuscript significantly contributes to enhancing our understanding of the tools used for designing and analyzing these new symmetric primitives defined on large finite fields. In particular, we propose a new family of hash functions, `Anemoi`, offering very good performance for zero-knowledge proofs. The authors of [Liu+22] have demonstrated the potential of `Anemoi` with additional optimizations. The insights provided by `Anemoi` contribute significantly to a deeper understanding of the design principles behind these new primitives. Particularly noteworthy is the identification of a link between CCZ equivalence and the performance of Arithmetization-Oriented primitives. This discovery has already had a tangible impact on the design of another primitive, named Arion [RST23]. The main components of the new `Anemoi` family are the `Flystel`, a nonlinear layer, and `Jive`, a compression mode, which are also of more general interest as they can be used in other schemes. It would also be particularly interesting to see whether it is possible to construct other functions CCZ-equivalent to low-degree functions, with more than two branches. Indeed, the current construction of the `Flystel` limits the use of `Anemoi` to instances with an even number of branches in the internal state. On a different subject, the $\texttt{Flystel}_{\texttt{p}}$ construction enabled us to solve the problem of finding an APN permutation over $\mathbb{F}_p^2$.

Furthermore, the security analysis of Feistel–MiMC, Poseidon or *Rescue–Prime* conducted during the challenges proposed by the Ethereum Foundation contribute to a better understanding of the behaviour of algebraic systems for some primitives currently used in the industry. Arithmetization-Oriented primitives rely on low-degree polynomial modelisation implying that algebraic attacks are often used to determine the number of rounds of these primitives. Therefore, beyond our exploration of algebraic attacks, we also present valuable suggestions for future designs. These recommendations emphasize the significance of meticulous modeling choices, exploring potential tricks to bypass rounds in substitution-permutation networks. They also point out the preference for univariate models over multivariate models whenever feasible.

Finally, the extensive analysis of the MiMC block cipher stands as a pioneering study, providing a comprehensive understanding of the evolution of the algebraic degree of this primitive. A large part of this thesis indeed focuses on the analysis of the algebraic degree of power functions when iterated with the example of the block cipher MiMC. It is important to note that this analysis to better understand the inherent properties of this cipher is quite complex but there are still many aspects to explain. Our deeper insight into the univariate representation of the polynomials used at each round of MiMC, allows us to derive precise bounds on the algebraic degree of the transformation. As a consequence, this analysis allows a more accurate assessment of the complexity of higher-order differential attacks, thus significantly enhancing the overall security evaluation of MiMC block ciphers. As a result, this analysis has already had a significant influence, inspiring several works in this direction [Liu+23a; Cui+22]. As of the current state of writing, we have not discovered a means to effectively exploit particular structures in the univariate polynomial representation for constructing distinguishers. Nonetheless, it is important to highlight that some constructions may have vulnerabilities. Notably, Gold functions are appealing inner power permutations due to their low degree and high efficiency. However, the security they provide is uncertain because they lead to a relatively sparse univariate representation. It then becomes crucial to conduct further research and analysis to better understand the security implications of these constructions. More generally, although we cannot provide precise answers to all the questions surrounding the study of the algebraic degree of these new primitives, we believe that our results can inspire and encourage future efforts to further understand the algebraic properties and implications of these new constructions.

Clearly, some aspects still require further security analysis efforts to better understand Arithmetization-Oriented primitives and identify potential vulnerabilities. Indeed, we are mainly recycling and adapting methods that are already well understood for the case of classical primitives. The question of whether we could imagine other types of attacks therefore makes perfect sense.

Open problems

We list different open problems we encountered in this thesis.

In Chapter 2

Open Problem 7.1 (Conjecture 2.1)**.** *How to determine an accurate bound for the linearity of the* $\texttt{Flystel}_p$*? Is* $p \log p$ *a good one?*

In Chapter 5

Open Problem 7.2 (Conjecture A.1)**.** *Can we determine bounds for the Hamming weight of exponents appearing in the univariate polynomials describing* MiMC_3^{-1}*? More generally, how to give a precise bound for the algebraic degree of* MiMC_3^{-1}*?*

In Chapter 6

Open Problem 7.3 (Conjecture 6.1)**.** *Can we prove that for any round* $r \geqslant 4$*, there exists one exponent of maximum weight of the form* $2^{k_{3,r}} - \alpha_{b_{3,r}}$ *where* $\alpha_{b_{3,r}} = 7$ *if* $b_{3,r} = 0$ *and* $\alpha_{b_{3,r}} = 5$ *if* $b_{3,r} = 1$.

Open Problem 7.4 (Conjecture 6.2)**.** *Is it always true that the minimum value of* $\mathcal{L}_r = \{\ell,\ 1 \leqslant \ell < r,\ \text{s.t. } k_{3,r-\ell} = k_{3,r} - k_{3,\ell}\}$ *is in* $\mathcal{P}_r = \{r_i < r \text{ s.t. } (s_1 \dots s_{r_i}) \text{ is a palindrome}\}$*?*
Similarly, is it always true that the maximum value of $\mathcal{P}_r$ *is in* $\mathcal{L}_r$*?*

Open Problem 7.5 (Observation 6.1)**.** *How to prove that for any* $r \geqslant 4, 3^r$ *is bigger than* $2^{\lfloor r \log_2 3 \rfloor} + 2^r$*?*

Open Problem 7.6 (Observation 6.2)**.** *Can we express each element of* $\mathbb{Z}/3^t\mathbb{Z}$*, for any* t*, as a sum of at most* $2t+1$ *powers of* 4*, i.e. a sum of* 4^i *for* $i \in \{2, \dots 2t+2\}$*?*

Bibliography

[AD18] Tomer Ashur and Siemen Dhooghe. *MARVELlous: a STARK-Friendly Family of Cryptographic Primitives.* Cryptology ePrint Archive, Report 2018/1098. https://eprint.iacr.org/2018/1098. 2018 (cit. on pp. 17, 21).

[Alb+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. “Ciphers for MPC and FHE”. In: *EUROCRYPT 2015, Part I.* Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9056. LNCS. Springer, Heidelberg, Apr. 2015, pp. 430–454 (cit. on p. 28).

[Alb+16] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. “MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity”. In: *ASIACRYPT 2016, Part I.* Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Vol. 10031. LNCS. Springer, Heidelberg, Dec. 2016, pp. 191–219 (cit. on pp. 10, 17, 19, 35, 86, 107, 214, 218).

[Alb+19a] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. “Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC”. In: *ASIACRYPT 2019, Part III.* Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11923. LNCS. Springer, Heidelberg, Dec. 2019, pp. 371–397 (cit. on p. 21).

[Alb+19b] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. “Feistel Structures for MPC, and More”. In: *ESORICS 2019, Part II.* Ed. by Kazue Sako, Steve Schneider, and Peter Y. A. Ryan. Vol. 11736. LNCS. Springer, Heidelberg, Sept. 2019, pp. 151–171 (cit. on pp. 17, 19, 62).

[Aly+19] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. *Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols.* Cryptology ePrint Archive, Report 2019/426. https://eprint.iacr.org/2019/426. 2019 (cit. on p. xvii).

[Aly+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. “Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols”. In: *IACR Trans. Symm. Cryptol.* 2020.3 (2020), pp. 1–45. ISSN: 2519-173X (cit. on pp. 17, 22, 35, 80, 85, 93).

[AM09] Jean-Philippe Aumasson and Willi Meier. *Zero-sum distinguishers for reduced Keccak-f and for the core functions of Luffa and Hamsi.* Rump session of Cryptographic Hardware and Embedded Systems-CHES. 2009 (cit. on p. 214).

[Amb+22] Miguel Ambrona, Anne-Laure Schmitt, Raphael R. Toledo, and Danny Willems. *New optimization techniques for PlonK’s arithmetization.* Cryptology ePrint Archive, Report 2022/462. https://eprint.iacr.org/2022/462. 2022 (cit. on p. 79).

[AMT22] Tomer Ashur, Mohammad Mahzoun, and Dilara Toprakhisar. “Chaghri - A FHE-friendly Block Cipher”. In: *ACM CCS 2022.* Ed. by Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi. ACM Press, Nov. 2022, pp. 139–150 (cit. on pp. 28, 218, 228).

[Bar+22] Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, and Léo Perrin. “Algebraic attacks against some arithmetization-oriented primitives”. In: *IACR Trans. Symm. Cryptol.* (2022), pp. 73–101 (cit. on pp. 83, 307).

[BC13] Christina Boura and Anne Canteaut. “On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$”. In: *IEEE Trans. Inf. Theory* Vol. 59.1 (2013), pp. 691–702 (cit. on pp. 145, 202, 212).

[BC90] Jurjen N. Bos and Matthijs J. Coster. “Addition Chain Heuristics”. In: *CRYPTO’89*. Ed. by Gilles Brassard. Vol. 435. LNCS. Springer, Heidelberg, Aug. 1990, pp. 400–407 (cit. on p. 74).

[BCP06] Lilya Budaghyan, Claude Carlet, and Alexander Pott. “New classes of almost bent and almost perfect nonlinear polynomials”. In: *IEEE Trans. Inf. Theory* Vol. 52.3 (2006), pp. 1141–1152 (cit. on pp. 32, 33).

[BCP23] Clémence Bouvier, Anne Canteaut, and Léo Perrin. “On the algebraic degree of iterated power functions”. In: *Designs, Codes and Cryptography* (2023), pp. 997–1033 (cit. on pp. 107, 108, 310).

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. “The Magma algebra system. I. The user language”. In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171 (cit. on p. 97).

[Bei+20] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. “Lightweight AEAD and Hashing using the Sparkle Permutation Family”. In: *IACR Trans. Symm. Cryptol.* 2020.S1 (2020), pp. 208–261. ISSN: 2519-173X (cit. on p. 70).

[Ben+13] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. “SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge”. In: *CRYPTO 2013, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. LNCS. Springer, Heidelberg, Aug. 2013, pp. 90–108 (cit. on pp. 11, 12).

[Ben+18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. *Scalable, transparent, and post-quantum secure computational integrity*. Cryptology ePrint Archive, Report 2018/046. `https://eprint.iacr.org/2018/046`. 2018 (cit. on pp. 11, 16, 80).

[Ber+07] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. “Sponge functions”. In: *ECRYPT hash workshop*. 9. `https://csrc.nist.rip/groups/ST/hash/documents/JoanDaemen.pdf`. 2007 (cit. on pp. 7, 62, 63).

[Ber+11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. *Cryptographic Sponge functions*. `keccak.team/files/CSF-0.1.pdf`. 2011 (cit. on p. 84).

[Ber08a] Daniel J Bernstein. *ChaCha, a variant of Salsa20*. `http://cr.yp.to/chacha.html`. 2008 (cit. on pp. 61, 64).

[Ber08b] Daniel J Bernstein. “The Salsa20 family of stream ciphers”. In: *New stream cipher designs*. Springer, 2008, pp. 84–97 (cit. on pp. 61, 64).

[Bey+20a] Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer. “Out of Oddity - New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems”. In: *CRYPTO 2020, Part III*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12172. LNCS. Springer, Heidelberg, Aug. 2020, pp. 299–328 (cit. on p. 75).

[Bey+20b] Tim Beyne, Anne Canteaut, Gregor Leander, María Naya-Plasencia, Léo Perrin, and Friedrich Wiemer. *On the security of the Rescue hash function*. Cryptology ePrint Archive, Report 2020/820. `https://eprint.iacr.org/2020/820`. 2020 (cit. on p. 38).

[BFS04] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. “On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations”. In: *Proceedings of the International Conference on Polynomial System Solving*. 2004, pp. 71–74 (cit. on pp. 85, 98).

[BFS15] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. “On the complexity of the F5 Gröbner basis algorithm”. In: *Journal of Symbolic Computation* Vol. 70 (2015), pp. 49–70 (cit. on pp. 85, 99).

[Bou+23] Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. "New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode". In: *CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. LNCS. Springer, 2023, pp. 507–539 (cit. on pp. 17, 31, 54, 65, 67, 79, 101, 306).

[Bou22a] Clémence Bouvier. *New Approach for Arithmetization-Oriented Symmetric Primitives*. CrossFyre Workshop. Passau, Germany. https://crossfyre22.github.io/docs/Bouvier.pdf. Oct. 2022.

[Bou22b] Clémence Bouvier. *On the Algebraic Degree of Iterated Power Functions*. WCC - Workshop on Coding and Cryptography. Virtual (Rostock, Germany). https://www.wcc2022.uni-rostock.de/storages/uni-rostock/Tagungen/WCC2022/Papers/WCC_2022_paper_47.pdf. Mar. 2022.

[Bou23] Clémence Bouvier. *Iterated Power Functions: from Univariate Polynomial Representation to Multivariate Degree*. Fq15 - International Conference on Finite Fields and Their Applications. Aubervilliers, France. https://org.uib.no/selmer/fq15/abstracts.pdf. June 2023 (cit. on p. 107).

[BP23] Lilya Budaghyan and Mohit Pal. *Arithmetization-Oriented APN Functions*. Cryptology ePrint Archive, Paper 2023/1081. https://eprint.iacr.org/2023/1081. 2023 (cit. on p. 60).

[BR22] Tim Beyne and Vincent Rijmen. "Differential Cryptanalysis in the Fixed-Key Model". In: *CRYPTO 2022, Part III*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13509. LNCS. Springer, Heidelberg, Aug. 2022, pp. 687–716 (cit. on p. 8).

[Bro+10] Keith A. Browning, John F. Dillon, M. T. McQuistan, and Alan J. Wolfe. "An APN Permutation in Dimension Six". In: *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications*. Vol. 518. American Mathematical Society, 2010, pp. 33–42 (cit. on p. 36).

[Bro+21] Olivier Bronchain, Sebastian Faust, Virginie Lallemand, Gregor Leander, Léo Perrin, and François-Xavier Standaert. "MOE: Multiplication Operated Encryption with Trojan Resilience". In: *IACR Trans. Symm. Cryptol.* Vol. 2021.1 (Mar. 2021), pp. 78–129 (cit. on p. 166).

[BS91] Eli Biham and Adi Shamir. "Differential Cryptanalysis of DES-like Cryptosystems". In: *CRYPTO'90*. Ed. by Alfred J. Menezes and Scott A. Vanstone. Vol. 537. LNCS. Springer, Heidelberg, Aug. 1991, pp. 2–21 (cit. on p. 7).

[BSV07] Thomas Baignères, Jacques Stern, and Serge Vaudenay. "Linear Cryptanalysis of Non Binary Ciphers". In: *SAC 2007*. Ed. by Carlisle M. Adams, Ali Miri, and Michael J. Wiener. Vol. 4876. LNCS. Springer, Heidelberg, Aug. 2007, pp. 184–211 (cit. on p. 75).

[Buc76] Bruno Buchberger. "A theoretical basis for the reduction of polynomials to canonical forms". In: *ACM SIGSAM Bulletin* Vol. 10.3 (1976), pp. 19–29 (cit. on p. 85).

[Bün+18] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. "Bulletproofs: Short Proofs for Confidential Transactions and More". In: *2018 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2018, pp. 315–334 (cit. on p. 12).

[BW22] Clémence Bouvier and Danny Willems. *Anemoi and Jive : New Arithmetization-Oriented tools for Plonk-based applications*. ZKProof5 - Zero-Knowledge Proofs. Tel Aviv, Israel. https://youtu.be/3EdbLiC1FPI. Nov. 2022.

[Can+18] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. "Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression". In: *Journal of Cryptology* 31.3 (July 2018), pp. 885–916 (cit. on p. 28).

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. "Codes, bent functions and permutations suitable for DES-like cryptosystems". In: *Designs, Codes and Cryptography* Vol. 15.2 (1998), pp. 125–156 (cit. on p. 32).

[CDP17] Anne Canteaut, Sébastien Duval, and Léo Perrin. “A Generalisation of Dillon’s APN Permutation With the Best Known Differential and Nonlinear Properties for All Fields of Size 2^{4k+2}”. In: *IEEE Trans. Inf. Theory* Vol. 63.11 (Nov. 2017), pp. 7575–7591 (cit. on pp. 36, 38, 54).

[Cha13] Pascale Charpin. “Handbook of Finite Fields”. In: CRC Press, 2013. Chap. PN and APN functions (cit. on p. 2).

[CP02] Nicolas Courtois and Josef Pieprzyk. “Cryptanalysis of Block Ciphers with Overdefined Systems of Equations”. In: *ASIACRYPT 2002*. Ed. by Yuliang Zheng. Vol. 2501. LNCS. Springer, Heidelberg, Dec. 2002, pp. 267–287 (cit. on p. 10).

[CP19] Anne Canteaut and Léo Perrin. “On CCZ-equivalence, extended-affine equivalence, and function twisting”. In: *Finite Fields and Their Applications* Vol. 56 (2019), pp. 209–246 (cit. on p. 34).

[CPT19] Anne Canteaut, Léo Perrin, and Shizhu Tian. “If a generalised butterfly is APN then it operates on 6 bits”. In: *Cryptography and Communications* Vol. 11.6 (2019), pp. 1147–1164 (cit. on p. 36).

[Cui+22] Jiamin Cui, Kai Hu, Meiqin Wang, and Puwen Wei. “On the Field-Based Division Property: Applications to MiMC, Feistel MiMC and GMiMC”. In: *ASIACRYPT 2022, Part III*. Ed. by Shweta Agrawal and Dongdai Lin. Vol. 13793. LNCS. Springer, Heidelberg, Dec. 2022, pp. 241–270 (cit. on pp. 123, 124, 255, 311).

[Dae95] Joan Daemen. *Cipher and hash function design, strategies based on linear and differential cryptanalysis, PhD Thesis*. `http://jda.noekeon.org/`. K.U.Leuven, 1995 (cit. on p. 67).

[Dam90] Ivan Damgård. “A Design Principle for Hash Functions”. In: *CRYPTO’89*. Ed. by Gilles Brassard. Vol. 435. LNCS. Springer, Heidelberg, Aug. 1990, pp. 416–427 (cit. on pp. 6, 64).

[Das02] Pinaki Das. “The Number of Permutation Polynomials of a Given Degree Over a Finite Field”. In: *Finite Fields and Their Applications* Vol. 8.4 (2002), pp. 478–490 (cit. on p. 10).

[DG10] Vivien Dubois and Nicolas Gama. “The Degree of Regularity of HFE Systems”. In: *ASIACRYPT 2010*. Ed. by Masayuki Abe. Vol. 6477. LNCS. Springer, Heidelberg, Dec. 2010, pp. 557–576 (cit. on p. 85).

[Dil06] John F. Dillon. *APN Polynomials and Related Codes*. Workshop on Polynomials over Finite Fields and Their Applications, Banff International Research Station (BIRS). Alberta, Canada. Nov. 2006 (cit. on p. 32).

[DL18] Sébastien Duval and Gaëtan Leurent. “MDS Matrices with Lightweight Circuits”. In: *IACR Trans. Symm. Cryptol.* 2018.2 (2018), pp. 48–78. ISSN: 2519-173X (cit. on pp. 23, 68).

[Dob+18] Christoph Dobraunig, Maria Eichlseder, Lorenzo Grassi, Virginie Lallemand, Gregor Leander, Eik List, Florian Mendel, and Christian Rechberger. “Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit”. In: *CRYPTO 2018, Part I*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10991. LNCS. Springer, Heidelberg, Aug. 2018, pp. 662–692 (cit. on p. 28).

[Dob+21] Christoph Dobraunig, Lorenzo Grassi, Anna Guinet, and Daniël Kuijsters. “Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields”. In: *EUROCRYPT 2021, Part II*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12697. LNCS. Springer, Heidelberg, Oct. 2021, pp. 3–34 (cit. on pp. 29, 85, 98).

[Dob+23] Christoph Dobraunig, Lorenzo Grassi, Lukas Helminger, Christian Rechberger, Markus Schofnegger, and Roman Walch. “Pasta: A Case for Hybrid Homomorphic Encryption”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* Vol. 2023.3 (2023), pp. 30–73 (cit. on p. 28).

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Berlin, Heidelberg, New York: Springer Verlag, Aug. 29, 2002. ISBN: 3-540-42580-2 (cit. on p. 5).

[Eic+20] Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, and Qingju Wang. "An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC". In: *ASIACRYPT 2020, Part I*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12491. LNCS. Springer, Heidelberg, Dec. 2020, pp. 477–506 (cit. on pp. 108, 109, 121, 149, 211–214, 216, 308).

[Fau+14] Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaël Renault. "Sub-cubic change of ordering for Gröbner basis: a probabilistic approach". In: *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*. 2014, pp. 170–177 (cit. on p. 85).

[Fau+93] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. "Efficient computation of zero-dimensional Gröbner bases by change of ordering". In: *Journal of Symbolic Computation* Vol. 16.4 (1993), pp. 329–344 (cit. on p. 85).

[FM17] Jean-Charles Faugère and Chenqi Mou. "Sparse FGLM algorithms". In: *Journal of Symbolic Computation* Vol. 80 (2017), pp. 538–569 (cit. on p. 85).

[Fou21] Ethereum Foundation. *ZK Hash Function Cryptanalysis Bounties*. Available online at https://www.zkhashbounties.info/. 2021 (cit. on pp. 83, 86).

[Gam+20] Gerald Gamrath, Daniel Anderson, Ksenia Bestuzheva, Wei-Kun Chen, Leon Eifler, Maxime Gasse, Patrick Gemander, Ambros Gleixner, Leona Gottwald, Katrin Halbig, Gregor Hendel, Christopher Hojny, Thorsten Koch, Pierre Le Bodic, Stephen J. Maher, Frederic Matter, Matthias Miltenberger, Erik Mühmer, Benjamin Müller, Marc E. Pfetsch, Franziska Schlösser, Felipe Serrano, Yuji Shinano, Christine Tawfik, Stefan Vigerske, Fabian Wegscheider, Dieter Weninger, and Jakob Witzig. *The SCIP Optimization Suite 7.0*. ZIB-Report 20-10. http://nbn-resolving.de/urn:nbn:de:0297-zib-78023. Zuse Institute Berlin, Mar. 2020 (cit. on p. 166).

[GKS23] Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger. "Poseidon2: A Faster Version of the Poseidon Hash Function". In: *AFRICACRYPT 2023*. Ed. by Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne. Springer, 2023, pp. 177–203 (cit. on pp. 17, 20).

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The knowledge complexity of interactive proof-systems". In: *Symposium on the Theory of Computing*. 1985 (cit. on p. xiv).

[Gol68] Robert Gold. "Maximal recursive sequences with 3-valued recursive crosscorrelation functions". In: *IEEE Transactions on Information Theory* Vol. 14 (1968), pp. 154–156 (cit. on p. 116).

[Gra+20] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. "On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy". In: *EUROCRYPT 2020, Part II*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12106. LNCS. Springer, Heidelberg, May 2020, pp. 674–704 (cit. on p. 19).

[Gra+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. "Poseidon: A New Hash Function for Zero-Knowledge Proof Systems". In: *USENIX Security 2021*. Ed. by Michael Bailey and Rachel Greenstadt. USENIX Association, Aug. 2021, pp. 519–535 (cit. on pp. 17, 19, 35, 62, 76, 78, 85, 92, 96).

[Gra+22a] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. "Reinforced Concrete: A Fast Hash Function for Verifiable Computation". In: *ACM CCS 2022*. Ed. by Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi. ACM Press, Nov. 2022, pp. 1323–1335 (cit. on pp. 17, 25, 62, 79).

[Gra+22b] Lorenzo Grassi, Silvia Onofri, Marco Pedicini, and Luca Sozzi. "Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$: Application to Poseidon". In: *IACR Trans. Symm. Cryptol.* 2022.3 (2022), pp. 20–72 (cit. on pp. 17, 20).

[Gra+23a] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. "Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications". In: *CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. LNCS. Springer, 2023, pp. 573–606 (cit. on pp. 17, 23).

[Gra+23b] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. *Hash Functions Monolith for ZK Applications: May the Speed of SHA-3 be With You*. Cryptology ePrint Archive, Paper 2023/1025. https://eprint.iacr.org/2023/1025. 2023 (cit. on pp. 17, 27).

[Gro16] Jens Groth. "On the Size of Pairing-Based Non-interactive Arguments". In: *EUROCRYPT 2016, Part II*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9666. LNCS. Springer, Heidelberg, May 2016, pp. 305–326 (cit. on pp. 11, 12).

[GW20] Ariel Gabizon and Zachary J. Williamson. *plookup: A simplified polynomial protocol for lookup tables*. Cryptology ePrint Archive, Report 2020/315. https://eprint.iacr.org/2020/315. 2020 (cit. on p. 79).

