DE CIFRIS KOINE
Book Series
Volume V

CIFRIS24 ACTA
PREPROCEEDINGS DRAFT

DE CIFRIS KOINE
Series Editorial Board

DE CIFRIS KOINE
Book Series

De Cifris Koine è una collana editoriale curata da De Cifris Press, marchio dell'associazione nazionale De Componendis Cifris dedicata allo studio e alla divulgazione della crittografia e delle discipline correlate.

Questa collana rappresenta un punto di riferimento per la comunità crittografica italiana, offrendo una panoramica delle ricerche e delle innovazioni nel campo. Attraverso la pubblicazione degli atti di conferenze e workshop, De Cifris Koine fornisce non solo approfondimenti scientifici, ma anche contributi divulgativi, mettendo in luce i progressi e le attività dei principali esponenti in questo ambito.

La serie abbraccia un ampio spettro di argomenti, estendendosi oltre la crittografia stessa per includere le sue molteplici applicazioni e intersezioni con altre discipline. Tra queste, si annoverano la teoria dei codici, vari rami della matematica come l'algebra, la teoria dei numeri e la geometria, l'informatica con un focus particolare sulla cybersecurity e sull'informatica teorica, nonché l'ingegneria elettrica, le telecomunicazioni, la storia e gli aspetti legali legati alla crittografia.

Gli articoli pubblicati in questa collana sono accettati in tre lingue: italiano, inglese e francese.

La periodicità della pubblicazione è trimestrale.

De Cifris Koine is a book series published by De Cifris Press, publishing house of the national association De Componendis Cifris, whose activities focus on cryptography and related topics. De Cifris Koine volumes form the voice of the Italian cryptographic community, as they collect communications from both scientific and educational events and summaries of papers of its members and of their activities. In particular, De Cifris Koine hosts conference and workshop proceedings, including short abstracts.

Topics covered in De Cifris Koine volumes relate to cryptography and its applications to and connections with other disciplines, as for example coding theory, maths (mainly algebra, number theory and geometry), computer science (mainly cyber security and theoretical computer science), electronic engineering, telecommunication engineering, history of cryptography and law.
Accepted articles are either in Italian, English or French.
Volumes are published quarterly.

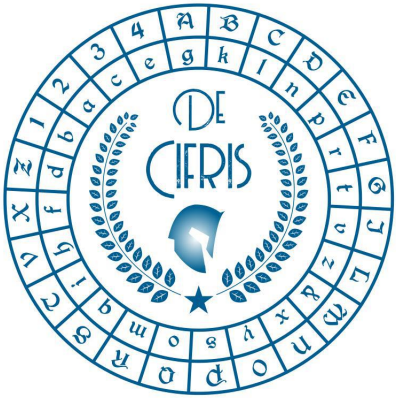
La De Cifris Koine est une collection publiée par la De Cifris Press de l'association nationale italienne De Componendis Cifris. Elle est consacrée à l'étude et à la diffusion de la cryptographie et des disciplines connexes.

Cette collection est une référence importante pour la communauté cryptographique italienne, offrant une vue d'ensemble de la recherche et des innovations dans ce domaine. Grâce à la publication d'actes de conférences et de groupes de travail (workshops), la De Cifris Koine fournit non seulement des contributions scientifiques académiques, mais aussi des contributions à destination du grand publique, mettant en lumière les progrès et les activités des principaux acteurs et des principales actrices du domaine.

Les articles de cette collection couvrent un large éventail de sujets allant de la cryptographie à ses nombreuses applications et intersections avec d'autres disciplines. Par exemple, la théorie des codes, diverses branches des mathématiques telles que l'algèbre, la théorie des nombres et la géométrie, l'informatique, avec un accent sur la sécurité informatique et l'informatique théorique, ainsi que le génie électrique, les télécommunications et les aspects juridiques de la cryptographie. Les articles soumis à la De Cifris Koine sont acceptés en italien, anglais et français. La fréquence de publication est trimestrielle.

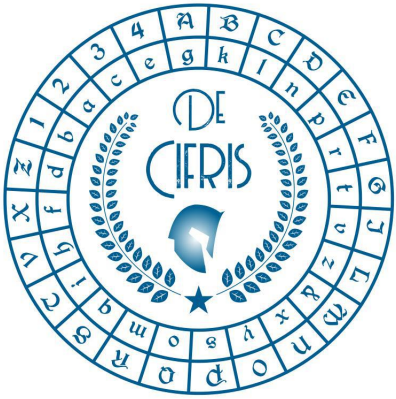
CIFRIS23 ACTA

Draft PreProceedings of the 2024 Congress of *De Componendis Cifris*



Edited by:

- *Giulia Cavicchioni*,
  Università di Trento, Italy
- *Luca De Feo*,
  IBM Zurich, Italy
- *Barbara Masucci*,
  Università di Salerno, Italy
- *Marco Pedicini*,
  Università RomaTre, Italy
- *Massimiliano Sala*,
  Università di Trento, Italy.