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. *PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge*. Cryptology ePrint Archive, Report 2019/953. https://eprint.iacr.org/2019/953. 2019 (cit. on p. 13).

[Her36] Aaron Herschfeld. "The equation $2^x - 3^y = d$". In: *Bull. Amer. Math. Soc.* Vol. 42.4 (Apr. 1936), pp. 231–234 (cit. on p. 124).

[Hir16] Shoichi Hirose. "Sequential Hashing with Minimum Padding". In: *NIST Workshop on Lightweight Cryptography 2016*. National Institute of Standards and Technology (NIST). 2016 (cit. on pp. 62, 63).

[Knu95] Lars R. Knudsen. "Truncated and Higher Order Differentials". In: *FSE'94*. Ed. by Bart Preneel. Vol. 1008. LNCS. Springer, Heidelberg, Dec. 1995, pp. 196–211 (cit. on pp. 10, 75).

[KP02] Sergei Konyagin and Francesco Pappalardi. "Enumerating Permutation Polynomials over Finite Fields by Degree". In: *Finite Fields and Their Applications* Vol. 8.4 (2002), pp. 548–553 (cit. on p. 10).

[Lai94] Xuejia Lai. "Higher Order Derivatives and Differential Cryptanalysis". In: *Communications and Cryptography: Two Sides of One Tapestry*. Ed. by Richard E. Blahut, Daniel J. Costello, Ueli Maurer, and Thomas Mittelholzer. Boston, MA: Springer US, 1994, pp. 227–233. ISBN: 978-1-4615-2694-0 (cit. on p. 10).

[Lea+11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. "A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack". In: *CRYPTO 2011*. Ed. by Phillip Rogaway. Vol. 6841. LNCS. Springer, Heidelberg, Aug. 2011, pp. 206–221 (cit. on p. 10).

[Li+18] Yongqiang Li, Shizhu Tian, Yuyin Yu, and Mingsheng Wang. "On the Generalization of Butterfly Structure". In: *IACR Trans. Symm. Cryptol.* 2018.1 (2018), pp. 160–179. ISSN: 2519-173X (cit. on pp. 36, 54, 55, 57, 59).

[Liu+22] Jianwei Liu, Harshad Patil, Akhil Sai Peddireddy, Kevin Singh, Haifeng Sun, Huachuang Sun, and Weikeng Chen. *An efficient verifiable state for zk-EVM and beyond from the Anemoi hash function*. Cryptology ePrint Archive, Report 2022/1487. https://eprint.iacr.org/2022/1487. 2022 (cit. on pp. 82, 255, 311).

[Liu+23a] Fukang Liu, Ravi Anand, Libo Wang, Willi Meier, and Takanori Isobe. "Coefficient Grouping: Breaking Chaghri and More". In: *EUROCRYPT 2023, Part IV*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. LNCS. Springer, Heidelberg, Apr. 2023, pp. 287–317 (cit. on pp. 28, 123, 219, 220, 222, 255, 311).

[Liu+23b] Fukang Liu, Lorenzo Grassi, Clémence Bouvier, Willi Meier, and Takanori Isobe. "Coefficient Grouping for Complex Affine Layers". In: *CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. LNCS. Springer, 2023, pp. 540–572 (cit. on pp. 217, 218, 220, 222, 224, 227, 310).

[LW14] Yongqiang Li and Mingsheng Wang. "Constructing S-boxes for Lightweight Cryptography with Feistel Structure". In: *CHES 2014*. Ed. by Lejla Batina and Matthew Robshaw. Vol. 8731. LNCS. Springer, Heidelberg, Sept. 2014, pp. 127–146 (cit. on p. 47).

[Mat94] Mitsuru Matsui. “Linear Cryptanalysis Method for DES Cipher”. In: *EUROCRYPT’93*. Ed. by Tor Helleseth. Vol. 765. LNCS. Springer, Heidelberg, May 1994, pp. 386–397 (cit. on p. 8).

[McE87] Robert J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Springer Verlag, 1987. ISBN: 978-1-4613-1983-2 (cit. on p. 116).

[McL21] Michael B. McLoughlin. *addchain: Cryptographic Addition Chain Generation in Go*. Repository https://github.com/mmcloughlin/addchain. Version 0.4.0. https://doi.org/10.5281/zenodo.5622943. Oct. 2021 (cit. on p. 74).

[Mer90] Ralph C. Merkle. “One Way Hash Functions and DES”. In: *CRYPTO’89*. Ed. by Gilles Brassard. Vol. 435. LNCS. Springer, Heidelberg, Aug. 1990, pp. 428–446 (cit. on p. 6).

[Mid22] Polygon Miden. *Miden*. Repository https://github.com/maticnetwork/miden. Version 0.2.0. Sept. 2022 (cit. on p. 76).

[Nat15] National Institute of Standards and Technology. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. NIST FIPS PUB 202, U.S. Department of Commerce. 2015 (cit. on p. 62).

[Nat22] National Institute of Standards and Technology. *Secure Hash Standard*. NIST FIPS PUB 180-2, U.S. Department of Commerce. Apr. 2022 (cit. on p. 7).

[Nat77] National Bureau of Standards. *Data Encryption Standard*. NBS FIPS PUB 46, U.S. Department of Commerce. Jan. 1977 (cit. on p. 5).

[Nat95] National Institute of Standards and Technology. *Secure Hash Standard*. NIST FIPS PUB 180-1, U.S. Department of Commerce. Apr. 1995 (cit. on p. 7).

[Nyb94] Kaisa Nyberg. “Differentially Uniform Mappings for Cryptography”. In: *EUROCRYPT’93*. Ed. by Tor Helleseth. Vol. 765. LNCS. Springer, Heidelberg, May 1994, pp. 55–64 (cit. on p. 131).

[Pre11] Bart Preneel. “Davies–Meyer”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 312–313 (cit. on p. 64).

[PUB16] Léo Perrin, Aleksei Udovenko, and Alex Biryukov. “Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem”. In: *CRYPTO 2016, Part II*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9815. LNCS. Springer, Heidelberg, Aug. 2016, pp. 93–122 (cit. on pp. 31, 36, 54, 304).

[Rec23] Christian Rechberger. *On the history of FHEMPCZK-friendly symmetric crypto*. STAP (Symmetric Techniques for Advanced Protocols). https://who.paris.inria.fr/Leo.Perrin/rescale/slides/Christian-STAP-2023.pdf. 2023 (cit. on p. 18).

[RST23] Arnab Roy, Matthias Johann Steiner, and Stefano Trevisani. *Arion: Arithmetization-Oriented Permutation and Hashing from Generalized Triangular Dynamical Systems*. 2023. arXiv: 2303.04639 [cs.CR] (cit. on pp. 17, 24, 60, 255, 311).

[SAD20] Alan Szepieniec, Tomer Ashur, and Siemen Dhooghe. *Rescue-Prime: a Standard Specification (SoK)*. Cryptology ePrint Archive, Report 2020/1143. https://eprint.iacr.org/2020/1143. 2020 (cit. on pp. 17, 22, 62, 93, 97).

[Sag22] The Sage Developers. *SageMath, the Sage Mathematics Software System*. Version 9.5. DOI 10.5281/zenodo.6259615. 2022 (cit. on p. 96).

[Sal23] Robin Salen. *Two additional instantiations from the Tip5 hash function construction*. https://toposware.com/paper_tip5.pdf. 2023 (cit. on pp. 17, 27).

[Sch80] Jacob Theodore Schwartz. “Fast Probabilistic Algorithms for Verification of Polynomial Identities”. In: *J. ACM* 27.4 (Oct. 1980), pp. 701–717. ISSN: 0004-5411 (cit. on p. 15).

[Sha49] Claude Elwood Shannon. “Communication theory of secrecy systems”. In: *The Bell System Technical Journal* Vol. 28.4 (1949), pp. 656–715 (cit. on p. 5).

[Sho] Victor Shoup. *NTL: A library for doing number theory*. https://libntl.org/ (cit. on p. 96).

[Sze+23] Alan Szepieniec, Alexander Lemmens, Jan Ferdinand Sauer, and Bobbin Threadbare. *The Tip5 Hash Function for Recursive STARKs*. Cryptology ePrint Archive, Report 2023/107. `https://eprint.iacr.org/2023/107`. 2023 (cit. on pp. 17, 27).

[Sze21] Alan Szepieniec. *On the Use of the Legendre Symbol in Symmetric Cipher Design*. Cryptology ePrint Archive, Report 2021/984. `https://eprint.iacr.org/2021/984`. 2021 (cit. on pp. 17, 22).

[TG92] Anne Tardy-Corfdir and Henri Gilbert. "A Known Plaintext Attack of FEAL-4 and FEAL-6". In: *CRYPTO'91*. Ed. by Joan Feigenbaum. Vol. 576. LNCS. Springer, Heidelberg, Aug. 1992, pp. 172–181 (cit. on p. 8).

[TLS19] Yosuke Todo, Gregor Leander, and Yu Sasaki. "Nonlinear invariant attack: practical attack on full SCREAM, i SCREAM, and Midori 64". In: *Journal of Cryptology* Vol. 32 (2019), pp. 1383–1422 (cit. on p. 10).

[Ver26] Gilbert Sandford Vernam. "Cipher printing telegraph systems: For secret wire and radio telegraphic communications". In: *Journal of the A.I.E.E.* Vol. 45.2 (1926), pp. 109–115 (cit. on pp. xiv, 3).

[Wel69] Charles Wells. "The degrees of permutation polynomials over finite fields". In: *Journal of Combinatorial Theory* Vol. 7.1 (1969), pp. 49–55 (cit. on p. 10).

[Zer22] Polygon Zero. *Plonky2*. Repository `https://github.com/mir-protocol/plonky2`. Sept. 2022 (cit. on p. 76).

[Zha+14] Zhengbang Zha, Lei Hu, Siwei Sun, and Yao Sun. "New constructions of APN polynomial functions in odd characteristic". In: *Applicable Algebra in Engineering, Communication and Computing* Vol. 25 (Aug. 2014) (cit. on p. 56).

[Zip79] Richard Zippel. "Probabilistic Algorithms for Sparse Polynomials". In: *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*. EUROSAM '79. Berlin, Heidelberg: Springer-Verlag, 1979, pp. 216–226. ISBN: 3540095195 (cit. on p. 15).

Appendix A

Bound on the Hamming weight of js

In order to get a more accurate bound on the algebraic degree of MiMC_3^{-1} for a larger number of rounds, we need to study in more details the exponents $js \bmod (2^n-1)$ not only for $j \preceq s$. Therefore, in this section our aim is to investigate some directions to establish, in light of Section 5.4.1, a link between the Hamming weight of exponents js and exponents j. First, let us observe that for $\mathrm{wt}(j)=0,1,n-1$, we have respectively $\mathrm{wt}(js)=0,\frac{n+1}{2},\frac{n-1}{2}$. The cases where $\mathrm{wt}(j)=0,1$ have been discussed in Section 5.4.1. Then if $\mathrm{wt}(j)=n-1$, we have $j=2^n-2^i-1$ where $0\leqslant i\leqslant n-1$. Noting that $(2^n-2^i-1)s=-2^is \bmod (2^n-1)$, if i is even we have:

$$(2^n-2^i-1)s=-\sum_{\ell=i/2}^{(n+i-1)/2}2^{2l}\equiv\mathcal{E}_0^{i-2}+\mathcal{O}_i^{n-3} \bmod (2^n-1)\,,$$

and if i is odd, we have:

$$(2^n-2^i-1)s=-\sum_{\ell=(i-1)/2}^{(n+i-2)/2}2^{2l+1}\equiv\mathcal{O}_0^{i-3}+\mathcal{E}_{i+1}^{n-1} \bmod (2^n-1)\,.$$

In both cases, we have $\mathrm{wt}\left((2^n-2^i-1)s \bmod (2^n-1)\right)=\frac{n-1}{2}$.

Therefore it remains to investigate cases such that $\mathrm{wt}(j)\notin\{0,1,n-1\}$. In particular, our aim is to prove that the following conjecture is true for j of low Hamming weight.

Conjecture A.1. *Let j be an integer such that $2\leqslant j\leqslant 2^n-2$, then*

$$\mathrm{wt}\,(js \bmod (2^n-1))\in\begin{cases}[\![\mathrm{wt}(j)/2,(n+\mathrm{wt}(j)-3)/2]\!] & \textit{if } \mathrm{wt}(j)=0 \bmod 2\\ [\![(\mathrm{wt}(j)+3)/2,(n+\mathrm{wt}(j))/2]\!] & \textit{if } \mathrm{wt}(j)=1 \bmod 2\,.\end{cases}$$

Using some ideas from the proof of the existence of a plateau between the first two rounds of MiMC_3^{-1} (see Section 5.4.1), we can prove this conjecture for integers j when $\mathrm{wt}(j)\in\{2,3,4,5\}$ (see Proposition A.1). We could expect to build an inductive proof for the case $\mathrm{wt}(j)\equiv 0 \bmod 2$, starting from $\mathrm{wt}(j)=2$, and for the case $\mathrm{wt}(j)\equiv 1 \bmod 2$ starting from the case $\mathrm{wt}(j)=3$. However, given the expressions of js when $\mathrm{wt}(j)=4$ or $\mathrm{wt}(j)=5$, it seems difficult to find such a relation. Indeed, if $j=\sum_{\alpha=0}^{\mathrm{wt}(j)-1}2^{i_\alpha}$, then the Hamming weight of js depends on the parity of the exponents i_α. Therefore $2^{\mathrm{wt}(j)}$ different cases must be investigated. Finding a way to automate these calculations is then an interesting problem.

Using Lemmas 5.8 and 5.9 we can then prove the following proposition.

Proposition A.1. *Let j be an integer such that $\mathrm{wt}(j)\in\{2,3,4,5\}$. Then*

$$\mathrm{wt}\,(js \bmod (2^n-1))\in\begin{cases}[\![\mathrm{wt}(j)/2,(n+\mathrm{wt}(j)-3)/2]\!] & \textit{if } \mathrm{wt}(j)\in\{2,4\}\\ [\![(\mathrm{wt}(j)+3)/2,(n+\mathrm{wt}(j))/2]\!] & \textit{if } \mathrm{wt}(j)\in\{3,5\}\,.\end{cases}$$

Proof. In the proof, we rely on the exact representation of each exponent js. We first investigate the case $\mathrm{wt}(j) = 2$ and we construct all the corresponding exponents js from which we deduce bounds on $\mathrm{wt}(js)$. By induction, we study the case $\mathrm{wt}(j) = 3$, then the case $\mathrm{wt}(j) = 4$ and finally the case $\mathrm{wt}(j) = 5$. Each time we double the number of subcases since we need to consider the parity of each exponent of the powers of 2 representing j.

Let $j = \sum_{\alpha=0}^{\mathrm{wt}(j)-1} 2^{i_\alpha}$. In the following we will denote $\mathcal{S}_{(i_\alpha \bmod 2)_{1\leqslant\alpha\leqslant\mathrm{wt}(j)-1}}$ the result of $sj \bmod (2^n - 1)$. Without loss of generality, we can assume that $i_0 = 0$. For example, if $j = 1 + 2^{i_1} + 2^{i_2}$ where i_1 is odd and i_2 is even, then $sj \bmod (2^n - 1) = \mathcal{S}_{(1,0)}$. In particular, let us notice that

$$\mathcal{S}_{(i_\alpha \bmod 2)_{1\leqslant\alpha\leqslant\mathrm{wt}(j)-1}} = s \times \sum_{\alpha=0}^{\mathrm{wt}(j)-1} 2^{i_\alpha} = s \times \sum_{\alpha=0}^{\mathrm{wt}(j)-2} 2^{i_\alpha} + s \times 2^{i_{\mathrm{wt}(j)-1}}\,,$$

leading to

$$\mathcal{S}_{(i_\alpha \bmod 2)_{1\leqslant\alpha\leqslant\mathrm{wt}(j)-1}} \equiv \mathcal{S}_{(i_\alpha \bmod 2)_{1\leqslant\alpha\leqslant\mathrm{wt}(j)-2}} + s \times 2^{i_{\mathrm{wt}(j)-1}} \bmod (2^n - 1)\,.$$

First, let j be such that $\mathrm{wt}(j) = 2$ with $j = 1 + 2^{i_1}$ and where $1 \leqslant i_1 \leqslant n - 1$.

- If i_1 is even, then we have computed in the proof of Proposition 5.13 (see Equation (5.4) page 139) that
$$\mathcal{S}_{(0)} = 2^{i_1} + \mathcal{O}_{i_1}^{n-3}$$
so that
$$\mathrm{wt}(\mathcal{S}_{(0)}) = (n - i_1 + 1)/2\,,$$
where $i_1 \in [\![2, n-1]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(0)}) \in [\![1, (n-1)/2]\!]$.

- If i_1 is odd, then:
$$\begin{aligned}
\mathcal{S}_{(1)} &= \mathcal{E}_0^{n-1} + \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{n-3} \\
&= 2 \cdot \mathcal{E}_0^{i_1-1} + \mathcal{E}_{i_1+1}^{n-1} + \mathcal{O}_{i_1-1}^{n-3} \\
&= \mathcal{O}_0^{i_1-1} + 2^{i_1} + \mathcal{A}_{i_1+1}^{n-1} && \text{by Lemma 5.9 (iii) and (i)} \\
&= \mathcal{O}_0^{i_1-3} + 2^{i_1+1} + \mathcal{A}_{i_1+1}^{n-1} \\
&= 1 + \mathcal{O}_0^{i_1-3} && \text{by Lemma 5.9 (iv)}\,,
\end{aligned}$$
so that
$$\mathrm{wt}(\mathcal{S}_{(1)}) = 1 + (i_1 - 3 + 2)/2 = (i_1 + 1)/2\,,$$
where $i_1 \in [\![1, n-2]\!]$, implying $\mathrm{wt}(\mathcal{S}_{(1)}) \in [\![1, (n-1)/2]\!]$.

We summarize the results in Table A.1. Therefore, we have $\mathrm{wt}(sj) \in [\![1, (n-1)/2]\!]$.

$i_1 \bmod 2$	$\mathrm{wt}\,(sj \bmod (2^n - 1))$	$[\![\min, \max]\!]$
0	$(n - i_1 + 1)/2$	$[\![1, \frac{n-1}{2}]\!]$
1	$(i_1 + 1)/2$	$[\![1, \frac{n-1}{2}]\!]$

Table A.1: $\mathrm{wt}(js)$ *for* $j = 1 + 2^{i_1}$.

Then let j be such that $\mathrm{wt}(j) = 3$, with $j = 1 + 2^{i_1} + 2^{i_2}$ and where $1 \leqslant i_1 < i_2 \leqslant n - 1$.

- If i_1 and i_2 are even, we deduce from Remark 5.3 that:

  $$\mathcal{S}_{(0,0)} = 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} ,$$

  so that

  $$\mathrm{wt}(\mathcal{S}_{(0,0)}) = 1 + (i_1 - 2 + 2)/2 + (i_2 - 2 - i_1 + 2)/2 = (i_2 + 2)/2 ,$$

  where $i_2 \in [\![4, n-1]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(0,0)}) \in [\![3, (n+1)/2]\!]$.

- If i_1 is even and i_2 odd, then:

  $$\begin{aligned}\mathcal{S}_{(0,1)} &= \mathcal{S}_{(0)} + \mathcal{E}_0^{i_2-1} + \mathcal{O}_{i_2-1}^{n-3}\\ &= 2^{i_1} + \mathcal{O}_{i_1}^{n-3} + \mathcal{E}_0^{i_2-1} + \mathcal{O}_{i_2-1}^{n-3}\\ &= \mathcal{E}_0^{i_1-2} + (2^{i_1} + \mathcal{O}_{i_1}^{i_2-1} + \mathcal{E}_{i_1}^{i_2-1}) + \mathcal{O}_{i_2+1}^{n-3} + \mathcal{O}_{i_2-1}^{n-3}\\ &= \mathcal{E}_0^{i_1-2} + 2^{i_2+1} + \mathcal{O}_{i_2+1}^{n-3} + \mathcal{O}_{i_2-1}^{n-3}\\ &= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{E}_{i_2+1}^{n-1} ,\end{aligned}$$

  so that

  $$\mathrm{wt}(\mathcal{S}_{(0,1)}) = (i_1 - 2 + 2)/2 + 1 + (n - 1 - i_2 - 1 + 2)/2 = (n + i_1 - i_2 + 2)/2 ,$$

  where $i_1 \in [\![2, n-3]\!]$ and $i_2 \in [\![i_1+1, n-2]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1)}) \in [\![3, (n+1)/2]\!]$.

- If i_1 is odd and i_2 even, then:

  $$\begin{aligned}\mathcal{S}_{(1,0)} &= \mathcal{S}_{(1)} + \mathcal{O}_0^{i_2-2} + \mathcal{E}_{i_2}^{n-1}\\ &= 1 + \mathcal{O}_0^{i_1-3} + \mathcal{O}_0^{i_2-2} + \mathcal{E}_{i_2}^{n-1}\\ &= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-2} + \mathcal{E}_{i_2}^{n-1} ,\end{aligned}$$

  so that

  $$\mathrm{wt}(\mathcal{S}_{(1,0)}) = (i_1 - 1 + 2)/2 + (i_2 - 2 - i_1 + 1 + 2)/2 + (n - 1 - i_2 + 2)/2 = (n+3)/2 .$$

- If i_1 and i_2 are odd, then:

  $$\begin{aligned}\mathcal{S}_{(1,1)} &= \mathcal{S}_{(1)} + \mathcal{E}_0^{i_2-1} + \mathcal{O}_{i_2-1}^{n-3}\\ &= 1 + \mathcal{O}_0^{i_1-3} + \mathcal{E}_0^{i_2-1} + \mathcal{O}_{i_2-1}^{n-3}\\ &= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-1} + \mathcal{O}_{i_2-1}^{n-3} .\end{aligned}$$

  so that

  $$\mathrm{wt}(\mathcal{S}_{(1,1)}) = 1 + (i_2 - 1 - i_1 - 1 + 2)/2 + (n - 3 - i_2 + 1 + 2)/2 = (n - i_1 + 2)/2 ,$$

  where $i_1 \in [\![1, n-4]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1)}) \in [\![3, (n+1)/2]\!]$.

We summarize the results in Table A.2. Thus, we have $\mathrm{wt}(sj) \in [\![3, (n+3)/2]\!]$ for all j of Hamming weight 3.

Let j be such that $\mathrm{wt}(j) = 4$, with $j = 1 + 2^{i_1} + 2^{i_2} + 2^{i_3}$ and where $1 \leqslant i_1 < i_2 < i_3 \leqslant n-1$.

$i_1 \bmod 2$	$i_2 \bmod 2$	$\mathrm{wt}\,(sj \bmod (2^n-1))$	$[\![\min, \max]\!]$
0	0	$(i_2+2)/2$	$[\![3, \frac{n+1}{2}]\!]$
0	1	$(n+i_1-i_2+2)/2$	$[\![3, \frac{n+1}{2}]\!]$
1	0	$(n+3)/2$	$\frac{n+3}{2}$
1	1	$(n-i_1+2)/2$	$[\![3, \frac{n+1}{2}]\!]$

Table A.2: $\mathrm{wt}(js)$ *for* $j = 1 + 2^{i_1} + 2^{i_2}$.

- If i_1, i_2, i_3 are even, then:

$$\begin{aligned}
\mathcal{S}_{(0,0,0)} &= \mathcal{S}_{(0,0)} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= 1 + 2\cdot\mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{O}_{i_1}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_1} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{O}_{i_1}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1}\,,
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{wt}(\mathcal{S}_{(0,0,0)}) &= (i_1-2+2)/2 + 1 + (i_3-2-i_2+2)/2 + (n-1-i_3+2)/2 \\
&= (n+i_1-i_2+3)/2\,,
\end{aligned}$$

where $i_1 \in [\![2, n-5]\!]$ and $i_2 \in [\![i_1+2, n-3]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(0,0,0)}) \in [\![4, (n+1)/2]\!]$.

- If i_1, i_2 are even and i_3 odd, then:

$$\begin{aligned}
\mathcal{S}_{(0,0,1)} &= \mathcal{S}_{(0,0)} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\
&= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\
&= 2^{i_1+1} + \mathcal{E}_{i_1}^{i_2-2} + \mathcal{E}_{i_1+2}^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\
&= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3}\,,
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{wt}(\mathcal{S}_{(0,0,1)}) &= 1 + (i_2-2-i_1+2+i_3-1-i_2+2+n-3-i_3+1+2)/2 \\
&= (n-i_1+3)/2\,,
\end{aligned}$$

where $i_1 \in [\![2, n-5]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(0,0,1)}) \in [\![4, (n+1)/2]\!]$.

- If i_1 is even, i_2 odd, and i_3 even, then:

$$\begin{aligned}
\mathcal{S}_{(0,1,0)} &= \mathcal{S}_{(0,1)} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{E}_{i_2+1}^{n-1} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= \mathcal{A}_0^{i_1-1} + \mathcal{O}_{i_1}^{i_2-3} + 2^{i_2} + \mathcal{A}_{i_2}^{i_3-1} + 2\mathcal{E}_{i_3}^{n-1} \\
&= \mathcal{A}_0^{i_1-1} + \mathcal{O}_{i_1}^{i_2-3} + 2^{i_3} + \mathcal{O}_{i_3}^{n-1} \\
&= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-3} + 2^{i_3} + \mathcal{O}_{i_3}^{n-3}\,,
\end{aligned}$$

so that

$$\begin{aligned}\mathrm{wt}(\mathcal{S}_{(0,1,0)}) &= 1 + (i_2 - 3 - i_1 + 2)/2 + 1 + (n - 3 - i_3 + 2)/2 \\ &= (n - i_1 + i_2 - i_3 + 2)/2 \,,\end{aligned}$$

where $i_1 \in \llbracket 2, n-3 \rrbracket$, $i_2 \in \llbracket i_1+1, n-2 \rrbracket$ and $i_3 \in \llbracket i_2+1, n-1 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1,0)}) \in \llbracket 2, (n-1)/2 \rrbracket$.

- If i_1 is even, and i_2, i_3 are odd, then:

$$\begin{aligned}\mathcal{S}_{(0,1,1)} &= \mathcal{S}_{(0,1)} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\ &= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{E}_{i_2+1}^{n-1} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\ &= \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-1} + \mathcal{E}_{i_3+1}^{n-1} + \mathcal{O}_{i_3-1}^{n-3} \\ &= \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-3} + 2^{i_3} + \mathcal{A}_{i_3}^{n-1} \\ &= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-3} \,,\end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(0,1,1)}) = 1 + (i_1 - 2 + 2 + i_2 - 1 - i_1 + 2 + i_3 - 3 - i_2 + 1 + 2)/2 = (i_3 + 3)/2 \,,$$

where $i_3 \in \llbracket 5, n-2 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1,1)}) \in \llbracket 4, (n+1)/2 \rrbracket$.

- If i_1 is odd and i_2, i_3 are even, then:

$$\begin{aligned}\mathcal{S}_{(1,0,0)} &= \mathcal{S}_{(1,0)} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\ &= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-2} + \mathcal{E}_{i_2}^{n-1} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\ &= \mathcal{A}_0^{i_1-1} + \mathcal{E}_{i_1+1}^{i_2} + \mathcal{E}_{i_2}^{n-1} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\ &= \mathcal{A}_0^{i_1-1} + \mathcal{E}_{i_1+1}^{i_2-2} + 2^{i_3+1} + \mathcal{E}_{i_3+2}^{n-1} + \mathcal{E}_{i_3}^{n-1} \\ &= \mathcal{A}_0^{i_1-1} + \mathcal{E}_{i_1+1}^{i_2-2} + 2^{i_3} + \mathcal{O}_{i_3}^{n-1} \\ &= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-2} + 2^{i_3} + \mathcal{O}_{i_3}^{n-3} \,,\end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(1,0,0)}) = 1 + (i_2 - i_1 - 1)/2 + 1 + (n - 1 - i_3)/2 = (n - i_1 + i_2 - i_3 + 2)/2 \,,$$

where $i_1 \in \llbracket 1, n-4 \rrbracket$, $i_2 \in \llbracket i_1+1, n-3 \rrbracket$ and $i_3 \in \llbracket i_2+2, n-1 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(1,0,0)}) \in \llbracket 2, (n-1)/2 \rrbracket$.

- If i_1 is odd, i_2 even, and i_3 odd, then:

$$\begin{aligned}\mathcal{S}_{(1,0,1)} &= \mathcal{S}_{(1,0)} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\ &= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-2} + \mathcal{E}_{i_2}^{n-1} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\ &= \mathcal{O}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-3} + \mathcal{E}_{i_1+1}^{i_3-1} + \mathcal{A}_{i_3-1}^{n-1} \\ &= \mathcal{O}_0^{i_1-3} + 2^{i_2+1} + \mathcal{E}_{i_2}^{i_3-3} + \mathcal{E}_{i_2+2}^{i_3-1} + \mathcal{A}_{i_3-1}^{n-1} \\ &= \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-3} + 2^{i_3-1} + \mathcal{A}_{i_3-1}^{n-1} \\ &= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-3} \,,\end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(1,0,1)}) = 1 + (i_1 - 1)/2 + 1 + (i_3 - 1 - i_2)/2 = (i_1 - i_2 + i_3 + 2)/2\,,$$

where $i_1 \in [\![1, n-4]\!]$, $i_2 \in [\![i_1+1, n-3]\!]$ and $i_3 \in [\![i_2+1, n-2]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(1,0,1)}) \in [\![2, (n-1)/2]\!]$.

- If i_1, i_2 are odd, and i_3 even, then:

$$\begin{aligned}
\mathcal{S}_{(1,1,0)} &= \mathcal{S}_{(1,1)} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-1} + \mathcal{O}_{i_2-1}^{n-3} + \mathcal{O}_0^{i_3-2} + \mathcal{E}_{i_3}^{n-1} \\
&= \mathcal{O}_0^{i_1-3} + 2^{i_2+1} + \mathcal{O}_{i_2-1}^{i_3-2} + \mathcal{O}_{i_2+1}^{i_3-2} + \mathcal{A}_{i_3}^{n-1} \\
&= \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2} + 2^{i_3} + \mathcal{A}_{i_3}^{n-1} \\
&= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2}\,,
\end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(1,1,0)}) = 1 + (i_1 - 1)/2 + 1 + (i_3 - i_2 - 1)/2 = (i_1 - i_2 + i_3 + 2)/2\,,$$

where $i_1 \in [\![1, n-4]\!]$, $i_2 \in [\![i_1+2, n-2]\!]$ and $i_3 \in [\![i_2+1, n-1]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(1,1,0)}) \in [\![2, (n-1)/2]\!]$.

- If i_1, i_2, i_3 are odd then:

$$\begin{aligned}
\mathcal{S}_{(1,1,1)} &= \mathcal{S}_{(1,1)} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\
&= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-1} + \mathcal{O}_{i_2-1}^{n-3} + \mathcal{E}_0^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} \\
&= \mathcal{E}_0^{i_1-1} + 2^{i_1} + \mathcal{O}_{i_1+1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-3} + \mathcal{E}_{i_2+1}^{i_3-1} + \mathcal{E}_{i_3+1}^{n-1} \\
&= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-3} + 2^{i_3} + \mathcal{E}_{i_3+1}^{n-1}\,,
\end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(1,1,1)}) = (i_1 + 1)/2 + (i_2 - i_1)/2 + 1 + (n - i_3)/2 = (n + i_2 - i_3 + 3)/2\,,$$

where $i_2 \in [\![3, n-4]\!]$ and $i_3 \in [\![i_2+2, n-2]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(1,1,1)}) \in [\![4, (n+1)/2]\!]$.

We summarize the results in Table A.3. Therefore, we have $\mathrm{wt}(sj) \in [\![2, (n+1)/2]\!]$.

Finally let j be such that $\mathrm{wt}(j) = 5$, with $j = 1 + 2^{i_1} + 2^{i_2} + 2^{i_3} + 2^{i_4}$ and where $1 \leqslant i_1 < i_2 < i_3 < i_4 \leqslant n-1$.

- If i_1, i_2, i_3, i_4 are even, then we have:

$$\begin{aligned}
\mathcal{S}_{(0,0,0,0)} &= \mathcal{S}_{(0,0,0)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= \mathcal{A}_0^{i_1-1} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{i_4-2} + \mathcal{O}_{i_1}^{i_4-2} + \mathcal{O}_{i_4}^{n-1} \\
&= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3} + \mathcal{E}_{i_3}^{i_4-2} + \mathcal{O}_{i_3}^{i_4-2} + \mathcal{O}_{i_4}^{n-3} \\
&= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-2} + 2^{i_4} + \mathcal{O}_{i_4}^{n-3}\,,
\end{aligned}$$

$i_1 \bmod 2$	$i_2 \bmod 2$	$i_3 \bmod 2$	$\mathrm{wt}\,(sj \bmod (2^n-1))$	$\llbracket \min, \max \rrbracket$
0	0	0	$(n+i_1-i_2+3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
0	0	1	$(n-i_1+3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
0	1	0	$(n-i_1+i_2-i_3+2)/2$	$\llbracket 2, \frac{n-1}{2} \rrbracket$
0	1	1	$(i_3+3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
1	0	0	$(n-i_1+i_2-i_3+2)/2$	$\llbracket 2, \frac{n-1}{2} \rrbracket$
1	0	1	$(i_1-i_2+i_3+2)/2$	$\llbracket 2, \frac{n-1}{2} \rrbracket$
1	1	0	$(i_1-i_2+i_3+2)/2$	$\llbracket 2, \frac{n-1}{2} \rrbracket$
1	1	1	$(n+i_2-i_3+3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$

Table A.3: $\mathrm{wt}(js)$ *for* $j = 1 + 2^{i_1} + 2^{i_2} + 2^{i_3}$.

so that

$$\begin{aligned} \mathrm{wt}(\mathcal{S}_{(0,0,0,0)}) &= 1 + (i_2 - i_1)/2 + (i_3 - i_2)/2 + 1 + (n - 1 - i_4)/2 \\ &= (n - i_1 + i_3 - i_4 + 3)/2\,, \end{aligned}$$

where $i_1 \in \llbracket 2, n-7 \rrbracket$, $i_3 \in \llbracket i_1 + 4, n-3 \rrbracket$ and $i_4 \in \llbracket i_3 + 2, n-1 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,0,0,0)}) \in \llbracket 4, (n-1)/2 \rrbracket$.

- If i_1, i_2, i_3 are even, and i_4 odd, then:

$$\begin{aligned} \mathcal{S}_{(0,0,0,1)} &= \mathcal{S}_{(0,0,0)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\ &= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{n-1} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\ &= \mathcal{O}_0^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{i_4-1} + \mathcal{E}_{i_1}^{i_4-1} + \mathcal{A}_{i_4}^{n-1} \\ &= \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + 2^{i_3} + \mathcal{O}_{i_3}^{i_4-3} + 2^{i_4} + \mathcal{A}_{i_4}^{n-1} \\ &= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + 2^{i_3} + \mathcal{O}_{i_3}^{i_4-3}\,, \end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(0,0,0,1)}) = 1 + i_1/2 + (i_2 - i_1)/2 + 1 + (i_4 - 1 - i_3)/2 = (i_2 - i_3 + i_4 + 3)/2\,,$$

where $i_2 \in \llbracket 4, n-5 \rrbracket$, $i_3 \in \llbracket i_2 + 2, n-3 \rrbracket$ and $i_4 \in \llbracket i_3 + 1, n-2 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,0,0,1)}) \in \llbracket 4, (n-1)/2 \rrbracket$.

- If i_1, i_2 are even, i_3 odd, and i_4 even, then:

$$\begin{aligned} \mathcal{S}_{(0,0,1,0)} &= \mathcal{S}_{(0,0,1)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\ &= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\ &= \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2} + \mathcal{E}_{i_2}^{i_3-1} + \mathcal{O}_{i_3-1}^{i_4-2} + \mathcal{O}_{i_2}^{i_4-2} + \mathcal{A}_{i_4}^{n-1} \\ &= \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + 2^{i_3+1} + \mathcal{O}_{i_3-1}^{i_4-2} + \mathcal{O}_{i_3+1}^{i_4-2} + \mathcal{A}_{i_4}^{n-1} \\ &= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-2} + 2^{i_3} + \mathcal{E}_{i_3+1}^{i_4-2}\,, \end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(0,0,1,0)}) = 1 + i_1/2 + (i_2 - i_1)/2 + 1 + (i_4 - i_3 - 1)/2 = (i_2 - i_3 + i_4 + 3)/2\,,$$

where $i_2 \in \llbracket 4, n-3 \rrbracket$, $i_3 \in \llbracket i_2+1, n-2 \rrbracket$ and $i_4 \in \llbracket i_3+1, n-1 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,0,1,0)}) \in \llbracket 4, (n+1)/2 \rrbracket$.

- If i_1, i_2 are even, i_3, i_4 odd, then:

$$\begin{aligned}
\mathcal{S}_{(0,0,1,1)} &= \mathcal{S}_{(0,0,1)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-1} + \mathcal{O}_{i_3-1}^{n-3} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2+1} + \mathcal{E}_{i_2}^{i_3-1} + \mathcal{O}_{i_3-1}^{i_4-3} + \mathcal{E}_{i_2+2}^{i_4-1} + \mathcal{E}_{i_4+1}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-1} + \mathcal{O}_{i_3-1}^{i_4-3} + \mathcal{E}_{i_3+1}^{i_4-1} + \mathcal{E}_{i_4+1}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-3} + 2^{i_4} + \mathcal{E}_{i_4+1}^{n-1}\,,
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{wt}(\mathcal{S}_{(0,0,1,1)}) &= i_1/2 + 1 + (i_3 - 1 - i_2)/2 + 1 + (n - i_4)/2 \\
&= (n + i_1 - i_2 + i_3 - i_4 + 3)/2\,,
\end{aligned}$$

where $i_1 \in \llbracket 2, n-7 \rrbracket$, $i_2 \in \llbracket i_1+2, n-5 \rrbracket$, $i_3 \in \llbracket i_2+1, n-4 \rrbracket$ and $i_4 \in \llbracket i_3+2, n-2 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,0,1,1)}) \in \llbracket 4, (n-1)/2 \rrbracket$.

- If i_1 is even, i_2 odd, and i_3, i_4 even, then:

$$\begin{aligned}
\mathcal{S}_{(0,1,0,0)} &= \mathcal{S}_{(0,1,0)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-3} + 2^{i_3} + \mathcal{O}_{i_3}^{n-3} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + 2^{i_3} + \mathcal{O}_{i_3}^{i_4-2} + \mathcal{O}_{i_2-1}^{i_4-2} + \mathcal{A}_{i_4}^{n-1} \\
&= \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-2} + \mathcal{E}_{i_3}^{i_4} + \mathcal{A}_{i_4}^{n-1} \\
&= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-2} + \mathcal{E}_{i_3}^{i_4-2}\,,
\end{aligned}$$

so that

$$\mathrm{wt}(\mathcal{S}_{(0,1,0,0)}) = 1 + i_1/2 + (i_2 + 1 - i_1)/2 + (i_3 - i_2 + 1)/2 + (i_4 - i_3)/2 = (i_4 + 4)/2\,,$$

where $i_4 \in \llbracket 6, n-1 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1,0,0)}) \in \llbracket 5, (n+3)/2 \rrbracket$.

- If i_1 is even, i_2 odd, i_3 even, and i_4 odd, then:

$$\begin{aligned}
\mathcal{S}_{(0,1,0,1)} &= \mathcal{S}_{(0,1,0)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-3} + 2^{i_3} + \mathcal{O}_{i_3}^{n-3} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + 2^{i_3} + \mathcal{E}_{i_2+1}^{i_4-1} + \mathcal{O}_{i_3}^{i_4-3} + \mathcal{E}_{i_4+1}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2} + 2^{i_3} + \mathcal{A}_{i_3}^{i_4-1} + \mathcal{E}_{i_4+1}^{n-1} \\
&= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2} + 2^{i_4} + \mathcal{E}_{i_4+1}^{n-1}\,,
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{wt}(\mathcal{S}_{(0,1,0,1)}) &= i_1/2 + 1 + (i_3 - i_2 - 1)/2 + 1 + (n - i_4)/2 \\
&= (n + i_1 - i_2 + i_3 - i_4 + 3)/2\,,
\end{aligned}$$

where $i_1 \in \llbracket 2, n-5 \rrbracket$, $i_2 \in \llbracket i_1+1, n-4 \rrbracket$, $i_3 \in \llbracket i_2+1, n-3 \rrbracket$ and $i_4 \in \llbracket i_3+1, n-2 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1,0,1)}) \in \llbracket 4, (n+1)/2 \rrbracket$.

- If i_1 is even, i_2, i_3 are odd, and i_4 even, then:

$$\begin{aligned} \mathcal{S}_{(0,1,1,0)} &= \mathcal{S}_{(0,1,1)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\ &= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-3} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\ &= \mathcal{E}_0^{i_1-2} + 2^{i_2+1} + \mathcal{O}_{i_2-1}^{i_3-3} + \mathcal{O}_{i_2+1}^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\ &= \mathcal{E}_0^{i_1-2} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-1} + \mathcal{O}_{i_3-1}^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \,, \end{aligned}$$

so that

$$\begin{aligned} \mathrm{wt}(\mathcal{S}_{(0,1,1,0)}) &= i_1/2 + 1 + (i_3 - i_2)/2 + (i_4 - i_3 + 1)/2 + (n - i_4 + 1)/2 \\ &= (n + i_1 - i_2 + 4)/2 \,, \end{aligned}$$

where $i_1 \in \llbracket 2, n-5 \rrbracket$ and $i_2 \in \llbracket i_1+1, n-4 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1,1,0)}) \in \llbracket 5, (n+3)/2 \rrbracket$.

- If i_1 is even, and i_2, i_3, i_4 are odd, then:

$$\begin{aligned} \mathcal{S}_{(0,1,1,1)} &= \mathcal{S}_{(0,1,1)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\ &= 1 + \mathcal{O}_0^{i_1-2} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-3} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\ &= 2^{i_1+1} + \mathcal{E}_{i_1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-3} + \mathcal{E}_{i_1+2}^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\ &= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-3} + 2^{i_2} + \mathcal{O}_{i_2-1}^{i_3-3} + \mathcal{E}_{i_2+1}^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\ &= 2^{i_1} + \mathcal{O}_{i_1}^{i_2-3} + 2^{i_3} + \mathcal{E}_{i_3+1}^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \,, \end{aligned}$$

so that

$$\begin{aligned} \mathrm{wt}(\mathcal{S}_{(0,1,1,1)}) &= 1 + (i_2 - 1 - i_1)/2 + 1 + (i_4 - i_3)/2 + (n - i_4)/2 \\ &= (n - i_1 + i_2 - i_3 + 3)/2 \,, \end{aligned}$$

where $i_1 \in \llbracket 2, n-7 \rrbracket$, $i_2 \in \llbracket i_1+1, n-6 \rrbracket$ and $i_3 \in \llbracket i_2+2, n-4 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(0,1,1,1)}) \in \llbracket 4, (n-1)/2 \rrbracket$.

- If i_1 is odd, and i_2, i_3, i_4 are even, then:

$$\begin{aligned} \mathcal{S}_{(1,0,0,0)} &= \mathcal{S}_{(1,0,0)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\ &= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-2} + 2^{i_3} + \mathcal{O}_{i_3}^{n-3} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\ &= \mathcal{O}_0^{i_1-3} + 2^{i_2} + 2^{i_3} + \mathcal{O}_{i_3}^{i_4-2} + \mathcal{O}_{i_2}^{i_4-2} + \mathcal{A}_{i_4}^{n-1} \\ &= \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{i_4-2} + 2^{i_4} + \mathcal{A}_{i_4}^{n-1} \\ &= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-2} + \mathcal{E}_{i_3}^{i_4-2} \,, \end{aligned}$$

so that

$$\begin{aligned} \mathrm{wt}(\mathcal{S}_{(1,0,0,0)}) &= 1 + (i_1 - 1)/2 + 1 + (i_3 - i_2)/2 + (i_4 - i_3)/2 \\ &= (i_1 - i_2 + i_4 + 3)/2 \,, \end{aligned}$$

where $i_1 \in \llbracket 1, n-6 \rrbracket$, $i_2 \in \llbracket i_1+1, n-5 \rrbracket$ and $i_4 \in \llbracket i_2+4, n-1 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(1,0,0,0)}) \in \llbracket 4, (n+1)/2 \rrbracket$.

- If i_1 is odd, i_2, i_3 even, and i_4 odd, then:

$$\begin{aligned}
\mathcal{S}_{(1,0,0,1)} &= \mathcal{S}_{(1,0,0)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-2} + 2^{i_3} + \mathcal{O}_{i_3}^{n-3} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-2} + 2^{i_3} + \mathcal{O}_{i_3}^{i_4-3} + \mathcal{E}_{i_2}^{i_4-1} + \mathcal{E}_{i_4+1}^{n-1} \\
&= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-2} + 2^{i_4} + \mathcal{E}_{i_4+1}^{n-1} \,,
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{wt}(\mathcal{S}_{(1,0,0,1)}) &= (i_1+1)/2 + (i_2-i_1+1)/2 + (i_3-i_2)/2 + 1 + (n-i_4)/2 \\
&= (n+i_3-i_4+4)/2 \,,
\end{aligned}$$

where $i_3 \in \llbracket 4, n-3 \rrbracket$ and $i_4 \in \llbracket i_3+1, n-2 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(1,0,0,1)}) \in \llbracket 5, (n+3)/2 \rrbracket$.

- If i_1 is odd, i_2 even, i_3 odd, and i_4 even, then:

$$\begin{aligned}
\mathcal{S}_{(1,0,1,0)} &= \mathcal{S}_{(1,0,1)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-3} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= \mathcal{E}_0^{i_1-1} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-3} + \mathcal{O}_{i_1-1}^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-2} + \mathcal{E}_{i_2}^{i_3-1} + \mathcal{O}_{i_3-1}^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \,,
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{wt}(\mathcal{S}_{(1,0,1,0)}) &= (i_1+1)/2 + (i_2-i_1+1)/2 + (i_3-i_2+1)/2 \\
&\quad + (i_4-i_3+1)/2 + (n-i_4+1)/2 \\
&= (n+5)/2 \,.
\end{aligned}$$

- If i_1 is odd, i_2 even, and i_3, i_4 odd, then:

$$\begin{aligned}
\mathcal{S}_{(1,0,1,1)} &= \mathcal{S}_{(1,0,1)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-3} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= 2^{i_1} + 2^{i_2} + \mathcal{O}_{i_2}^{i_3-3} + \mathcal{E}_{i_1+1}^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \\
&= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-2} + 2^{i_3} + \mathcal{E}_{i_3+1}^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3} \,,
\end{aligned}$$

so that

$$\begin{aligned}
\mathrm{wt}(\mathcal{S}_{(1,0,1,1)}) &= 1 + (i_2-i_1-1)/2 + 1 + (i_4-i_3)/2 + (n-i_4)/2 \\
&= (n-i_1+i_2-i_3+3)/2 \,,
\end{aligned}$$

where $i_1 \in \llbracket 1, n-6 \rrbracket$, $i_2 \in \llbracket i_1+1, n-2 \rrbracket$ and $i_3 \in \llbracket i_2+1, n-4 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(1,0,1,1)}) \in \llbracket 4, (n+1)/2 \rrbracket$.

- If i_1, i_2 are odd, and i_3, i_4 even, then:

$$\begin{aligned}
\mathcal{S}_{(1,1,0,0)} &= \mathcal{S}_{(1,1,0)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= \mathcal{E}_0^{i_1-1} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2} + \mathcal{O}_{i_1-1}^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \\
&= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-3} + 2^{i_3} + \mathcal{O}_{i_3}^{i_4-2} + \mathcal{E}_{i_4}^{n-1} \,,
\end{aligned}$$

so that

$$\begin{aligned}\mathrm{wt}(\mathcal{S}_{(1,1,0,0)}) &= (i_1+1)/2 + (i_2-i_1)/2 + 1 + (i_4-i_3)/2 + (n-i_4+1)/2\\ &= (n+i_2-i_3+4)/2\,,\end{aligned}$$

where $i_2 \in [\![3, n-4]\!]$ and $i_3 \in [\![i_2+1, n-3]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(1,1,0,0)}) \in [\![5, (n+3)/2]\!]$.

- If i_1, i_2 are odd, i_3 even, and i_4 odd, then:

$$\begin{aligned}\mathcal{S}_{(1,1,0,1)} &= \mathcal{S}_{(1,1,0)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3}\\ &= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3}\\ &= 2^{i_1} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-2} + \mathcal{E}_{i_1+1}^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3}\\ &= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-2} + \mathcal{E}_{i_3}^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3}\,,\end{aligned}$$

so that

$$\begin{aligned}\mathrm{wt}(\mathcal{S}_{(1,1,0,1)}) &= 1 + (i_2-i_1)/2 + (i_3-i_2+1)/2 + (i_4-i_3+1)/2 + (n-i_4)/2\\ &= (n-i_1+4)/2\,,\end{aligned}$$

where $i_1 \in [\![1, n-6]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(1,1,0,1)}) \in [\![5, (n+3)/2]\!]$.

- If i_1, i_2, i_3 are odd, and i_4 even, then:

$$\begin{aligned}\mathcal{S}_{(1,1,1,0)} &= \mathcal{S}_{(1,1,1)} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1}\\ &= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-3} + 2^{i_3} + \mathcal{E}_{i_3+1}^{n-1} + \mathcal{O}_0^{i_4-2} + \mathcal{E}_{i_4}^{n-1}\\ &= \mathcal{A}_0^{i_1-1} + \mathcal{E}_{i_1+1}^{i_2-1} + 2^{i_3} + \mathcal{E}_{i_3+1}^{i_4-2} + \mathcal{O}_{i_2-1}^{i_4-2} + \mathcal{O}_{i_4}^{n-3} + 2^n\\ &= 2^{i_1} + \mathcal{E}_{i_1+1}^{i_2-1} + \mathcal{O}_{i_2-1}^{i_3-3} + 2^{i_4} + \mathcal{O}_{i_4}^{n-3}\,,\end{aligned}$$

so that

$$\begin{aligned}\mathrm{wt}(\mathcal{S}_{(1,1,1,0)}) &= 1 + (i_2-i_1)/2 + (i_3-i_2)/2 + 1 + (n-1-i_4)/2\\ &= (n-i_1+i_3-i_4+3)/2\,,\end{aligned}$$

where $i_1 \in [\![1, n-6]\!]$, $i_3 \in [\![i_1+4, n-4]\!]$ and $i_4 \in [\![i_3+1, n-1]\!]$, implying that $\mathrm{wt}(\mathcal{S}_{(1,1,1,0)}) \in [\![4, (n+1)/2]\!]$.

- If i_1, i_2, i_3, i_4 are odd, then:

$$\begin{aligned}\mathcal{S}_{(1,1,1,1)} &= \mathcal{S}_{(1,1,1)} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3}\\ &= \mathcal{E}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-3} + 2^{i_3} + \mathcal{E}_{i_3+1}^{n-1} + \mathcal{E}_0^{i_4-1} + \mathcal{O}_{i_4-1}^{n-3}\\ &= \mathcal{O}_0^{i_1-1} + \mathcal{O}_{i_1-1}^{i_2-3} + 2^{i_3} + \mathcal{E}_{i_3+1}^{i_4-1} + \mathcal{E}_{i_1+1}^{i_4-1} + \mathcal{A}_{i_4}^{n-1}\\ &= \mathcal{O}_0^{i_1-3} + 2^{i_2} + 2^{i_3} + \mathcal{E}_{i_3+1}^{i_4-1} + \mathcal{E}_{i_2+1}^{i_4-1} + \mathcal{A}_{i_4}^{n-1}\\ &= \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-1} + \mathcal{O}_{i_3-1}^{i_4-3} + 2^{i_4} + \mathcal{A}_{i_4}^{n-1}\\ &= 1 + \mathcal{O}_0^{i_1-3} + 2^{i_2} + \mathcal{E}_{i_2+1}^{i_3-1} + \mathcal{O}_{i_3-1}^{i_4-3}\,,\end{aligned}$$

so that

$$\begin{aligned}\mathrm{wt}(\mathcal{S}_{(1,1,1,1)}) &= 1 + (i_1 - 1)/2 + (i_3 - i_2)/2 + 1 + (i_4 - i_3)/2 \\ &= (i_1 - i_2 + i_4 + 3)/2\,,\end{aligned}$$

where $i_1 \in \llbracket 1, n-8 \rrbracket$, $i_2 \in \llbracket i_1 + 2, n-6 \rrbracket$, and $i_4 \in \llbracket i_2 + 4, n-2 \rrbracket$, implying that $\mathrm{wt}(\mathcal{S}_{(1,1,1,1)}) \in \llbracket 4, (n-1)/2 \rrbracket$.

We summarize the results in Table A.4. Thus, we have $\mathrm{wt}(sj) \in \llbracket 4, (n+1)/2 \rrbracket$. □

i_1 mod 2	i_2 mod 2	i_3 mod 2	i_4 mod 2	wt $(sj \bmod (2^n - 1))$	$\llbracket \min, \max \rrbracket$
0	0	0	0	$(n - i_1 + i_3 - i_4 + 3)/2$	$\llbracket 4, \frac{n-1}{2} \rrbracket$
0	0	0	1	$(i_2 - i_3 + i_4 + 3)/2$	$\llbracket 4, \frac{n-1}{2} \rrbracket$
0	0	1	0	$(i_2 - i_3 + i_4 + 3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
0	0	1	1	$(n + i_1 - i_2 + i_3 - i_4 + 3)/2$	$\llbracket 4, \frac{n-1}{2} \rrbracket$
0	1	0	0	$(i_4 + 4)/2$	$\llbracket 5, \frac{n+3}{2} \rrbracket$
0	1	0	1	$(n + i_1 - i_2 + i_3 - i_4 + 3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
0	1	1	0	$(n + i_1 - i_2 + 4)/2$	$\llbracket 5, \frac{n+3}{2} \rrbracket$
0	1	1	1	$(n - i_1 + i_2 - i_3 + 3)/2$	$\llbracket 4, \frac{n-1}{2} \rrbracket$
1	0	0	0	$(i_1 - i_2 + i_4 + 3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
1	0	0	1	$(n + i_3 - i_4 + 4)/2$	$\llbracket 5, \frac{n+3}{2} \rrbracket$
1	0	1	0	$(n + 5)/2$	$\frac{n+5}{2}$
1	0	1	1	$(n - i_1 + i_2 - i_3 + 3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
1	1	0	0	$(n + i_2 - i_3 + 4)/2$	$\llbracket 5, \frac{n+3}{2} \rrbracket$
1	1	0	1	$(n - i_1 + 4)/2$	$\llbracket 5, \frac{n+3}{2} \rrbracket$
1	1	1	0	$(n - i_1 + i_3 - i_4 + 3)/2$	$\llbracket 4, \frac{n+1}{2} \rrbracket$
1	1	1	1	$(i_1 - i_2 + i_4 + 3)/2$	$\llbracket 4, \frac{n-1}{2} \rrbracket$

Table A.4: $\mathrm{wt}(js)$ *for* $j = 1 + 2^{i_1} + 2^{i_2} + 2^{i_3} + 2^{i_4}$.

Proposition A.1 allows us to determine a bound on the algebraic degree. In Table A.5, we give the number of exponents appearing in $\mathcal{E}_{s,r}$ at each round for various instances of MiMC_3^{-1}. Figures in purple-bold indicate that the maximal number of exponents of a certain Hamming weight is reached. For example, when $n = 11$, in the second round we have exponents j of Hamming weight 5 meaning that the corresponding exponents js in the third round have Hamming weight at most $(n + 3)/2 = 7$. However the proposition is not sufficient, since we can only consider exponents j of Hamming weight at most 5. Therefore, proving the conjecture in the general case would help to ensure that the bound is exactly 7 in that case.

Round	$\#\{j, wt(j) = i\}$ where i is equal to										
	0	1	2	3	4	5	6	7	8	9	10
1	-	-	-	-	-	-	1	-	-	-	-
2	1	1	2	7	13	19	21	-	-	-	-
3	1	**11**	32	51	93	113	136	74	2	-	-
4	1	**11**	50	115	212	310	334	225	48	-	-
5	1	**11**	**55**	160	276	401	416	305	131	19	-
6	1	**11**	**55**	**165**	312	437	452	326	163	38	-
7	1	**11**	**55**	**165**	**330**	449	458	**330**	**165**	51	2

***(a)** For $n = 11, s = 1365$.*

Round	$\#\{j, wt(j) = i\}$ where i is equal to												
	0	1	2	3	4	5	6	7	8	9	10	11	12
1	-	-	-	-	-	-	-	1	-	-	-	-	-
2	1	1	2	8	16	26	37	37	-	-	-	-	-
3	1	**13**	50	94	179	273	317	355	220	18	-	-	-
4	1	**13**	72	213	448	784	1051	1106	781	250	12	-	-
5	1	**13**	**78**	280	637	1091	1460	1500	1121	554	144	-	-
6	1	**13**	**78**	**286**	695	1209	1619	1657	1264	691	225	23	-
7	1	**13**	**78**	**286**	**715**	1259	1675	1699	1276	**715**	276	54	-
8	1	**13**	**78**	**286**	**715**	1282	1698	1710	**1287**	**715**	**286**	73	-
9	1	**13**	**78**	**286**	**715**	**1287**	1703	**1716**	**1287**	**715**	**286**	**78**	8

***(b)** For $n = 13, s = 5461$.*

Round	$\#\{j, wt(j) = i\}$ where i is equal to														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-
2	1	1	2	9	19	33	54	72	65	-	-	-	-	-	-
3	1	**15**	72	164	323	570	788	914	942	625	95	-	-	-	-
4	1	**15**	98	356	869	1760	2837	3655	3738	2964	1056	123	-	-	-
5	1	**15**	**105**	448	1262	2558	4160	5359	5439	4185	2283	764	81	-	-
6	1	**15**	**105**	**455**	1342	2865	4684	6055	6152	4850	2849	1132	234	11	-
7	1	**15**	**105**	**455**	**1365**	2971	4896	6295	6333	4954	2986	1316	360	41	-
8	1	**15**	**105**	**455**	**1365**	**3003**	4960	6373	6401	4992	**3003**	**1365**	437	65	-
9	1	**15**	**105**	**455**	**1365**	**3003**	4993	6414	6428	4999	**3003**	**1365**	**455**	93	-
10	1	**15**	**105**	**455**	**1365**	**3003**	**5005**	6420	**6435**	**5005**	**3003**	**1365**	**455**	**105**	3

***(c)** For $n = 15, s = 21845$.*

Round	$\#\{j, wt(j) = i\}$ where i is equal to																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	-	-	-	-	-	-	1	-	-	-	-	-	-	-	-	-	-
2	1	1	2	10	22	40	72	112	138	114	-	-	-	-	-	-	-
3	1	**17**	98	270	567	1104	1714	2336	2604	2530	1742	392	4	-	-	-	-
4	1	**17**	128	549	1572	3586	6699	10168	12710	12658	9323	4216	809	27	-	-	-
5	1	**17**	**136**	672	2250	5424	10304	15848	19765	19860	15629	9161	3598	719	15	-	-
6	1	**17**	**136**	**680**	2353	5974	11652	18115	22749	23055	18592	11592	5221	1490	196	2	-
7	1	**17**	**136**	**680**	2380	6151	12175	18993	23737	23852	19205	12234	5955	2025	408	29	-
8	1	**17**	**136**	**680**	**2380**	**6188**	12323	19266	24095	24155	19379	12361	6173	2300	542	46	-
9	1	**17**	**136**	**680**	**2380**	**6188**	12368	19379	24232	24263	19431	12369	**6188**	**2380**	638	81	-
10	1	**17**	**136**	**680**	**2380**	**6188**	**12376**	19427	24272	24294	19441	**12376**	**6188**	**2380**	**680**	121	-
11	1	**17**	**136**	**680**	**2380**	**6188**	**12376**	**19448**	24293	**24310**	**19448**	**12376**	**6188**	**2380**	**680**	**136**	2

***(d)** For $n = 17, s = 87381$.*

***Table A.5:** Number of exponents in $\mathcal{E}_{s,r}$ for MiMC_3^{-1}.*

Appendix B
Open problems on the sequences $k_{d,r}$

In this section, we will investigate the sequences $(b_{d,r})_{r\geqslant 1}$ for other instances of MiMC$_d$, when $d > 3$. In what follows, our method will be the same as in Section 7.2 and will consist in starting from a round r for which $b_{d,r} = \mathsf{b}$, and then going back some rounds before to find out which sub-sequences of $(b_{d,r-i})_{1\leqslant i<r}$ made it possible to get $b_{d,r}$ at round r.

B.1 When using MiMC$_d$, with $d = 2^j + 1$

In the following, we will investigate the case where a Gold function is used as the iterated power function, i.e. when we will study the sequences $(b_{2^j+1,r})_{r>0}$. However, unlike the case of MiMC$_3$ for which we were able to determine the exact algebraic degree for a certain number of rounds, we did not go so far for the other instances of MiMC$_d$. Therefore, when choosing the number of impossible and possible sub-sequences to look at, we will not have a clearly identified limit, our choice will be subjective, but mainly related to the complexity of figure representations. Let us study the examples of $d = 5$ and $d = 9$.

B.1.1 When using MiMC$_5$

For MiMC$_5$ let us recall that the sequences $(k_{5,r})_{r>0}$ and $(b_{5,r})_{r>0}$ are defined by $k_{5,r} = \lfloor r \log_2 5 \rfloor$ and $b_{5,r} = k_{5,r} \bmod 4$.

Lemma B.1. *Let $(b_{5,r})_{r>0}$ be the sequence defined by $b_{5,r} = k_{5,r} \bmod 4$, and let b be any value in $\{0,1,2,3\}$. Then, for any $r \geqslant 1$ none of the following situations can occur:*

- ***(i)*** $(b_{5,r-2}b_{5,r-1}b_{5,r}) = (\mathsf{bbb}) + (210)$,
- ***(ii)*** $(b_{5,r-3}\dots b_{5,r}) = (\mathsf{b}\dots\mathsf{b}) + (0310)$,
- ***(iii)*** $(b_{5,r-4}\dots b_{5,r}) = (\mathsf{b}\dots\mathsf{b}) + (02020) = (\mathsf{b}\dots\mathsf{b}) + (0(20)^2)$,
- ***(iv)*** $(b_{5,r-7}\dots b_{5,r}) = (\mathsf{b}\dots\mathsf{b}) + (13132020) = (\mathsf{b}\dots\mathsf{b}) + ((13)^2(20)^2)$,
- ***(v)*** $(b_{5,r-10}\dots b_{5,r}) = (\mathsf{b}\dots\mathsf{b}) + (20203132020) = (\mathsf{b}\dots\mathsf{b}) + ((20)^2 313(20)^2)$.

Proof. In this proof, we will use that:

$$\forall r, i, \quad k_{5,r-i} + \lfloor i \log_2 5 \rfloor \leqslant k_{5,r} \leqslant k_{5,r-i} + \lfloor i \log_2 5 \rfloor + 1\,.$$

To simplify the proof, let us take $\mathsf{b} = 0$. Recall that $\log_2 5 \approx 2.322$, then we can derive the following contradictions:

(i) $(b_{5,r-2}b_{5,r-1}b_{5,r}) = (210)$ implies

$$k_{5,r} = k_{5,r-2} + 3 + 3 = k_{5,r-2} + 6\,,$$

so that

$$k_{5,r} \leqslant k_{5,r-2} + \lfloor 2\log_2 5 \rfloor + 1 = k_{5,r-2} + 5 < k_{5,r-2} + 6\,.$$

(ii) $(b_{5,r-3} \dots b_{5,r}) = (0310)$ implies

$$k_{5,r} = k_{5,r-3} + 3 + 2 + 3 = k_{5,r-3} + 8\,,$$

so that

$$k_{5,r} \leqslant k_{5,r-3} + \lfloor 3\log_2 5 \rfloor + 1 = k_{5,r-3} + 7 < k_{5,r-2} + 8\,.$$

(iii) $(b_{5,r-4} \dots b_{5,r}) = (0(20)^2)$ implies

$$k_{5,r} = k_{5,r-4} + 4 \times 2 = k_{5,r-4} + 8\,.$$

so that

$$k_{5,r} \geqslant k_{5,r-4} + \lfloor 4\log_2 5 \rfloor = k_{5,r-4} + 9 > k_{5,r-4} + 8\,.$$

(iv) $(b_{5,r-7} \dots b_{5,r}) = ((13)^2(20)^2)$ implies

$$k_{5,r} = k_{5,r-7} + (2 \times 3) \times 2 + 3 = k_{5,r-7} + 15\,.$$

so that

$$k_{5,r} \geqslant k_{5,r-7} + \lfloor 7\log_2 5 \rfloor = k_{5,r-7} + 16 > k_{5,r-7} + 15\,.$$

(v) $(b_{5,r-10} \dots b_{5,r}) = ((20)^2 313 (20)^2)$ implies

$$k_{5,r} = k_{5,r-10} + 2 \times (3 \times 2 + 2) + 3 \times 2 = k_{5,r-10} + 22\,.$$

so that

$$k_{5,r} \geqslant k_{5,r-10} + \lfloor 10\log_2 5 \rfloor = k_{5,r-10} + 23 > k_{5,r-10} + 22\,.$$

We now observe that all these arguments depend on the differences $(b_{5,r} - b_{5,r-i})$, implying that adding the same value $\mathsf{b} \in \{0,1,2,3\}$ to all elements in the sequence does not modify the result. □

In Figure B.1 we represent the impossible sub-sequences in the sequence $(b_{5,r})_{r>0}$. A red arrow means that the transition is impossible because of a case in Lemma B.1. We recall that in Figure 7.6, for each node, the left arrow represents the case $b_{3,r-1} = b_{r,-}1$ and the right arrow represents the case $b_{3,r-1} = b_{r,-}2$. Then for the sake of consistency, in Figure B.1, the left arrow represents the case $b_{5,r-1} = b_{5,r} - \lfloor \log_2 5 \rfloor = b_{r,-}2$ and the right arrow represents the case $b_{5,r-1} = b_{5,r} - \lfloor \log_2 5 \rfloor - 1 = b_{5,r} - 3$.

Now, to be consistent with Proposition 7.1, we investigate the possible sub-sequences in $(b_{5,r})_{r>0}$ by looking at the right part of the graph. This means that each time we encounter a node that has two children, the left child represents the end of a sequence.

Proposition B.1. *Let $(k_{5,r})_{r>0}$ and $(b_{5,r})_{r>0}$ be the sequences defined in Lemma B.1. Then, for any $r \geqslant 1$, there exists $\mathsf{b} \in \{0,1,2,3\}$ such that one of the following situations occurs:*

(i) $(b_{5,r-1}b_{5,r}) = (\mathsf{bb}) + (20)$,

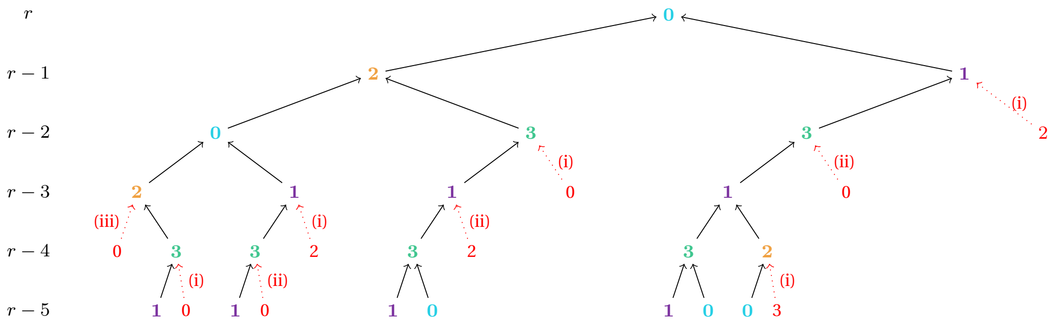


Figure B.1: *Impossible sub-sequences in the sequence* $(b_{5,r})_{r>0}$.

(ii) $(b_{5,r-4} \dots b_{5,r}) = (\mathsf{b} \dots \mathsf{b}) + ((31)^2 0)$,

(iii) $(b_{5,r-7} \dots b_{5,r}) = (\mathsf{b} \dots \mathsf{b}) + ((02)^2 1310)$,

(iv) $(b_{5,r-10} \dots b_{5,r}) = (\mathsf{b} \dots \mathsf{b}) + ((13)^2 2021310)$,

(v) $(b_{5,r-10} \dots b_{5,r}) = (\mathsf{b} \dots \mathsf{b}) + (03132021310)$.

Proof. As previously explained, adding the same value b to all elements of the sequence does not affect the properties. We can then prove the result for $\mathsf{b} = 0$ only.

Let $b_{5,r} = 0$, then we will look at the $b_{5,r-i}$ according to Lemma B.1. To better understand the different steps involved in this proof, we will refer to Figure B.2. Starting from the first node at the top, we have two branches, either $b_{5,r-1} = 2$ or $b_{5,r-1} = 1$.

- **If $\boldsymbol{b_{5,r-1} = 2}$:** this is a left child, meaning that we stop the process. We obtain $(b_{5,r-1} b_{5,r}) = (20)$, which corresponds to the first sequence **(i)**.

- **If $\boldsymbol{b_{5,r-1} = 1}$:** we know from Lemma B.1-**(i)** and **(ii)** that we have $(b_{5,r-3} \dots b_{5,r}) = (1310)$. In Figure B.2, we indeed observe that the nodes, on the right, at rounds $(r-1)$ and $(r-2)$ have only one branching. Then, at round $(r-3)$, the node 1 has two branches, either $b_{5,r-4} = 3$ or $b_{5,r-4} = 2$.

- **If $\boldsymbol{b_{5,r-4} = 3}$:** this is a left child leading to the sequence **(ii)** since we have $(b_{5,r-4} \dots b_{5,r}) = ((31)^2 0)$.

- **If $\boldsymbol{b_{5,r-4} = 2}$:** we have necessarily $(b_{5,r-6} \dots b_{5,r}) = (2021310)$, because of Lemma B.1-**(i)** and **(ii)** applied with $\mathsf{b} = 1$. In Figure B.2, we notice that the nodes, on the right, at rounds $(r-4)$ and $(r-5)$ have only one branching. Then, at round $(r-6)$, the node 2 has two branches, either $b_{5,r-7} = 0$ or $b_{5,r-7} = 3$.

- **If $\boldsymbol{b_{5,r-7} = 0}$:** we have a left child so that we stop the process. We get $(b_{5,r-7} \dots b_{5,r}) = ((02)^2 1310)$, corresponding to the sequence **(iii)**.

- **If $\boldsymbol{b_{5,r-7} = 3}$:** we have necessarily $(b_{5,r-9} \dots b_{5,r}) = (3132021310)$, using Lemma B.1-**(i)** and **(ii)** with $\mathsf{b} = 2$. Similarly, in Figure B.2, we have nodes, on the right, with only one branching, at rounds $(r-7)$ and $(r-8)$. Then, at round $(r-9)$, the node 3 has two branches, either $b_{5,r-10} = 1$ or $b_{5,r-10} = 0$.

- **If $\boldsymbol{b_{5,r-10} = 1}$:** we have $(b_{5,r-10} \dots b_{5,r}) = ((13)^2 2021310)$, so this is the sequence **(iv)**.

- **If $b_{5,r-10} = 0$:** we have $(b_{5,r-10} \dots b_{5,r}) = (03132021310)$, which corresponds to the last sequence **(v)**.

□

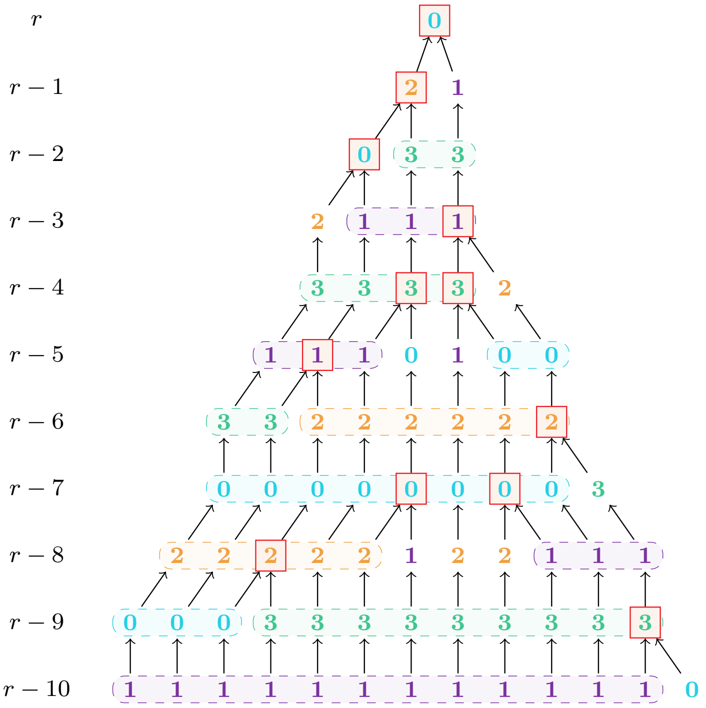


Figure B.2: *The different sub-sequences that could occur in the sequence $(b_{5,r})_{r>0}$.*

While for MiMC$_3$ we could notice that there is only one node with two children per round, we can observe that for MiMC$_5$ at round $r-4$ and $r-7$, two different nodes have two children.

Moreover, let us notice that the denominators of semi-convergents of $\log_2 5$ are:

$$\mathfrak{D}_5 = \{1, 3, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 59, 87, 146, 205, 351, 497, 643, 789, \dots\} .$$

We recover $\{1, 4, 7, 10\}$, that are the integers corresponding to lengths of the possible sub-sequences in Proposition B.1. However for the impossible sub-sequences from Lemma B.1, we note that 2 is not part of the semi-convergents.

B.1.2 When using MiMC$_9$

For MiMC$_9$ let us recall that we define the sequences $(k_{9,r})_{r>0}$ and $(b_{9,r})_{r>0}$ by $k_{9,r} = \lfloor r \log_2 9 \rfloor$ and $b_{9,r} = k_{9,r} \bmod 6$.

Lemma B.2. *Let $(b_{9,r})_{r>0}$ be the sequence defined by $b_{9,r} = k_{9,r} \bmod 6$, and let* b *be any value in $\{0, \dots, 5\}$. Then, for any $r \geqslant 1$ none of the following situations can occur:*

(i) $(b_{9,r-2} b_{9,r-1} b_{9,r}) = (\mathsf{bbb}) + (420)$,

(ii) $(b_{9,r-3} \dots b_{9,r}) = (\mathsf{b} \dots \mathsf{b}) + (1520)$,

(iii) $(b_{9,r-4} \dots b_{9,r}) = (\mathsf{b} \dots \mathsf{b}) + (42520)$,

(iv) $(b_{9,r-5} \dots b_{9,r}) = (\mathsf{b} \dots \mathsf{b}) + (1(52)^2 0)$,

(v) $(b_{9,r-6} \dots b_{9,r}) = (\mathsf{b} \dots \mathsf{b}) + ((03)^3 0)$,

(vi) $(b_{9,r-7} \dots b_{9,r}) = (\mathsf{b} \dots \mathsf{b}) + (042(52)^2 0)$,

Proof. The proof is similar as for Lemma B.1. We will use that:

$$\forall r, i, \quad k_{9,r-i} + \lfloor i \log_2 9 \rfloor \leqslant k_{9,r} \leqslant k_{9,r-i} + \lfloor i \log_2 9 \rfloor + 1 \,,$$

and we fix $\mathsf{b} = 0$. Recall that $\log_2 9 \approx 3.170$, then we can derive the following contradictions:

(i) $(b_{9,r-2} b_{9,r-1} b_{9,r}) = (420)$ implies

$$k_{9,r} = k_{9,r-2} + 4 + 4 = k_{9,r-2} + 8 \,,$$

so that

$$k_{9,r} \leqslant k_{9,r-2} + \lfloor 2 \log_2 9 \rfloor + 1 = k_{9,r-2} + 7 < k_{9,r-2} + 8 \,.$$

(ii) $(b_{9,r-3} \dots b_{9,r}) = (1520)$ implies

$$k_{9,r} = k_{9,r-3} + 4 + 3 + 4 = k_{9,r-3} + 11 \,,$$

so that

$$k_{9,r} \leqslant k_{9,r-3} + \lfloor 3 \log_2 9 \rfloor + 1 = k_{9,r-3} + 10 < k_{9,r-2} + 11 \,.$$

(iii) $(b_{9,r-4} \dots b_{9,r}) = (42520)$ implies

$$k_{9,r} = k_{9,r-4} + 4 + 3 \times 2 + 4 = k_{9,r-4} + 14 \,,$$

so that

$$k_{9,r} \geqslant k_{9,r-4} + \lfloor 4 \log_2 9 \rfloor = k_{9,r-4} + 13 > k_{9,r-4} + 14 \,.$$

(iv) $(b_{9,r-5} \dots b_{9,r}) = (1(52)^2 0)$ implies

$$k_{9,r} = k_{9,r-5} + 4 + 3 \times 3 + 4 = k_{9,r-5} + 17 \,,$$

so that

$$k_{9,r} \leqslant k_{9,r-5} + \lfloor 5 \log_2 9 \rfloor + 1 = k_{9,r-5} + 16 < k_{9,r-5} + 17 \,.$$

(v) $(b_{9,r-6} \dots b_{9,r}) = ((03)^3 0)$ implies

$$k_{9,r} = k_{9,r-6} + 3 \times 6 = k_{9,r-6} + 18 \,,$$

so that

$$k_{9,r} \geqslant k_{9,r-6} + \lfloor 6 \log_2 9 \rfloor = k_{9,r-6} + 19 > k_{9,r-6} + 18 \,.$$

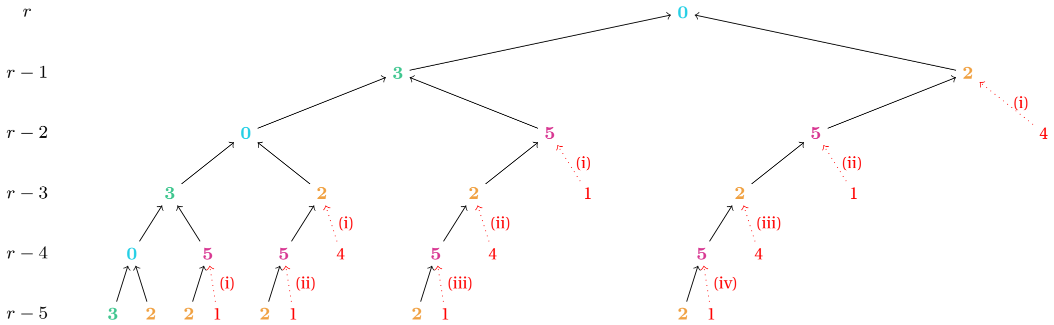


Figure B.3: *Impossible subsequences in the sequence* $(b_{9,r})_{r>0}$.

(vi) $(b_{9,r-7}\ldots b_{9,r}) = (042(52)^2 0)$ implies

$$k_{9,r} = k_{9,r-7} + 4\times 2 + 3\times 4 + 4 = k_{9,r-7} + 24\,,$$

so that

$$k_{9,r} \leqslant k_{9,r-7} + \lfloor 7\log_2 9\rfloor + 1 = k_{9,r-7} + 23 < k_{9,r-7} + 24\,.$$

□

We illustrate these observations in Figure B.3, where a red arrow means that the transition is impossible because of a case in Lemma B.2.

Proposition B.2. *Let* $(k_{9,r})_{r>0}$ *and* $(b_{9,r})_{r>0}$ *be the sequences defined in Lemma B.2. Then, for any* $r\geqslant 1$, *there exists* $\mathsf{b}\in\{0,\ldots,5\}$ *such that one of the following situations occurs:*

(i) $(b_{9,r-1}b_{9,r}) = (\mathsf{bb}) + (30)$,

(ii) $(b_{9,r-6}\ldots b_{9,r}) = (\mathsf{b}\ldots\mathsf{b}) + ((52)^3 0)$,

(iii) $(b_{9,r-6}\ldots b_{9,r}) = (\mathsf{b}\ldots\mathsf{b}) + (42(52)^2 0)$.

Proof. Without loss of generality, we can set $b_{9,r} = 0$, and look at the $b_{9,r-i}$ according to Lemma B.2. We will use Figure B.4 to have a deeper insight of the different steps of this proof. Starting with the node 0 at the top, there are two branches implying that we have either $b_{9,r-1} = 3$ or $b_{9,r-1} = 2$.

- **If $b_{9,r-1} = 3$:** this is a left child leading to the sequence **(i)** since we have $(b_{9,r-1}b_{9,r}) = (30)$.
- **If $b_{9,r-1} = 2$:** we have necessarily $(b_{9,r-5}\ldots b_{9,r}) = (2(52)^2 0)$, using the first four items of Lemma B.2. In Figure 7.7, this observation is translated by a sequence of nodes with only one branching until round $(r-5)$. Then, at round $(r-5)$, the node 2 has two branches, either $b_{9,r-6} = 5$ or $b_{9,r-6} = 4$.
- **If $b_{9,r-6} = 5$:** we have $(b_{9,r-6}\ldots b_{9,r}) = ((52)^3 0)$, which corresponds to the sequence **(ii)**.
- **If $b_{9,r-6} = 4$:** we have $(b_{9,r-6}\ldots b_{9,r}) = (42(52)^2 0)$, so this is the sequence **(iii)**.

□

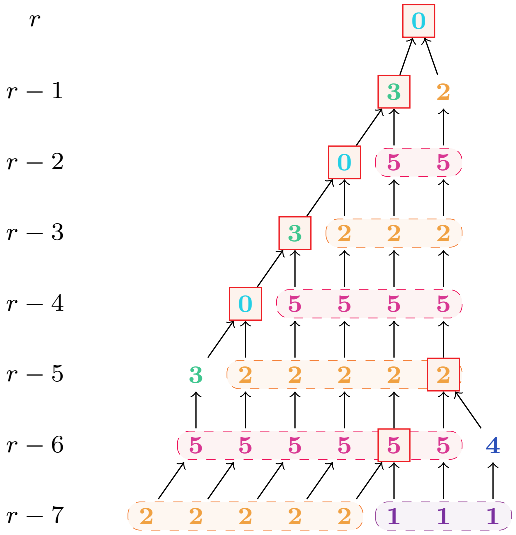


Figure B.4: *The different subsequences that could occur in the sequence* $(b_{9,r})_{r>0}$.

Let us observe that the denominators of the semi-convergents of $\log_2 9$ are

$$\mathfrak{D}_9 = \{1, 5, 6, 11, 17, 23, 29, 35, 41, 47, 53, 100, 153, 206, 359, 512, 665, 818, \ldots\}\,.$$

As for MiMC_5, we notice that integers i such that $(b_{3,r-i} \ldots b_{3,r})$ is an impossible sequence are not necessarily part of the denominators of the semi-convergents, but those involved in the possible sub-sequences in Proposition B.2 are denominators of the semi-convergents of $\log_2 9$.

B.2 When using MiMC_d, with $d = 2^j - 1$

In this section we now investigate the behaviour of sequences $(b_{d,r})_{r>0}$ when $d = 2^j - 1$. Let us recall that in this case, we have $b_{d,r} = k_{d,r} \bmod j$ (see Section 6.3.2). We first take the example of MiMC_7 and then generalize the observations.

B.2.1 When using MiMC_7

We recall that in the case of MiMC_7, the sequences $(k_{7,r})_{r>0}$ and $(b_{7,r})_{r>0}$ are defined by $k_{7,r} = \lfloor r \log_2 7 \rfloor$ and $b_{7,r} = k_{7,r} \bmod 3$.

Lemma B.3. *Let* $(b_{7,r})_{r>0}$ *be the sequence defined by* $b_{7,r} = k_{7,r} \bmod 3$*, and let* $\mathsf{b} \in \{0, 1, 2\}$*. Then, for any* $r \geqslant 1$ *none of the following situations can occur:*

(i) $(b_{7,r-i} \ldots b_{7,r}) = (\mathsf{b} \ldots \mathsf{b}) + (21^{i-1}0)$*, for all* $i = 2, \ldots, 5$,

(ii) $(b_{7,r-6} \ldots b_{7,r}) = (\mathsf{b} \ldots \mathsf{b}) + (0^7)$,

(iii) $(b_{7,r-11} \ldots b_{7,r}) = (\mathsf{b} \ldots \mathsf{b}) + (1^6 0^6)$,

(iv) $(b_{7,r-16} \ldots b_{7,r}) = (\mathsf{b} \ldots \mathsf{b}) + (2^6 1^5 0^6)$,

(v) $(b_{7,r-21}\dots b_{7,r}) = (\mathsf{b}\dots\mathsf{b}) + (0^6 2^5 1^5 0^6)$.

Proof. As previously observed, we can set $\mathsf{b} = 0$ without loss of generality. We will use that

$$\forall r, i, \quad k_{7,r-i} + \lfloor i \log_2 7 \rfloor \leqslant k_{7,r} \leqslant k_{7,r-i} + \lfloor i \log_2 7 \rfloor + 1\,.$$

Recall that $\log_2 7 \approx 2.807$, then we can derive the following contradictions:

(i) $(b_{7,r-i}\dots b_{7,r}) = (21^{i-1}0)$ for all $i = 2,\dots,5$ implies $k_{7,r} = k_{7,r-i} + 4 + 3(i-2)$. Then

$$k_{7,r} \geqslant k_{7,r-i} + \lfloor i \log_2 7 \rfloor = k_{7,r-i} + 5 + 3(i-2) > k_{7,r-i} + 4 + 3(i-2)\,.$$

(ii) $(b_{7,r-6}\dots b_{7,r}) = (0^7)$ implies $k_{7,r} = k_{7,r-6} + 18$. Then

$$k_{7,r} \leqslant k_{7,r-6} + \lfloor 6 \log_2 7 \rfloor + 1 = k_{7,r-6} + 17 < k_{7,r-6} + 18\,.$$

(iii) $(b_{7,r-11}\dots b_{7,r}) = (1^6 0^6)$ implies $k_{7,r} = k_{7,r-11} + 32$. Then

$$k_{7,r} \leqslant k_{7,r-11} + \lfloor 11 \log_2 7 \rfloor + 1 = k_{7,r-11} + 31 < k_{7,r-11} + 32\,.$$

(iv) $(b_{7,r-16}\dots b_{7,r}) = (2^6 1^5 0^6)$ implies $k_{7,r} = k_{7,r-16} + 46$. Then

$$k_{7,r} \leqslant k_{7,r-16} + \lfloor 16 \log_2 7 \rfloor + 1 = k_{7,r-16} + 45 < k_{7,r-16} + 46\,.$$

(v) $(b_{7,r-21}\dots b_{7,r}) = (0^6 2^5 1^5 0^6)$ implies $k_{7,r} = k_{7,r-21} + 60$. Then

$$k_{7,r} \leqslant k_{7,r-21} + \lfloor 21 \log_2 7 \rfloor + 1 = k_{7,r-21} + 59 < k_{7,r-21} + 60\,.$$

□

To illustrate the beginning of the procedure, we propose Figure B.5. In this figure, a red arrow means that the transition is impossible because of a case in Lemma B.3.

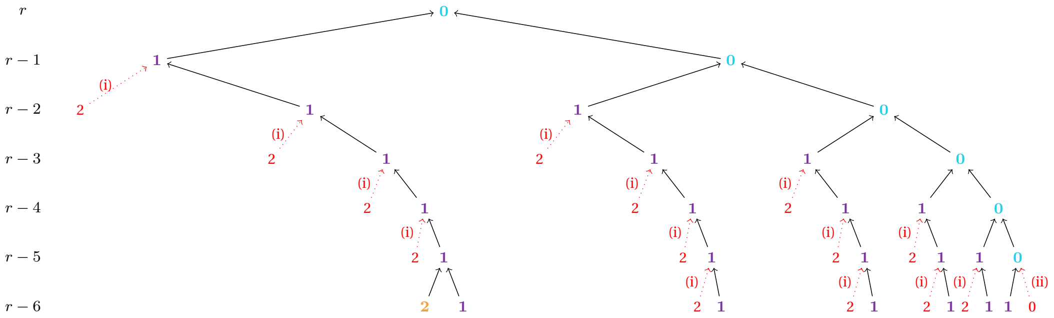


Figure B.5: *Impossible subsequences in the sequence* $(b_{7,r})_{r>0}$.

Proposition B.3. *Let* $(k_{7,r})_{r>0}$ *and* $(b_{7,r})_{r>0}$ *be the sequences defined in Lemma B.3. Then, for any* $r \geqslant 1$*, there exists* $\mathsf{b} \in \{0,1,2\}$ *such that one of the following situations occurs:*

(i) $(b_{7,r-i}\dots b_{7,r}) = (\mathsf{b}\dots\mathsf{b}) + (10^i)$*, for all* $i = 1,\dots,5$*,*

(ii) $(b_{7,r-5} \ldots b_{7,r}) = (\mathsf{b} \ldots \mathsf{b}) + (0^6)$.

Proof. Without loss of generality we set $b_{7,r} = 0$. As we are considering possible sequences on the right part of the graph there is no restriction from Lemma B.3 for the few cases we want to check. Let us use Figure B.6 for a better overview of the different steps of this proof. Starting with the node 0 at the top, there are two branches so that we have either $b_{7,r-1} = 1$ or $b_{7,r-1} = 0$.

- **If $\boldsymbol{b_{7,r-1} = 1}$:** this is a left child implying that we stop the process. We obtain $(b_{7,r-1}b_{7,r}) = (10)$, which corresponds to the sequence **(i)** with $i = 1$.

- **If $\boldsymbol{b_{7,r-1} = 0}$:** we have a node with two branches, implying that we have either $b_{7,r-2} = 1$ or $b_{7,r-2} = 0$.

- **If $\boldsymbol{b_{7,r-2} = 1}$:** this is a left child so that $(b_{7,r-2} \ldots b_{7,r}) = (10^2)$, leading to the sequence **(i)** with $i = 2$.

- **If $\boldsymbol{b_{7,r-2} = 0}$:** we have a node with two branches, implying that $b_{7,r-3} \in \{0, 1\}$.

- **If $\boldsymbol{b_{7,r-3} = 1}$:** we have a left child, so we stop the process. We get $(b_{7,r-3} \ldots b_{7,r}) = (10^3)$, which corresponds to the sequence **(i)** with $i = 3$.

- **If $\boldsymbol{b_{7,r-3} = 0}$:** we have a node with two branches, implying that $b_{7,r-4} \in \{0, 1\}$.

- **If $\boldsymbol{b_{7,r-4} = 1}$:** this is a left child, leading to the sequence **(i)** with $i = 4$ since we have $(b_{7,r-4} \ldots b_{7,r}) = (10^4)$.

- **If $\boldsymbol{b_{7,r-4} = 0}$:** we have a node with two branches, implying that $b_{7,r-5} \in \{0, 1\}$.

- **If $\boldsymbol{b_{7,r-5} = 1}$:** we have $(b_{7,r-5} \ldots b_{7,r}) = (10^5)$, so this is the sequence **(i)** with $i = 5$.

- **If $\boldsymbol{b_{7,r-5} = 0}$:** we have $(b_{7,r-5} \ldots b_{7,r}) = (0^6)$, which corresponds to the last sequence **(ii)**.

□

In Figure B.6, we can see the six possible situations of Proposition B.3. For the sake of clarity, we omitted the impossible transitions. We can also observe a well-structured pattern in the tree. This looks encouraging to better understand the property of the sequence $(b_{7,r})_{r>0}$, while for the case MiMC_5 and MiMC_9 it seemed complicated to give a precise understanding of the sub-sequences in $(b_{5,r})_{r>0}$ and $(b_{9,r})_{r>0}$, as discussed in Sections B.1.1 and B.1.2.

Let us notice that the denominators of semi-convergents of $\log_2 7$ are

$$\mathfrak{D}_7 = \{1, 2, 3, 4, 5, 6, 11, 16, 21, 26, 31, 57, 83, 109, 135, 244, 353, 462, 571, 680, \ldots\} .$$

We notice that the integers i involved in the impossible sub-sequences of Lemma B.3 and the possible sub-sequences of Proposition B.3 are part of the set $\mathfrak{D}_7$.

Moreover, in Section 6.3.2, we saw that we could construct exponents

$$\begin{aligned} e_{11} &= 2^{28} - 9 && \text{at round } 11\,, \\ e_{12} &= 2^{31} - 9 && \text{at round } 12\,, \\ e_{13} &= 2^{34} - 9 && \text{at round } 13\,, \\ e_{14} &= 2^{37} - 9 && \text{at round } 14\,, \end{aligned}$$

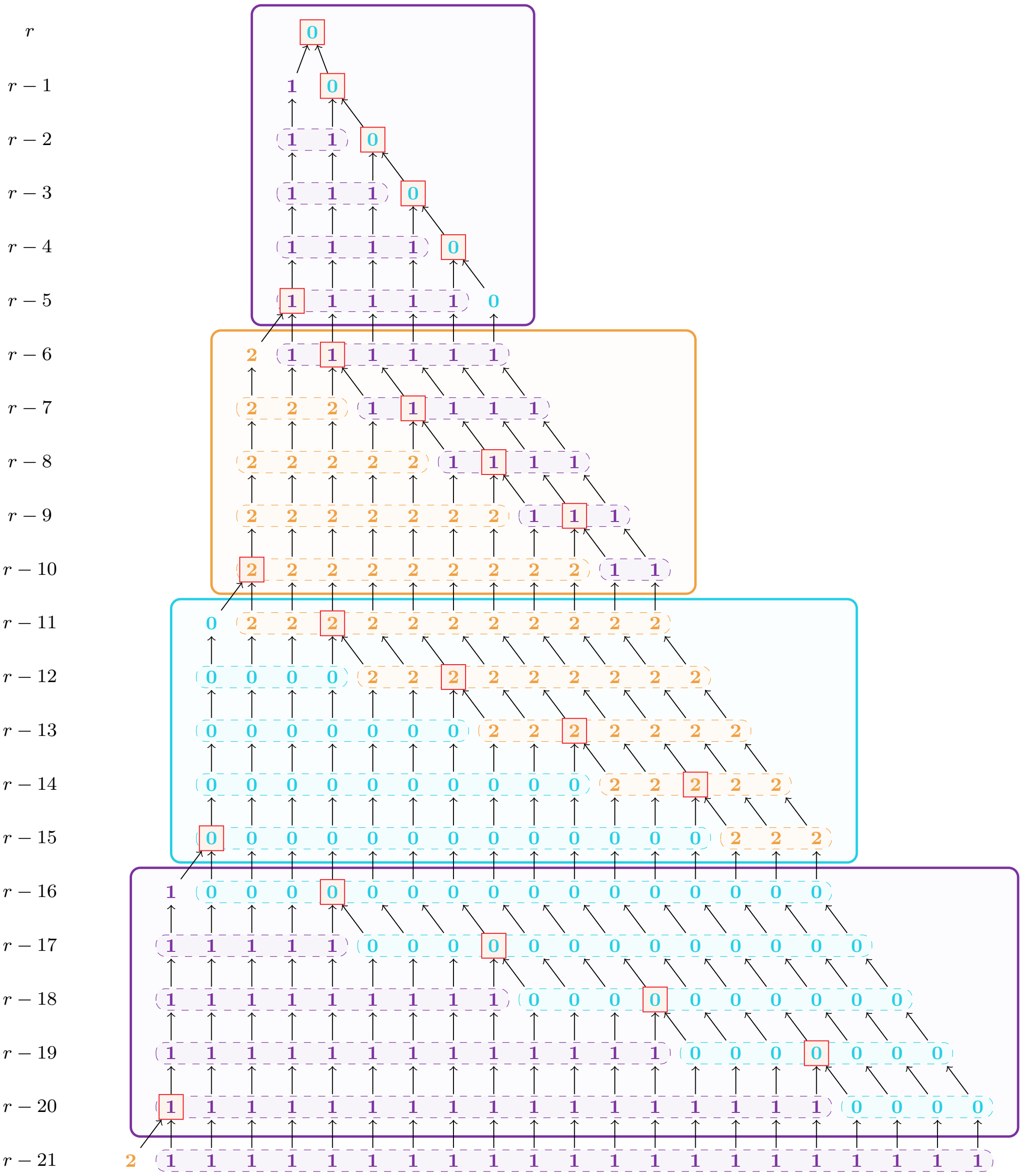

r 0
$r-1$ 1 0
$r-2$ 1 1 0
$r-3$ 1 1 1 0
$r-4$ 1 1 1 1 0
$r-5$ 1 1 1 1 1 0
$r-6$ 2 1 1 1 1 1 1
$r-7$ 2 2 2 1 1 1 1 1
$r-8$ 2 2 2 2 2 1 1 1 1
$r-9$ 2 2 2 2 2 2 2 1 1 1
$r-10$ 2 2 2 2 2 2 2 2 2 1 1
$r-11$ 0 2 2 2 2 2 2 2 2 2 2 2
$r-12$ 0 0 0 0 2 2 2 2 2 2 2 2 2
$r-13$ 0 0 0 0 0 0 0 2 2 2 2 2 2 2
$r-14$ 0 0 0 0 0 0 0 0 0 0 2 2 2 2 2
$r-15$ 0 0 0 0 0 0 0 0 0 0 0 0 0 2 2 2
$r-16$ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
$r-17$ 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0
$r-18$ 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0
$r-19$ 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0
$r-20$ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0
$r-21$ 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Figure B.6: *The different subsequences that could occur in the sequence* $(b_{7,r})_{r>0}$.

starting from $e_{10} = 2^{28} - 9$ at round 10. It is worth observing that we have

$$\begin{aligned}
(b_{7,10}b_{7,11}) &= (10)\,,\\
(b_{7,10}b_{7,11}b_{7,12}) &= (100)\,,\\
(b_{7,10}b_{7,11}b_{7,12}b_{7,13}) &= (1000)\,,\\
(b_{7,10}b_{7,11}b_{7,12}b_{7,13}b_{7,14}) &= (10000)\,,
\end{aligned}$$

which are exactly the first four forms of Proposition B.3. This observation suggests that there might exist a link between the tracing of exponents and the sequences of $(b_{7,r})_{r>0}$. More precisely, it seems that to construct exponents of maximum-weight it is necessary to go back to the first round $(r - i)$ such that $b_{7,r-i} = 1$. As a consequence a better understanding of the sequences of $(b_{7,r})_{r>0}$ would imply a better understanding of how to construct exponents of maximum weight.

B.2.2 When using MiMC_{2^j-1}, with $j \in \{4, 5, 6\}$

Let us adapt the result to MiMC_{15}, MiMC_{31} and MiMC_{63}. In this section we have chosen not to propose a tree representation for the impossible sequences because the figure would have become too complex. However, we still suggest Figures B.7, B.8 and B.9 for the possible sequences.

In what follows, we will need one lemma for each $d = 2^j - 1$, where $j \in \{4, 5, 6\}$. Moreover, we will be able to prove Proposition 7.2 that exhibits some patterns in the sequences $(b_{d,r})_{r>0}$.

Lemma B.4. *Let* $(k_{15,r})_{r>0}$ *and* $(b_{15,r})_{r>0}$ *be the sequences defined by* $k_{15,r} = \lfloor r \log_2 15 \rfloor$ *and* $b_{15,r} = k_{15,r} \bmod 4$*. Let* b *be any value in* $\{0, 1, 2, 3\}$*. Then, for any* $r \geqslant 1$ *none of the following situations can occur:*

(i) $(b_{15,r-i} \dots b_{15,r}) = (\mathsf{b} \dots \mathsf{b}) + (21^{i-1}0)$*, for all* $i = 2, \dots, 10$*,*

(ii) $(b_{15,r-11} \dots b_{15,r}) = (\mathsf{b} \dots \mathsf{b}) + (0^{12})$*,*

(iii) $(b_{15,r-21} \dots b_{15,r}) = (\mathsf{b} \dots \mathsf{b}) + (32^{10}1^{10}0)$*,*

(iv) $(b_{15,r-32} \dots b_{15,r}) = (\mathsf{b} \dots \mathsf{b}) + (03^{10}2^{11}1^{10}0)$*.*

Proof. In this proof, we will use that:

$$\forall r, i, \quad k_{15,r-i} + \lfloor i \log_2 15 \rfloor \leqslant k_{15,r} \leqslant k_{15,r-i} + \lfloor i \log_2 15 \rfloor + 1 \,.$$

Let $\mathsf{b} = 0$. Recall that $\log_2 15 \approx 3.907$, then we can derive the following contradictions:

(i) If $(b_{15,r-i} \dots b_{15,r}) = (21^{i-1}0)$ for all $i = 2, \dots, 10$, then it implies

$$k_{15,r} = k_{15,r-i} + 3 + 4(i-2) + 3 = k_{15,r-i} + 6 + 4(i-2) \,,$$

so that

$$k_{15,r} \geqslant k_{15,r-i} + \lfloor i \log_2 15 \rfloor = k_{15,r-i} + 7 + 4(i-2) > k_{15,r-i} + 6 + 4(i-2) \,.$$

(ii) If $(b_{15,r-11} \dots b_{15,r}) = (0^{12})$, then it implies

$$k_{15,r} = k_{15,r-11} + 4 \times 11 = k_{15,r-11} + 44 \,,$$

so that

$$k_{15,r} \leqslant k_{15,r-11} + \lfloor 11 \log_2 15 \rfloor + 1 = k_{15,r-11} + 43 < k_{15,r-11} + 44 \,.$$

(iii) If $(b_{15,r-21} \dots b_{15,r}) = (32^{10}1^{10}0)$, then it implies

$$k_{15,r} = k_{15,r-21} + 3 + (4 \times 9 + 3) \times 2 = k_{15,r-21} + 81 \,,$$

so that

$$k_{15,r} \geqslant k_{15,r-21} + \lfloor 21 \log_2 15 \rfloor = k_{15,r-21} + 82 > k_{15,r-21} + 81 \,.$$

(iv) If $(b_{15,r-32}\dots b_{15,r}) = (03^{10}2^{11}1^{10}0)$, then it implies

$$k_{15,r} = k_{15,r-32} + 3 + 4 \times 9 + 3 + 4 \times 10 + 3 + 4 \times 9 + 3 = k_{15,r-32} + 124\,,$$

so that

$$k_{15,r} \geqslant k_{15,r-32} + \lfloor 32 \log_2 15 \rfloor = k_{15,r-32} + 125 > k_{15,r-32} + 124\,.$$

□

We illustrate the different sub-sequences that can be observed in Figure B.7.

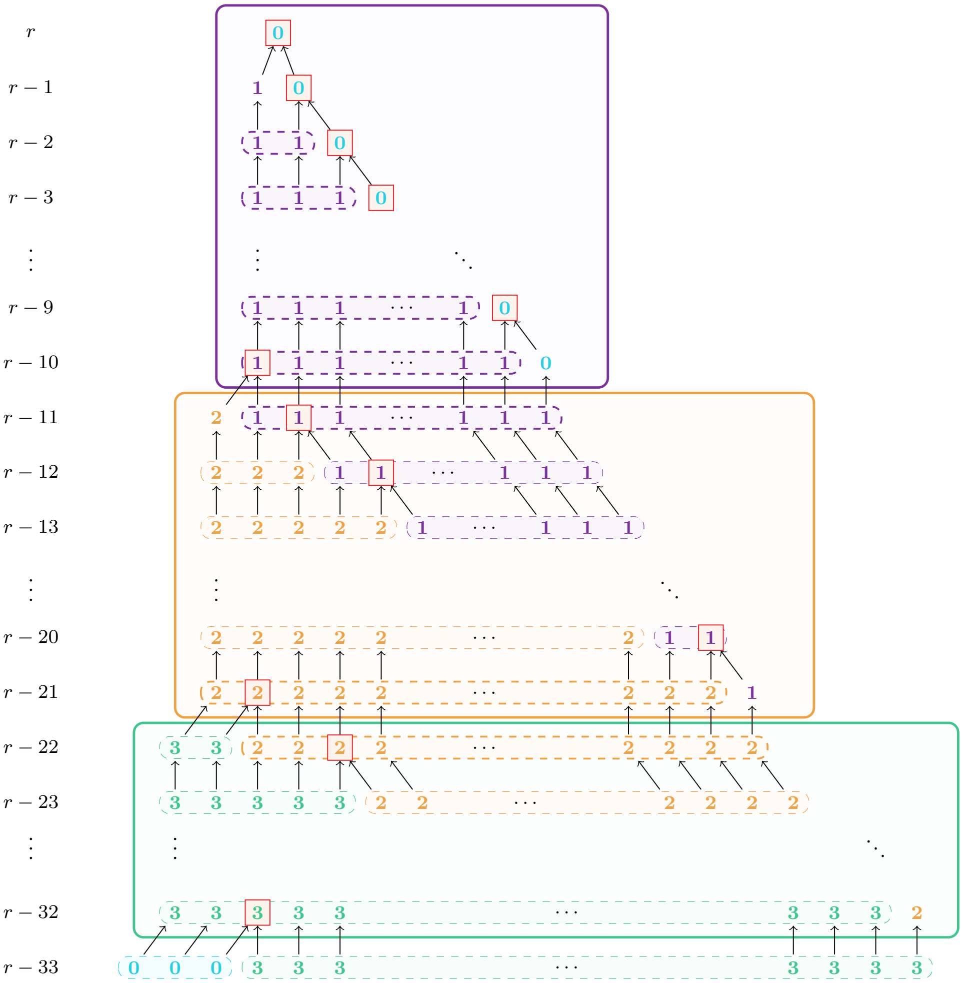

r 0
$r-1$ 1 0
$r-2$ 1 1 0
$r-3$ 1 1 1 0
⋮ ⋮ ⋱
$r-9$ 1 1 1 ··· 1 0
$r-10$ 1 1 1 ··· 1 1 0
$r-11$ 2 1 1 1 ··· 1 1 1
$r-12$ 2 2 2 1 1 ··· 1 1 1
$r-13$ 2 2 2 2 2 1 ··· 1 1 1
⋮ ⋮ ⋱
$r-20$ 2 2 2 2 2 ··· 2 1 1
$r-21$ 2 2 2 2 2 ··· 2 2 2 1
$r-22$ 3 3 2 2 2 2 ··· 2 2 2 2
$r-23$ 3 3 3 3 3 2 2 ··· 2 2 2 2
⋮ ⋮ ⋱
$r-32$ 3 3 3 3 3 ··· 3 3 3 2
$r-33$ 0 0 0 3 3 3 ··· 3 3 3 3

Figure B.7: The different subsequences that could occur in the sequence $(b_{15,r})_{r>0}$.

Lemma B.5. *Let $(k_{31,r})_{r>0}$ and $(b_{31,r})_{r>0}$ be the sequences defined by $k_{31,r} = \lfloor r \log_2 31 \rfloor$ and $b_{31,r} = k_{31,r} \bmod 5$. Let b be any value in $\{0,\dots,4\}$. Then, for any $r \geqslant 1$ none of the following situations can occur:*

(i) $(b_{31,r-i}\dots b_{31,r}) = (\mathsf{b}\dots\mathsf{b}) + (21^{i-1}0)$*, for all* $i = 2,\dots,21$,

(ii) $(b_{31,r-22} \ldots b_{31,r}) = (\mathsf{b} \ldots \mathsf{b}) + (0^{23})$,

(iii) $(b_{31,r-43} \ldots b_{31,r}) = (\mathsf{b} \ldots \mathsf{b}) + (32^{21}1^{21}0)$,

(iv) $(b_{31,r-65} \ldots b_{31,r}) = (\mathsf{b} \ldots \mathsf{b}) + (43^{21}2^{22}1^{21}0)$,

(v) $(b_{31,r-87} \ldots b_{31,r}) = (\mathsf{b} \ldots \mathsf{b}) + (04^{21}3^{22}2^{22}1^{21}0)$.

Proof. Without loss of generality, we set $\mathsf{b} = 0$ and we use that

$$\forall r, i, \quad k_{31,r-i} + \lfloor i \log_2 31 \rfloor \leqslant k_{31,r} \leqslant k_{31,r-i} + \lfloor i \log_2 31 \rfloor + 1 ,$$

with $\log_2 31 \approx 4.954$. Then we can derive the following contradictions:

(i) If $(b_{31,r-i} \ldots b_{31,r}) = (21^{i-1}0)$ for all $i = 2, \ldots, 21$, then it implies

$$k_{31,r} = k_{31,r-i} + 4 + 5(i-2) + 4 = k_{31,r-i} + 8 + 5(i-2) ,$$

so that

$$k_{31,r} \geqslant k_{31,r-i} + \lfloor i \log_2 31 \rfloor = k_{31,r-i} + 9 + 5(i-2) > k_{31,r-i} + 8 + 5(i-2) .$$

(ii) If $(b_{31,r-22} \ldots b_{31,r}) = (0^{23})$ then it implies

$$k_{31,r} = k_{31,r-22} + 5 \times 22 = k_{31,r-22} + 110 ,$$

so that

$$k_{31,r} \leqslant k_{31,r-22} + \lfloor 22 \log_2 31 \rfloor + 1 = k_{31,r-22} + 109 < k_{31,r-22} + 110 .$$

(iii) If $(b_{31,r-43} \ldots b_{31,r}) = (32^{21}1^{21}0)$ then it implies

$$k_{31,r} = k_{31,r-43} + 4 + (5 \times 20 + 4) \times 2 = k_{31,r-43} + 212 ,$$

so that

$$k_{31,r} \geqslant k_{31,r-43} + \lfloor 43 \log_2 31 \rfloor = k_{31,r-43} + 213 > k_{31,r-43} + 212 .$$

(iv) If $(b_{31,r-65} \ldots b_{31,r}) = (43^{21}2^{22}1^{21}0)$ then it implies

$$k_{31,r} = k_{31,r-65} + 4 + 5 \times 20 + 4 + 5 \times 21 + 4 + 5 \times 20 + 4 = k_{31,r-65} + 321 ,$$

so that

$$k_{31,r} \geqslant k_{31,r-65} + \lfloor 65 \log_2 31 \rfloor = k_{31,r-65} + 322 > k_{31,r-65} + 321 .$$

(v) If $(b_{31,r-87} \ldots b_{31,r}) = (04^{21}3^{22}2^{22}1^{21}0)$ then it implies

$$k_{31,r} = k_{31,r-87} + 4 + 5 \times 20 + 4 + (5 \times 21 + 4) \times 2 + 5 \times 20 + 4 = k_{31,r-87} + 430 ,$$

so that

$$k_{31,r} \geqslant k_{31,r-87} + \lfloor 87 \log_2 31 \rfloor = k_{31,r-87} + 431 > k_{31,r-87} + 430 .$$

□

We show the different sub-sequences in Figure B.8.

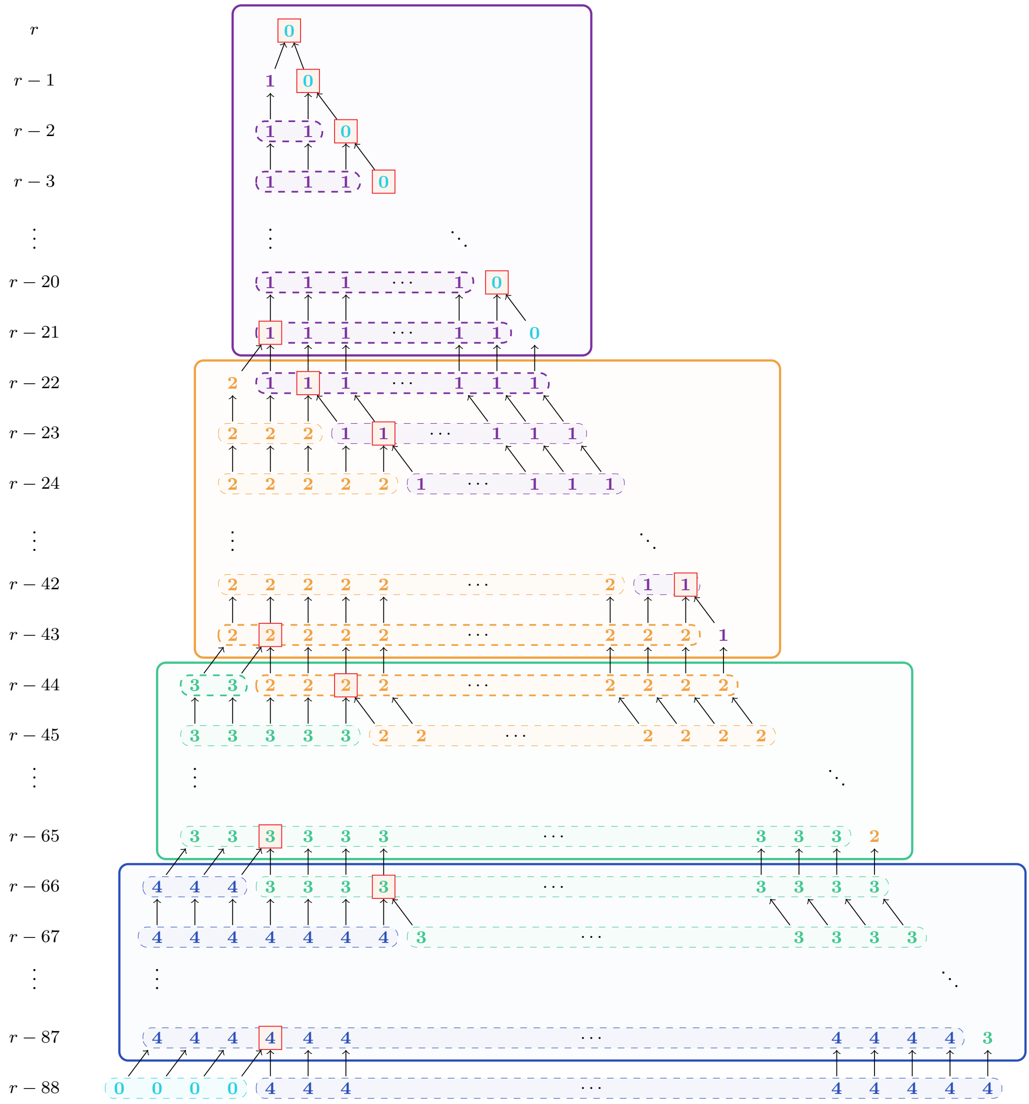


Figure B.8: *The different subsequences that could occur in the sequence* $(b_{31,r})_{r>0}$.

Lemma B.6. *Let* $(k_{63,r})_{r>0}$ *and* $(b_{63,r})_{r>0}$ *be the sequences defined by* $k_{63,r} = \lfloor r \log_2 63 \rfloor$ *and* $b_{63,r} = k_{63,r} \bmod 6$. *Let* b *be any value in* $\{0, \ldots, 5\}$. *Then, for any* $r \geqslant 1$ *none of the following situations can occur:*

(i) $(b_{63,r-i} \ldots b_{63,r}) = (\mathsf{b} \ldots \mathsf{b}) + (21^{i-1}0)$, *for all* $i = 2, \ldots, 44$,

(ii) $(b_{63,r-45} \ldots b_{63,r}) = (\mathsf{b} \ldots \mathsf{b}) + (0^{46})$,

(iii) $(b_{63,r-89} \ldots b_{63,r}) = (\mathsf{b} \ldots \mathsf{b}) + (1^{45}0^{45})$,

(iv) $(b_{63,r-133} \ldots b_{63,r}) = (\mathsf{b} \ldots \mathsf{b}) + (2^{45}1^{44}0^{45})$,

(v) $(b_{63,r-177} \dots b_{63,r}) = (\mathsf{b} \dots \mathsf{b}) + (3^{45}2^{44}1^{44}0^{45})$,

(vi) $(b_{63,r-221} \dots b_{63,r}) = (\mathsf{b} \dots \mathsf{b}) + (4^{45}3^{44}2^{44}1^{44}0^{45})$.

Proof. Without loss of generality, we set $\mathsf{b} = 0$ and we use that:

$$\forall r, i, \quad k_{63,r-i} + \lfloor i \log_2 63 \rfloor \leqslant k_{63,r} \leqslant k_{63,r-i} + \lfloor i \log_2 63 \rfloor + 1 \,,$$

where $\log_2 63 \approx 5.977$. Then we can derive the following contradictions:

(i) $(b_{63,r-i} \dots b_{63,r}) = (21^{i-1}0)$ for all $i = 2, \dots, 44$ implies

$$k_{63,r} = k_{63,r-i} + 5 + 6(i-2) + 5 = k_{63,r-i} + 10 + 6(i-2) \,,$$

so that

$$k_{63,r} \geqslant k_{63,r-i} + \lfloor i \log_2 63 \rfloor = k_{63,r-i} + 11 + 6(i-2) > k_{63,r-i} + 10 + 6(i-2) \,.$$

(ii) $(b_{63,r-45} \dots b_{63,r}) = (0^{46})$ implies

$$k_{63,r} = k_{63,r-45} + 6 \times 45 = k_{63,r-45} + 270 \,,$$

so that

$$k_{63,r} \leqslant k_{63,r-45} + \lfloor 45 \log_2 63 \rfloor + 1 = k_{63,r-45} + 269 < k_{63,r-45} + 270 \,.$$

(iii) $(b_{63,r-89} \dots b_{63,r}) = (1^{45}0^{45})$ implies

$$k_{63,r} = k_{63,r-89} + 6 \times 44 + 5 + 6 \times 44 = k_{63,r-89} + 533 \,,$$

so that

$$k_{63,r} \leqslant k_{63,r-89} + \lfloor 89 \log_2 63 \rfloor + 1 = k_{63,r-89} + 532 < k_{63,r-89} + 533 \,.$$

(iv) $(b_{63,r-133} \dots b_{63,r}) = (2^{45}1^{44}0^{45})$ implies

$$k_{63,r} = k_{63,r-133} + 6 \times (44 \times 2 + 43) + 5 \times 2 = k_{63,r-133} + 796 \,,$$

so that

$$k_{63,r} \leqslant k_{63,r-133} + \lfloor 133 \log_2 63 \rfloor + 1 = k_{63,r-133} + 795 < k_{63,r-133} + 796 \,.$$

(v) $(b_{63,r-177} \dots b_{63,r}) = (3^{45}2^{44}1^{44}0^{45})$ implies

$$k_{63,r} = k_{63,r-177} + 6 \times (44 \times 2 + 43 \times 2) + 5 \times 3 = k_{63,r-177} + 1059 \,,$$

so that

$$k_{63,r} \leqslant k_{63,r-177} + \lfloor 177 \log_2 63 \rfloor + 1 = k_{63,r-177} + 1058 < k_{63,r-177} + 1059 \,.$$

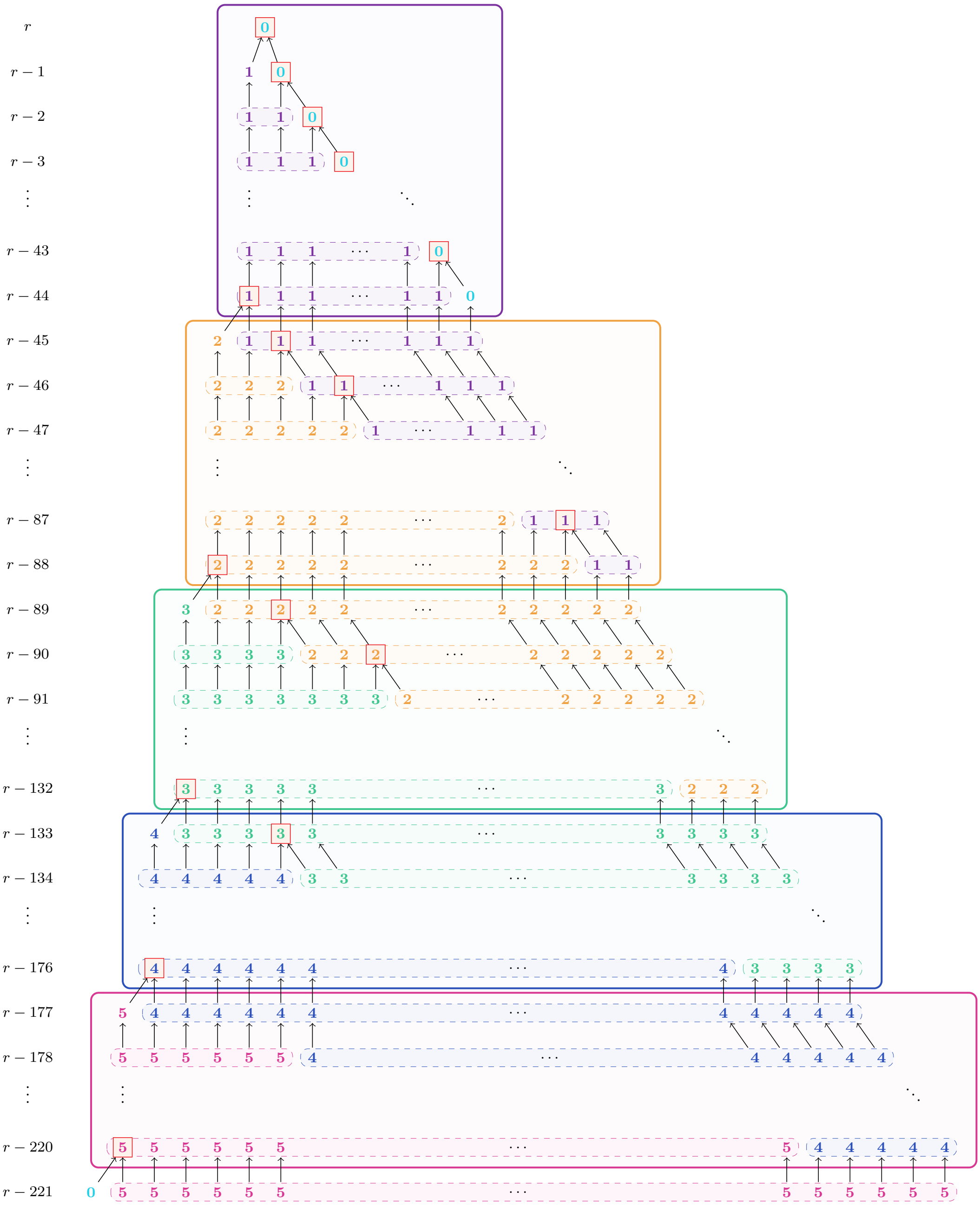


Figure B.9: The different subsequences that could occur in the sequence $(b_{63,r})_{r>0}$.

(vi) $(b_{63,r-221}\ldots b_{63,r}) = (4^{45}3^{44}2^{44}1^{44}0^{45})$ implies

$$k_{63,r} = k_{63,r-221} + 6\times(44\times 2 + 43\times 3) + 5\times 4 = k_{63,r-221} + 1322\,,$$

so that

$$k_{63,r} \leqslant k_{63,r-221} + \lfloor 221 \log_2 63 \rfloor + 1 = k_{63,r-221} + 1321 < k_{63,r-177} + 1322 \, .$$

□

The different sub-sequences are represented in Figure B.9.

In what follows we aim at proving Proposition 7.2, that generalize the result of Proposition B.3. Let us recall that this proposition identifies the possible subsequences for MiMC_d for $d \in \{7, 15, 31, 63\}$, i.e. if $(k_{d,r})_{r>0}$ and $(b_{d,r})_{r>0}$ are the sequences defined by $k_{d,r} = \lfloor r \log_2 d \rfloor$ and $b_{d,r} = k_{d,r} \bmod j$. Then, for any $r \geqslant 1$, there exists $\mathsf{b} \in \{0, \ldots, j\}$ such that one of the following situations occurs:

(i) $(b_{d,r-i} \ldots b_{d,r}) = (\mathsf{b} \ldots \mathsf{b}) + (10^i)$, for all $i = 1, \ldots, \gamma_d - 1$,

(ii) $(b_{d,r-\gamma_d-1} \ldots b_{d,r}) = (\mathsf{b} \ldots \mathsf{b}) + (0^{\gamma_d})$,

where γ_d is a constant defined as follows:

$$\gamma_7 = 6 \, , \qquad \gamma_{15} = 11 \, , \qquad \gamma_{31} = 22 \, , \qquad \text{and} \qquad \gamma_{63} = 45 \, .$$

Proof of Proposition 7.2. We fix $\mathsf{b} = 0$. The case $j = 3$ corresponds to Proposition B.3. Let us generalize the procedure. Let $b_{d,r} = 0$, then we will look at the $b_{d,r-i}$. As we are again considering possible sequences on the right part of the graph there is no restriction from Lemmas B.4, B.5 or B.6 for the few cases we want to check. For a deeper insight of the different steps of this proof, we will also rely on Figures B.7, B.8 and B.9. Starting with the node 0 at the top, there are 2 branches implying that for all cases we have either $b_{d,r-1} = 1$ or $b_{d,r-1} = 0$.

- **If $\boldsymbol{b_{d,r-1} = 1}$:** we have a left child meaning that we stop the process. We obtain $(b_{d,r-1} b_{d,r}) = (10)$, which corresponds to the sequence **(i)** with $i = 1$.
- **If $\boldsymbol{b_{d,r-1} = 0}$:** we have a node with two branches, implying that we have either $b_{d,r-2} = 1$ or $b_{d,r-2} = 0$.
- **If $\boldsymbol{b_{7,r-2} = 1}$:** this is **(i)** with $i = 2$.
  The same argument holds for all $i = 1, \ldots, \gamma_d$ so that we can cover all cases **(i)**.
- **If $\boldsymbol{b_{d,r-\gamma_d} = 0}$:** we have $(b_{d,r-\gamma_d} \ldots b_{d,r}) = (0^{\gamma_d+1})$, which corresponds to the last sequence **(ii)**.

□

Let us observe that the denominators of semi-convergents of $\log_2 d$ for $d \in \{15, 31, 63\}$ are:

$$\begin{aligned}
\mathfrak{D}_{15} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 21, 32, 43, 75, 118, 161, 204, 247, 290, 537, 827, \ldots\} \, , \\
\mathfrak{D}_{31} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 43, 65, 87, \\
&\quad 109, 131, 240, 371, 502, 633, 764, 895, \ldots\} \, , \\
\mathfrak{D}_{63} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, \\
&\quad 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 89, \\
&\quad 133, 177, 221, 265, 309, 353, 397, 441, 485, 529, 573, 617, 661, 705, 749, \\
&\quad 793, 837, 881, 925, 969, \ldots\} \, .
\end{aligned}$$

Unlike MiMC_5 and MiMC_9, in the case of MiMC_d with d of the form $d = 2^j - 1$ the integers i involved in the impossible and possible sub-sequences from Lemmas B.4, B.5, B.6 and Corollary 7.2 are part of the denominators of semi-convergents of $\log_2 d$.

B.3 When using MiMC_d, with other d

In Chapter 5, we saw that the families of missing exponents (i.e. integers equal to 5 or 7 modulo 8) for MiMC_3 are the same as for MiMC_{11}, since $11 \equiv 3 \bmod 8$. It is therefore interesting to ask whether such similarities can also be observed when analyzing the sequences of $(b_{d,r})_{r>0}$.

Let $(k_{11,r})_{r>0}$ and $(b_{11,r})_{r>0}$ be the sequences defined by $k_{11,r} = \lfloor r \log_2 11 \rfloor$ and $b_{11,r} = k_{11,r} \bmod 10$. We first investigate the impossible sub-sequences in $(b_{11,r})_{r>0}$.

Lemma B.7. *Let $(b_{11,r})_{r>0}$ be the sequence defined by $b_{11,r} = k_{11,r} \bmod 10$. Then, for any $r \geqslant 1$ none of the following situations can occur, where* b *can take any value in $\{0, \ldots 9\}$:*

(i) $(b_{11,r-2} \ldots b_{11,r}) = (\mathsf{bbb}) + (260)$,

(ii) $(b_{11,r-3} \ldots b_{11,r}) = (\mathsf{b} \ldots \mathsf{b}) + (1470)$,

(iii) $(b_{11,r-5} \ldots b_{11,r}) = (\mathsf{b} \ldots \mathsf{b}) + (470470) = (\mathsf{b} \ldots \mathsf{b}) + ((470)^2)$,

(iv) $(b_{11,r-7} \ldots b_{11,r}) = (\mathsf{b} \ldots \mathsf{b}) + (70370470)$,

(v) $(b_{11,r-9} \ldots b_{11,r}) = (\mathsf{b} \ldots \mathsf{b}) + (0360370470)$,

(vi) $(b_{11,r-11} \ldots b_{11,r}) = (\mathsf{b} \ldots \mathsf{b}) + (369360370470)$,

(vii) $(b_{11,r-13} \ldots b_{11,r}) = (\mathsf{b} \ldots \mathsf{b}) + (48158259269360)$.

Proof. We set $\mathsf{b} = 0$ and we use that:

$$\forall r, i, \quad k_{11,r-i} + \lfloor i \log_2 11 \rfloor \leqslant k_{11,r} \leqslant k_{11,r-i} + \lfloor i \log_2 11 \rfloor + 1 \,,$$

where $\log_2 11 \approx 3.459$. Then we can derive the following contradictions:

(i) $(b_{11,r-2} b_{11,r-1} b_{11,r}) = (260)$ implies

$$k_{11,r} = k_{11,r-2} + 4 + 4 = k_{11,r-2} + 8 \,,$$

so that

$$k_{11,r} \leqslant k_{11,r-2} + \lfloor 2 \log_2 11 \rfloor + 1 = k_{11,r-2} + 7 < k_{11,r-2} + 8 \,.$$

(ii) $(b_{11,r-3} \ldots b_{11,r}) = (1470)$ implies

$$k_{11,r} = k_{11,r-3} + 3 + 3 + 3 = k_{11,r-3} + 9 \,,$$

so that

$$k_{11,r} \geqslant k_{11,r-3} + \lfloor 3 \log_2 11 \rfloor = k_{11,r-3} + 10 > k_{11,r-2} + 9 \,.$$

(iii) $(b_{11,r-5} \ldots b_{11,r}) = ((470)^2)$ implies

$$k_{11,r} = k_{11,r-5} + (3 \times 2) \times 2 + 4 = k_{11,r-5} + 16 \,,$$

so that

$$k_{11,r} \geqslant k_{11,r-5} + \lfloor 5 \log_2 11 \rfloor = k_{11,r-5} + 17 > k_{11,r-5} + 16 \,.$$

(iv) $(b_{11,r-7}\dots b_{11,r}) = (70370470)$ implies

$$k_{11,r} = k_{11,r-7} + 3\times 2 + 4 + 3 + 4 + 3\times 2 = k_{11,r-7} + 23\,,$$

so that

$$k_{11,r} \geqslant k_{11,r-7} + \lfloor 7\log_2 11\rfloor = k_{11,r-7} + 24 > k_{11,r-7} + 23\,.$$

(v) $(b_{11,r-9}\dots b_{11,r}) = (0360370470)$ implies

$$k_{11,r} = k_{11,r-9} + 3\times 2 + 4 + (3+4)\times 2 + 3\times 2 = k_{11,r-9} + 30\,,$$

so that

$$k_{11,r} \geqslant k_{11,r-9} + \lfloor 9\log_2 11\rfloor = k_{11,r-9} + 31 > k_{11,r-9} + 30\,.$$

(vi) $(b_{11,r-11}\dots b_{11,r}) = (369360370470)$ implies

$$k_{11,r} = k_{11,r-11} + 3\times 2 + 4 + (3+4)\times 3 + 3\times 2 = k_{11,r-11} + 37\,,$$

so that

$$k_{11,r} \geqslant k_{11,r-11} + \lfloor 11\log_2 11\rfloor = k_{11,r-11} + 38 > k_{11,r-11} + 37\,.$$

(vii) $(b_{11,r-13}\dots b_{11,r}) = (48158259269360)$ implies

$$k_{11,r} = k_{11,r-13} + 4 + (3+4)\times 6 = k_{11,r-13} + 46\,,$$

so that

$$k_{11,r} \leqslant k_{11,r-13} + \lfloor 13\log_2 11\rfloor + 1 = k_{11,r-13} + 45 < k_{11,r-13} + 46\,.$$

□

In Figure B.10, a red arrow means is an impossible transition because of a case in Lemma B.7.

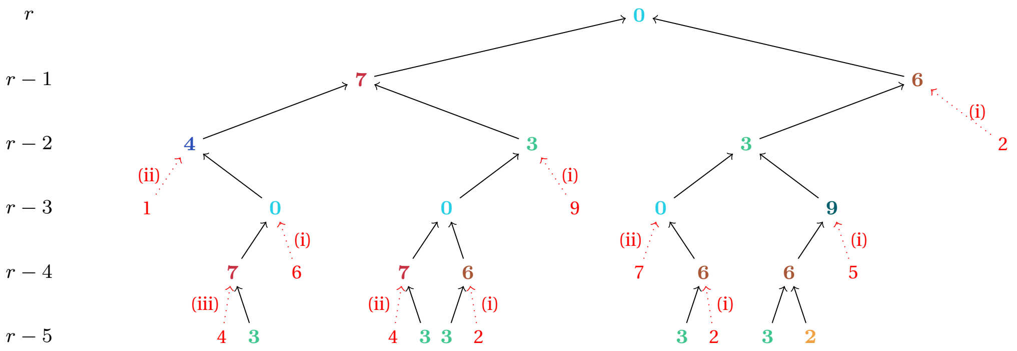


Figure B.10: *Impossible subsequences in the sequence* $(b_{11,r})_{r>0}$.

Proposition B.4. *Let* $(k_{11,r})_{r>0}$ *and* $(b_{11,r})_{r>0}$ *be the sequences defined in Lemma B.7. Then, for any* $r \geqslant 1$*, there exists* $\mathsf{b} \in \{0\dots,9\}$ *such that one of the following situations occurs:*

(i) $(b_{11,r-1}b_{11,r}) = (\mathsf{bb}) + (70)$,

(ii) $(b_{11,r-3} \dots b_{11,r}) = (\mathsf{b} \dots \mathsf{b}) + (0360)$,

(iii) $(b_{11,r-5} \dots b_{11,r}) = (\mathsf{b} \dots \mathsf{b}) + (369360)$,

(iv) $(b_{11,r-7} \dots b_{11,r}) = (\mathsf{b} \dots \mathsf{b}) + (69269360)$,

(v) $(b_{11,r-9} \dots b_{11,r}) = (\mathsf{b} \dots \mathsf{b}) + (9259269360)$,

(vi) $(b_{11,r-11} \dots b_{11,r}) = (\mathsf{b} \dots \mathsf{b}) + (258259269360)$,

(vii) $(b_{11,r-11} \dots b_{11,r}) = (\mathsf{b} \dots \mathsf{b}) + (158259269360)$.

Proof. Let $b_{11,r} = 0$, then we will look at the $b_{11,r-i}$ according to Lemma B.7. We will refer to Figure B.11 to get a better overview of the steps of this proof,. We start with the node 0 at the top. Then, there are two branches implying that we have either $b_{11,r-1} = 7$ or $b_{11,r-1} = 6$.

- **If $b_{11,r-1} = 7$:** this is a left child so that we stop the process. We have $(b_{11,r-1}b_{11,r}) = (70)$, which corresponds to the first sequence **(i)**.

- **If $b_{11,r-1} = 6$:** we know from Lemma B.7-**(i)** that we have $(b_{11,r-2} \dots b_{11,r}) = (360)$. In Figure B.11, we indeed observe that the node, on the right, at round $(r-1)$ has only one branching. Then, at round $(r-2)$, the node 3 has two branches, either $b_{11,r-3} = 0$ or $b_{11,r-3} = 9$.

- **If $b_{11,r-3} = 0$:** we have a left child, which leads to the second sequence **(ii)** since we have $(b_{11,r-3} \dots b_{11,r}) = (0360)$.

- **If $b_{11,r-3} = 9$:** we have necessarily $(b_{11,r-4} \dots b_{11,r}) = (69360)$, because of Lemma B.7-**(i)** applied with $\mathsf{b} = 3$. In Figure B.11, this observation corresponds to the unique branching for the node, on the right, at round $(r-3)$. Then, at round $(r-4)$, the node 6 has two branches, either $b_{11,r-5} = 3$ or $b_{11,r-5} = 2$.

- **If $b_{11,r-5} = 3$:** this is a left child implying that we stop the process. We obtain $(b_{11,r-5} \dots b_{11,r}) = (369360)$, that is the third case **(iii)**.

- **If $b_{11,r-5} = 2$:** we have necessarily $(b_{11,r-6} \dots b_{11,r}) = (9269360)$, using Lemma B.7-**(i)**. In Figure B.11, we can see that the node, on the right, at round $(r-5)$ has a unique branching. Then, at round $(r-6)$, the node 9 has two branches, either $b_{11,r-7} = 6$ or $b_{11,r-7} = 5$.

- **If $b_{11,r-7} = 6$:** we have a left node that gives $(b_{11,r-7} \dots b_{11,r}) = (69269360)$, which corresponds to the sequence **(iv)**.

- **If $b_{11,r-7} = 5$:** we have necessarily $(b_{11,r-8} \dots b_{11,r}) = (259269360)$, because of Lemma B.7-**(i)**. Indeed, we can observe in Figure B.11 a unique branching for the node, on the right, at round $(r-7)$. Then, at round $(r-8)$, the node 2 has two branches, either $b_{11,r-9} = 9$ or $b_{11,r-9} = 8$.

- **If $b_{11,r-9} = 9$:** this is a left child, meaning that we have to stop the process. We obtain $(b_{11,r-9} \dots b_{11,r}) = (9259269360)$, so this is the sequence **(v)**.

- **If $b_{11,r-9} = 8$:** we have necessarily $(b_{11,r-10} \dots b_{11,r}) = (58259269360)$, also using Lemma B.7-**(i)**. In Figure B.11, such an observation corresponds to the unique branching for the node, on the right, at round $(r-9)$. Then, at round $(r-10)$, the node 5 has two branches, either $b_{11,r-11} = 2$ or $b_{11,r-11} = 1$.

- **If $\boldsymbol{b_{11,r-11}} = 2$:** we have $(b_{11,r-11} \dots b_{11,r}) = (258259269360)$, so this is the sequence **(vi)**.
- **If $\boldsymbol{b_{11,r-11}} = 1$:** we have $(b_{11,r-11} \dots b_{11,r}) = (158259269360)$, which corresponds to the last sequence **(vii)**.

□

In Figure B.11, representing the possible sequences, it is worth observing that there is only one node with two branches at each round so that this node is either in the middle of the graph, at the far right or at the far left.

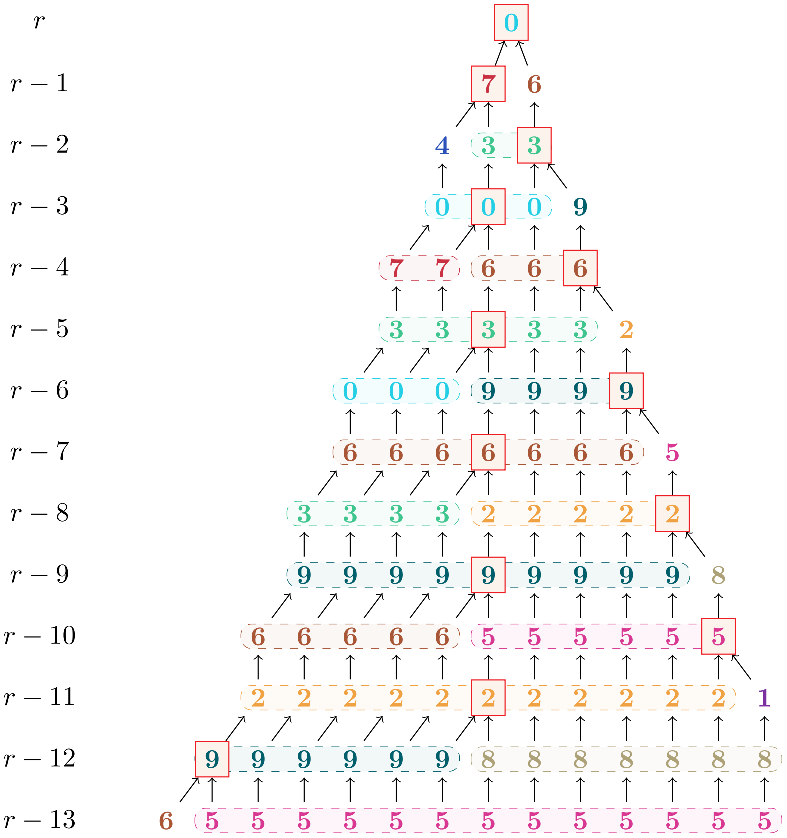

r 0
$r-1$ 7 6
$r-2$ 4 3 3
$r-3$ 0 0 0 9
$r-4$ 7 7 6 6 6
$r-5$ 3 3 3 3 3 2
$r-6$ 0 0 0 9 9 9 9
$r-7$ 6 6 6 6 6 6 6 5
$r-8$ 3 3 3 3 2 2 2 2 2
$r-9$ 9 9 9 9 9 9 9 9 9 8
$r-10$ 6 6 6 6 6 5 5 5 5 5 5
$r-11$ 2 2 2 2 2 2 2 2 2 2 2 1
$r-12$ 9 9 9 9 9 9 8 8 8 8 8 8 8
$r-13$ 6 5 5 5 5 5 5 5 5 5 5 5 5 5

***Figure B.11:** The different subsequences that could occur in the sequence $(b_{11,r})_{r>0}$.*

Let us notice that the denominators of semi-convergents of $\log_2 11$ are

$$\mathfrak{D}_{11} = \{1, 2, 3, 5, 7, 9, 11, 13, 24, 37, 61, 98, 135, 172, 209, 246, 283, 320, 357, 394, 431,\\ 468, 505, 542, 579, 616, 653, 690, 727, 764, 801, 838, 875, 912, 949, 986, \dots\}\,.$$

As for MiMC$_3$, we have that all the integers i, such that $(b_{11,r-i} \dots b_{11,r})$ is an impossible subsequences of Lemma B.7 or a possible sub-sequences of Proposition B.4 are part of $\mathfrak{D}_{11}$.

APPENDIX C

Résumé des travaux

Ce manuscrit est le fruit de trois années de recherche au sein de l'équipe COSMIQ d'Inria Paris. Nous présentons des travaux couvrant les deux sous-domaines de la cryptologie : la cryptographie et la cryptanalyse. Plus précisément, nous nous attachons à la conception et l'analyse de sécurité de nouvelles primitives symétriques définies sur de grands corps et notamment les primitives appelées *orientées arithmétisation*.

Ce manuscrit étant intégralement rédigé en anglais, nous proposons un résumé en français de quelques pages, chapitre par chapitre.

Introduction.

Au cours des dernières années, le nombre de primitives symétriques définies sur de grands corps a augmenté de façon considérable. De telles primitives ont été proposées pour être employées dans de nouveaux contextes tels que les systèmes de preuve à divulgation nulle de connaissance, notamment ceux déployés dans la blockchain Ethereum ou dans la crypto-monnaie Zcash. Les preuves à divulgation nulle de connaissance sont des protocoles impliquant plusieurs parties et permettant à un prouveur de convaincre un vérifieur qu'il connaît un secret *sans le révéler*.

Les performances de ces protocoles dépendent principalement du nombre de multiplications effectuées par la primitive dans des corps finis de grande taille. Les primitives adaptées à ces applications sont donc d'un type complètement nouveau, car pour optimiser leurs performances, elles manipulent des éléments de grands corps finis, à l'opposé de ce qui est habituellement proposé en cryptographie symétrique. En effet, si les primitives symétriques classiques (comme l'AES) utilisent des opérations sur de petits corps $\mathbb{F}_{2^n}$ où n est de l'ordre de 4 ou 8, ces nouvelles primitives utilisent des opérations sur un grand corps fini $\mathbb{F}_q$ où q est soit un grand entier premier soit une puissance de 2, généralement supérieure à 2^{32}.

Au-delà de l'alphabet utilisé, les propriétés recherchées sont également différentes. Si habituellement à partir de la donnée de x nous voulons pouvoir calculer efficacement $f(x)$, dans ce nouveau contexte, c'est la vérification qui doit être efficace : nous voulons pouvoir vérifier que y est bien l'image de x par la fonction f. L'idée la plus naturelle consiste à appliquer la fonction f et vérifier que $y = f(x)$. Mais ce changement de perspective offre aussi de nouvelles possibilités de calcul puisque l'on peut considérer l'inverse de certaines opérations et ainsi vérifier que $x = f^{-1}(y)$.

Alors que le nombre de primitives dites orientées arithmétisation augmente, il est nécessaire de mieux comprendre les propriétés des opérations sous-jacentes. En effet, il est indispensable de vérifier que les contraintes d'implémentation qui ont régi leur conception n'ont pas introduit de failles de sécurité. Bien que de nombreuses primitives orientées arithmétisation aient été mises en avant, très peu d'analyses de sécurité ont déjà été proposées. L'objectif de ce manuscrit est donc en premier lieu de contribuer à combler ce manque pour mieux comprendre les spécificités de ces nouveaux outils. Obtenir une meilleure compréhension des techniques de cryptanalyse qui peuvent menacer de telles primitives nécessite de revisiter les techniques connues mais aussi d'en étudier de nouvelles.

Chapitre 1. Un nouveau type de primitive.

Ce premier chapitre décrit le contexte qui a conduit à l'émergence de ces nouvelles primitives. En particulier, nous essayons de comprendre en quoi ces primitives diffèrent des primitives classiques, ou en d'autres termes, pourquoi ces dernières sont inappropriées dans ces nouveaux contextes. Pour ce faire, nous rappelons dans un premier temps les principes de conception des primitives classiques en cryptographie symétrique. Nous présentons quelques techniques de cryptanalyse couramment utilisées pour les primitives classiques, et ayant également été proposées pour évaluer la sécurité des nouvelles primitives.

Afin de mieux comprendre les principes gouvernant la conception de primitives définies sur de grands corps finis, nous décrivons les nouveaux systèmes de contraintes introduits par les protocoles avancés. Nous présenterons plus particulièrement trois des systèmes de contraintes pour les preuves à divulgation nulle de connaissance : R1CS, $\mathcal{P}\mathfrak{lon}\mathcal{K}$, AIR.

Bien qu'il soit difficile de lister précisément l'ensemble des nouvelles primitives tant elles sont nombreuses, nous proposons un état de l'art exhaustif des primitives orientées arithmétisation afin de mieux observer la diversité des schémas proposés.

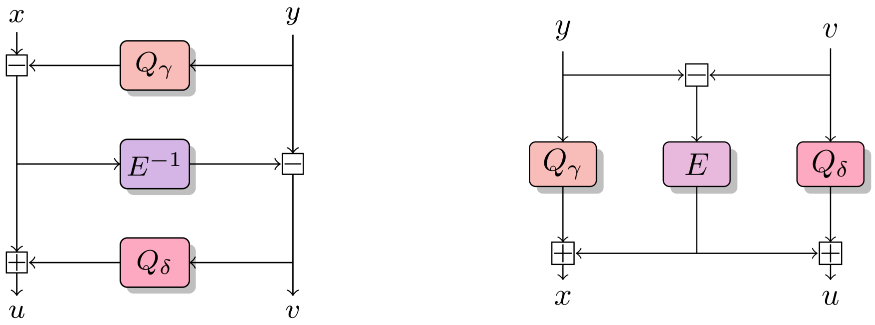
Chapitre 2. Équivalence CCZ et Flystel.

Dans ce deuxième chapitre nous allons plus loin dans la compréhension des primitives orientées arithmétisation. En effet, nous introduisons pour la première fois un lien entre les principes régissant la conception de telles primitives, et l'équivalence CCZ, une forme d'équivalence entre fonctions mathématiques, généralisation de l'inversion.

Partant de cette idée, nous proposons dans un premier temps une étude des "papillons" [PUB16] dans ce nouveau contexte. Les papillons sont une structure bien connue en fonctions booléennes. Etant donné l'équivalence CCZ entre les deux variantes que sont le papillon ouvert et le papillon fermé, leur adaptation en caractéristique impaire était jusqu'alors à découvrir. Nous proposons ainsi divers schémas de papillons, étudiant à la fois leur propriétés cryptographiques et leur efficacité pour ces nouveaux systèmes de preuves.

Cette étude nous amène à proposer un nouveau composant non linéaire : le `Flystel`, inspiré par cette structure bien connue des papillons et un réseau de Feistel à trois branches. L'équivalence CCZ des deux variantes du `Flystel` est à l'origine de son efficacité en offrant un bon niveau de sécurité grâce à l'utilisation du `Flystel` ouvert (figure C.1a) composé de deux fonctions quadratiques Q_γ, Q_δ et d'une fonction de haut degré E^{-1}, tout en ayant un très bon niveau de performance grâce à l'utilisation du `Flystel` fermé (figure C.1b), qui lui est équivalent, composé des deux fonctions quadratiques Q_γ, Q_δ et d'une fonction de faible degré E.

Plus étonnant, le `Flystel` répond à un problème ouvert consistant à trouver des fonctions APN sur $\mathbb{F}_p^2$, c'est-à-dire des fonctions ayant une uniformité différentielle égale à 2. En effet, nous montrons que l'uniformité différentielle du `Flystel` est égale à $d - 1$ lorsque la permutation E correspond à la fonction puissance $x \mapsto x^d$. En choisissant $d = 3$, nous contruisons ainsi une famille de fonctions APN sur $\mathbb{F}_p^2$.



(a) *Flystel ouvert.*

(b) *Flystel fermé.*

Figure C.1: *Les deux variantes équivalentes CCZ du* Flystel.

Chapitre 3. Conception d'Anemoi et Jive.

Dans ce chapitre, nous présentons une nouvelle famille de fonctions de hachage efficaces parmi les divers systèmes de contraintes des preuves à divulgation nulle de connaissance. Cette nouvelle famille porte le nom d'Anemoi et repose sur deux nouveaux composants : le Flystel, introduit au chapitre précédent et Jive, un nouveau mode opératoire, inspiré des algorithmes symétriques de "danse latine" comme Salsa ou ChaCha. Jive est un mode de compression de fonction particulièrement efficace pour les arbres de Merkle. Sur la figure C.2 nous décrivons une compression 2-vers-1.

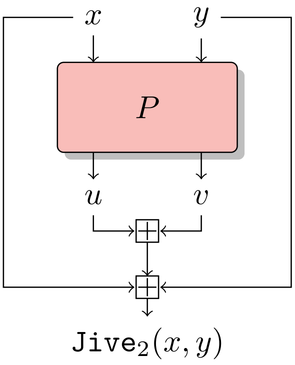


Figure C.2: *Mode* $\texttt{Jive}_2$ *(compression 2-vers-1).*

L'état interne d'Anemoi peut être représenté par une matrice de deux lignes et ℓ colonnes. Notre conception est classique : elle utilise une structure de réseau de substitution et de permutation comme illustré sur la figure C.3, avec pour composant non linéaire, le Flystel, $\mathcal{H}$, appliqué sur les colonnes de l'état interne, et pour composants linéaires, une matrice MDS appliquée sur les lignes et $\mathcal{P}$, la pseudo-transformation de Hadamard appliquée sur les colonnes.

Anemoi se révèle être une primitive particulièrement compétitive en offrant, par exemple, une amélioration d'un facteur 2 par rapport à Poseidon et *Rescue–Prime* en termes de nombre de contraintes R1CS, une réduction de $21\% - 35\%$ en termes de contraintes $\mathcal{P}$lon$\mathcal{K}$ par rapport à

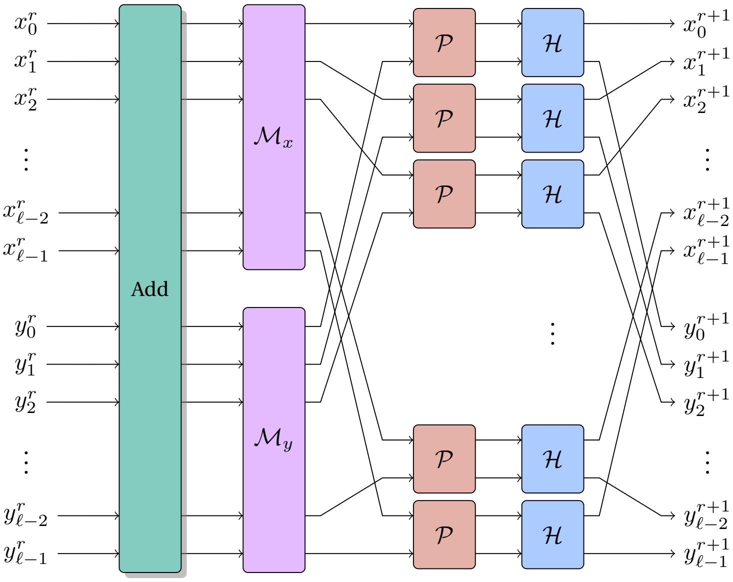


Figure C.3: *Un tour de la permutation* `Anemoi`*.*

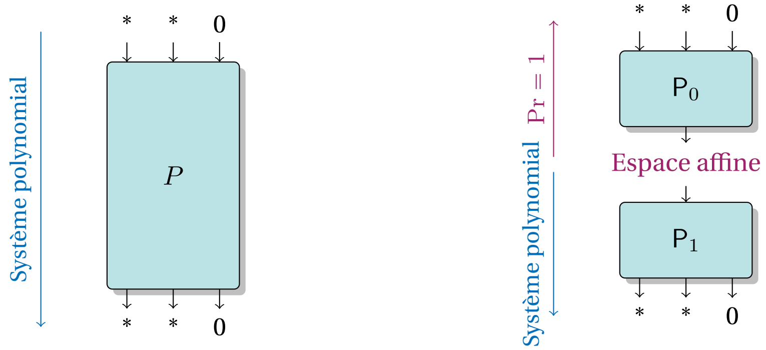
une implémentation hautement optimisée de POSEIDON, ainsi que des performances natives compétitives, s'exécutant entre deux et trois fois plus vite qu'une implémentation de *Rescue–Prime*, en fonction de la taille du corps.

Les travaux présentés dans les chapitres 2 et 3, ainsi que la cryptanalyse algébrique d'`Anemoi`, brièvement introduite dans le chapitre 4, ont été obtenus avec Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov et Danny Willems, ont fait l'objet d'une publication dans les proceedings de la conférence *CRYPTO* en 2023 [Bou+23].

Chapitre 4. Attaques algébriques contre certaines primitives orientées arithmétisation.

Les attaques algébriques sont généralement les plus efficaces pour attaquer ces nouvelles primitives. Ce type d'attaque exploite des relations algébriques entre le texte en clair, le texte chiffré et la clé. Plus le système d'équations modélisant la primitive est simple à résoudre, de part sa structure particulière ou son faible degré, plus elle est vulnérable à ce type d'attaque. Dans ce chapitre, nous évaluons la sécurité de certaines primitives telles que Feistel–MiMC, POSEIDON, *Rescue–Prime*, Ciminion, ou encore encore `Anemoi`. Nous étudions en particulier la difficulté pour ces primitives du problème CICO (Constrained Input Constrained Output). L'idée est de trouver un couple d'entrée et de sortie d'une permutation dont les derniers éléments valent 0.

Nous montrons que pour les réseaux de substitution-permutation, il est possible de gagner deux tours dans la construction du système polynomial décrivant le problème CICO, comme le montre la figure C.4. L'idée est de décomposer une permutation P en deux permutations P_0 et P_1 de façon à ne construire le système polynomial que pour l'une d'elle, l'espace affine intermédiaire assurant ainsi un 0 sur la troisième branche en entrée de la permutation.



***(a)** R tours.*

***(b)** $R-2$ tours.*

***Figure C.4:** Contournement de deux tours.*

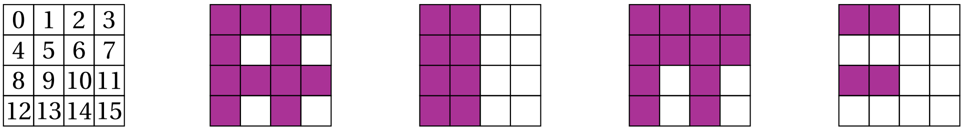
Nous mettons également en évidence l'importance du choix de la modélisation à travers les exemples de Ciminion et `Anemoi`. En effet, nous montrons que certaines modélisations permettent de simplifier la représentation du système polynomial, rendant la résolution du problème CICO plus facile.

Les travaux présentés dans ce chapitre ont été initiés suite à des challenges de cryptanalyse proposés par la fondation Ethereum. Les résultats obtenus avec Augustin Bariant, Gaëtan Leurent et Léo Perrin, sur Feistel–MiMC, Poseidon, *Rescue–Prime* et Ciminion, ont ensuite fait l'objet d'une publication dans le journal *IACR Transactions on Symmetric Cryptology* en 2022 [Bar+22].

Chapitre 5. Représentation polynomiale univariée et degré algébrique.

Dans ce chapitre nous étudions la forme univariée des polynômes représentant des fonctions puissances itérées. Nous nous intéressons plus particulièrement au chiffrement par bloc MiMC qui consiste à itérer un très grand nombre de fois une fonction de tour simple, composée de l'addition d'une clé et de constantes de tours, et d'une fonction puissance $x \mapsto x^d$ de faible degré sur $\mathbb{F}_{2^n}$, où n est de l'ordre de 129. Chaque tour du chiffrement MiMC peut ainsi être représenté par un polynôme univarié, et la fonction de tour est répétée suffisamment de fois pour que le degré univarié de la transformation après r itérations atteigne le degré attendu pour une permutation aléatoire.

En nous intéressant plus précisément à cette représentation univariée, nous montrons que pour certains choix de permutation itérée, des familles d'exposants n'apparaissent jamais dans le polynôme univarié représentant MiMC après chaque tour. Nous montrons notamment que dans le cas des fonctions Gold $x \mapsto x^d$ où d est de la forme 2^j+1, les polynômes sont très creux, et le sont encore davantage sur les premiers tours. Plus généralement, nous montrons que quel que soit le choix de l'exposant d pour la fonction puissance itérée dans MiMC_d, au moins un quart des exposants n'apparaît jamais. Une représentation des exposants modulo 16 est donnée dans la figure C.5 pour quelques instances de MiMC_d, de sorte que les exposants absents sont représentés par un carré non coloré.



0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

(a) *Représentation.* **(b)** *Pour* MiMC_3. **(c)** *Pour* MiMC_5. **(d)** *Pour* MiMC_7. **(e)** *Pour* MiMC_9.

Figure C.5: *Représentation des exposants modulo* 16 *pour diverses instances de* MiMC_d.

Bien qu'il n'ait pas encore été identifié de façon d'exploiter de tels polynômes univariés creux pour construire un distingueur efficace, nous pouvons utiliser cette observation pour déduire une borne sur le degré algébrique. Le degré algébrique est aussi connu sous le nom de degré multivarié, et correspond au degré de la fonction lorsqu'elle est écrite comme n coordonnées booléennes à n variables. Le degré multivarié correspond également au maximum des poids de Hamming des exposants (nombre de 1 dans la représentation binaire des exposants) apparaissant dans la forme développée du polynôme décrivant la transformation. Dans des attaques dites différentielles d'ordre supérieur, il est possible d'exploiter le fait que le degré algébrique du chiffrement reste inférieur à sa valeur maximale, c'est pourquoi il est essentiel d'étudier son évolution au fil des itérations. Ainsi, nous montrons que si le degré univarié de MiMC augmente de façon prévisible avec le nombre de tours, le degré algébrique a un comportement bien plus complexe, et reste constant pendant certains tours. De tels plateaux ralentissent légèrement la croissance du degré algébrique.

La borne que nous obtenons sur le degré algébrique de MiMC_3 améliore légèrement la borne donnée par [Eic+20] (voir figure C.6), de sorte que nous pouvons économiser un ou deux tours pour les attaques différentielles d'ordre supérieur proposées dans cet article. Dans le chapitre suivant nous montrons que cette borne correspond au degré algébrique exact.

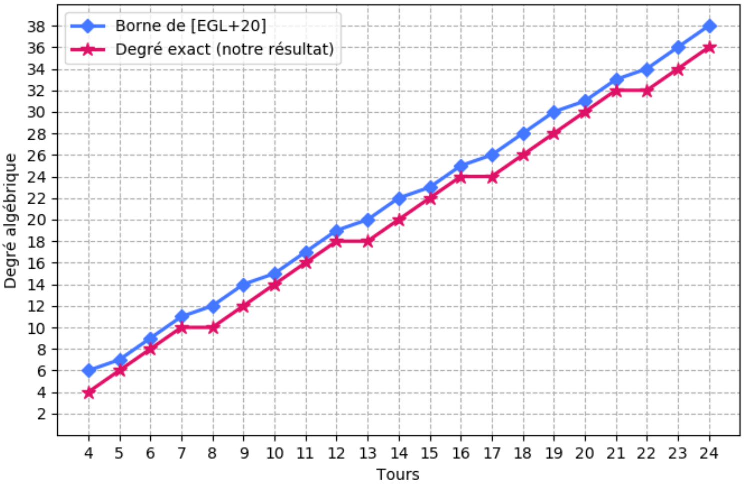


Figure C.6: *Comparaison de notre borne sur le degré algébrique de* MiMC_3 *avec la borne de [Eic+20]*

Par ailleurs, nous montrons qu'il existe un plateau entre les deux premiers tours de la transformation inverse MiMC_3^{-1}. Nous donnons également des indications pour mieux comprendre le comportement du degré algébrique de la transformation inverse.

Les résultats présentés dans ce chapitre contribuent à une meilleure compréhension de la représentation univariée et du degré algébrique des algorithmes de chiffrement par blocs reposant sur une fonction puissance définie sur un grand corps.

Chapitre 6. Traçage des exposants lors de l'itération de fonctions puissance.

Tandis qu'une borne sur le degré algébrique permet à un attaquant de monter des attaques différentielles d'ordre supérieur, elle ne donne en aucun cas de garantie aux concepteurs d'une primitive que de telles attaques ne peuvent pas être améliorées de façon significative. De nombreuses méthodes reposant sur des solveurs ont été proposées pour déterminer des bornes très précises sur le degré algébrique de primitives définies sur de grands corps. Dans ce chapitre nous proposons une vision différente limitant le recours aux solveurs et visant à mieux comprendre les propriétés mathématiques du chiffrement par bloc MiMC. Notre objectif est plus particulièrement de donner une méthodologie précise permettant de construire les exposants apparaissant dans le polynome univarié après chaque tour. Notre procédure repose sur une preuve par récurrence pour la majorité des tours, et un algorithme MILP pour certains cas particuliers non couverts par la récurrence. Nous montrons ainsi que la borne donnée dans le chapitre précédent pour MiMC_3 est atteinte. En effet, nous parvenons à évaluer le degré algébrique exact jusqu'à plus de 16000 tours en construisant certaines familles d'exposants pour lesquels le poids de Hamming atteint la borne.

Bien qu'il suffise de trouver un seul exposant de poids maximal pour prouver que la borne sur le degré algébrique est atteinte à chaque tour, nous allons plus loin dans cette réflexion en tentant d'identifier tous les exposants de poids maximal pour chaque tour de MiMC_3. Si nous ne pouvons garantir de ne pas manquer certains exposants, nous réussissons cependant à construire de grandes familles d'exposants de poids maximal pour plus de 400 tours. Une comparaison proposée sur la figure C.7 semble indiquer une grande proximité entre nos résultats et le nombre d'exposants observés.

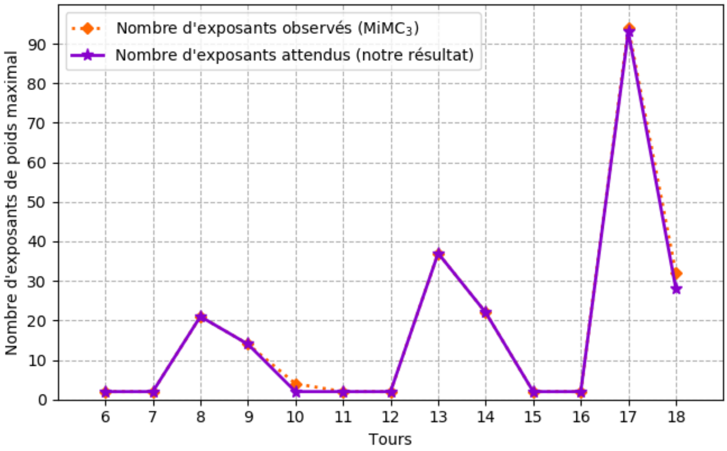


Figure C.7: Exposants dont le poids de Hamming atteint la borne sur le degré algébrique.

Tentant de généraliser la procédure de traçage des exposants, nous étudions également d'autres instances de MiMC et donnons des pistes de recherche pour construire des exposants de poids maximal atteignant les bornes pour les différentes instances de MiMC_d étudiées au chapitre 5. Enfin, nous dérivons des bornes inférieures pour le degré algébrique aux troisième et quatrième tours de la transformation inverse MiMC_3^{-1}.

Dans ce chapitre, nous offrons ainsi des garanties précises sur le degré algébrique de MiMC et donc sur la complexité minimale d'une attaque différentielle d'ordre supérieur.

Les résultats présentés dans les chapitres 5 et 6 sur le degré algébrique de MiMC_3 et sa transformation inverse, ont été obtenus avec Anne Canteaut et Léo Perrin, et ont fait l'objet d'une publication dans le journal *Designs, Codes and Cryptography* en 2023 [BCP23]. La généralisation des résultats aux autres instances de MiMC_d a été présentée à la conférence *Finite Fields and their Applications* à Paris en juin 2023, et fait l'objet d'un article en cours de rédaction.

Chapitre 7. Autres perspectives pour le degré algébrique.

Dans ce chapitre, nous poussons plus loin l'analyse du degré algébrique du chiffrement par bloc MiMC et nous étudions différentes directions. Plus précisément, notre but est de répondre à divers problèmes ouverts qui pourraient être soulevés par l'étude précédente du degré algébrique dans les chapitres 5 et 6. Bien que nous ne soyons pas en mesure de répondre précisément à toutes les questions, nous pensons qu'il est intéressant de les proposer comme une invitation à des travaux futurs dans ces différentes directions.

Nous étudions, dans un premier temps, l'évolution du degré algébrique des constructions en réseau de substitution et de permutation avec une transformation affine. En particulier, nous utilisons la stratégie dite de "regroupement des coefficients" pour étudier le degré algébrique de schémas comme Chaghri ou MiMC. Nous donnons notamment des conditions nécessaires sur la densité de la couche affine pour assurer une croissance exponentielle du degré algébrique pour un certain nombre de tours.

Nous proposons également un autre point de vue sur la suite des logarithmes en base 2 des puissances d'un entier rencontrée dans le chapitre 6. En particulier, nous essayons de mieux comprendre le lien entre le degré algébrique de MiMC étudié dans les chapitres précédents, et les dénominateurs des semi-convergents de $\log_2 d$. Cette séquence possède également des applications en musique dans le cas des puissances de 3.

Enfin, nous considérons la transformation représentant MiMC comme un polynôme bivarié en le texte en clair et la clé, suggérant alors quelques directions pour étudier l'influence des coefficients des polynômes lorsque le texte en clair ou la clé est fixé.

Les résultats présentés dans ce chapitre, sur le degré algébrique des constructions de type SPN avec une transformation affine, ont été obtenus avec Fukang Liu, Lorenzo Grassi, Willi Meier et Takanori Isobe, et ont également fait l'objet d'une publication dans les proceedings de la conférence *CRYPTO* en 2023 [Liu+23b].

Conclusion et perspectives.

Les travaux présentés dans ce manuscrit contribuent à mieux comprendre les outils de conception et d'analyse pour ces nouvelles primitives symétriques définies sur de grands corps. En particulier, nous proposons une nouvelle famille de fonctions de hachage, `Anemoi`, offrant de très bonnes performances pour une utilisation dans des preuves à divulgation nulle de connaissance. `Anemoi` suscite d'ailleurs un vif intérêt de la part d'industriels à l'image des auteurs de [Liu+22] ayant démontré le potentiel d'Anemoi avec des optimisations supplémentaires. D'un point de vue théorique, Anemoi améliore significativement la compréhension des principes de conception de ces nouvelles primitives. En effet, pour la première fois un lien est identifié entre l'équivalence CCZ et les performances des primitives orientées arithmétisation. La découverte de ce lien a aussi influencé la conception d'une autre primitive : Arion [RST23]. Les principaux composants de la nouvelle famille Anemoi, que sont le Flystel, composant non-linéaire, et Jive, mode de compression, sont également d'un intérêt plus général puisqu'ils peuvent aussi être utilisés pour d'autres schémas.

Par ailleurs, l'analyse de sécurité réalisée dans le cadre des challenges proposés par la fondation Ethereum a permis de mettre en lumière certaines faiblesses de primitives actuellement déployées dans l'industrie. Outre notre analyse des attaques algébriques, nous proposons également des recommandations pour de futurs primitives. Il est notamment important de porter une attention particulière au choix de la modélisation, aux simplifications possibles pour les réseaux de substitution-permutation, ou encore de privilégier un modèle univarié plutôt que multivarié lorsque cela est possible.

Enfin, l'analyse approfondie du chiffrement par bloc MiMC représente l'une des premières études apportant une compréhension aussi fine de l'évolution du degré algébrique de ces primitives. Notre meilleure compréhension de la représentation univariée des polynômes représentant MiMC après chaque tour nous permet de déduire des bornes précises sur le degré algébrique de la transformation, permettant de mieux évaluer la complexité des attaques différentielles d'ordre supérieur. En conséquence, cette analyse a déjà eu une influence significative en inspirant plusieurs travaux dans ce domaine [Liu+23a; Cui+22]. Bien qu'au moment d'écrire ce manuscrit nous ne sachions pas encore comment exploiter efficacement la représentation polynomiale univariée creuse pour construire des distingueurs, nous pouvons néanmoins souligner que certaines constructions semblent apporter de faibles garanties de sécurité. En effet, si les fonctions Gold sont particulièrement intéressantes et efficaces en raison de leur faible degré, le niveau de sécurité qu'elles apportent reste incertain étant donné leur représentation univariée très creuse. Plus généralement, si nous n'apportons pas nécessairement de réponses précises à toutes les questions relatives à l'étude du degré algébrique de ces nouvelles primitives, nous pensons néanmoins que ces résultats peuvent encourager la poursuite des travaux dans ce domaine.

Dans ce manuscrit nous apportons ainsi quelques réponses aux questions de cryptanalyse soulevées par l'émergence des nouvelles primitives. Cependant, il est essentiel de noter que certains aspects restent encore obscurs et nécessitent de poursuivre les efforts d'analyse de sécurité afin de mieux appréhender ces primitives et d'identifier d'éventuelles vulnérabilités.