Pubblicazione trimestrale di proprietà dell'associazione nazionale di crittografia
De Componendis Cifris

Autorizzazione del Tribunale di Milano in data 23 - 02 - 2024
Num. R.G. 1315/2024 Num. Reg. Stampa 22
ISSN 3034-9796 - ISBN xxxxxxxxx

Editore: De Componendis Cifris APS.
Marchio Editoriale: De Cifris Press.
Direttore responsabile: Massimiliano Sala
Redazione: Antonino Alì, Nadir Murru
Luogo di pubblicazione: Via Gianfranco Zuretti 34 - 20125 Milano
e-mail: editorial@decifris.it
Stampa in proprio
Numero 5 - Pubblicato il xxxxxxxx

PREFACE

Table of Contents

Protocols and Zero-Knowledge

Post-Quantum Cryptography

Public-Key Cryptography

Theoretical Cryptography

Applied Cryptography

Part IV
Workshops

FCiR - Financial Cryptography in Rome 2024

Organizers: Michela Iezzi and Massimiliano Sala

ReAdPQC - Recent Advances in Post-Quantum Cryptography 2024

Organizers: Giulio Codogni, Roberto La Scala, Edoardo Persichetti, and Federico Pintore

TAC - Topics in Applied Cryptography 2024

Organizers: Riccardo Longo, Alessandro Tomasi, Chiara Spadafora, Silvio Ranise, and Stefano Berlato

NTC - Number Theory for Cryptography 2024

Organizers: Federico Accossato, Gessica Alecci, Danilo Bazzanella, Laura Capuano, Giuseppe D'Alconzo, Simone Dutto, Nadir Murru, and Giordano Santilli

CPSID - Cryptography, Protocols and Security in Digital Identity 2024

Organizers: Andrea D'Intino and Denis "Jaromil" Roio

SymCrypt - Symmetric Cryptography and Boolean Functions 2024

Organizers: Marco Calderini, George Petrides, and Irene Villa

CodeMath - Coding Theory and Discrete Mathematics 2024

Organizers: Massimo Giulietti, Giuseppe Marino, Olga Polverino, and Ferdinando Zullo

QCifris - Quantum Cifris 2024

Organizers: Paolo Villoresi, Marco Genovese, Fabio Sciarrino, Cristian Antonelli, Giuseppe Vallone

CifrisCloud - Cryptography for the Cloud 2024

Organizers: Michela Iezzi, Matteo Nardelli, and Marco Pedicini.

Part I

Introduction to CIFRIS24 ACTA

[.....]

Program Committee Chairs

Luca De Feo	IBM Research Zurich, Switzerland
Barbara Masucci	University of Salerno, Italy

Program Committee

Christian Badertscher	Input Output, Switzerland
Charles Bouillaguet	Sorbonne University LIP6 Paris, France
Marco Calderini	University of Trento, Italy
Matteo Campanelli	Protocol Labs, Denmark
Claude Carlet	Univ. of Paris 8 and Univ. of Bergen, France and Norway
Michele Ciampi	University of Edinburgh, Scotland
Roberto Civino	University of L'Aquila, Italy
Miranda Chris	Columbia University, USA
Anna Lisa Ferrara	University of Molise, Italy
Tako Boris Fouotsa	EPFL, Switzerland
Danilo Francati	Aarhus University, Denmark
Daniele Friolo	Sapienza University of Rome, Italy
Philippe Gaborit	University of Limoges, France
Annamaria Iezzi	Université Grenoble Alpes, France
Delaram Kahrobaei	New York University, USA
Elena Kirshanova	Baltic Federal University, Russia
Gregor Leander	University Bochum, Germany
Nian Li	Hubei University, China
Atul Mantri	Virginia Tech, USA
Sihem Mesnager	University of Paris VIII, France
Giacomo Micheli	University of South Florida - USA
Marine Minier	Université de Lorraine - France
Alice Pellet-Mary	IMB, France
Svetla Petkova-Nikova	KU Leuven, Belgium
Alberto Ravagnani	The Eindhoven University, The Netherlands
Divya Ravi	University of Amsterdam, Netherlands
Simona Samardjiska	Radboud University, The Netherlands
Santanu Sarkar	Indian Institute of Technology Madras, India
Luisa Siniscalchi	Danmarks Tekniske Universitet (DTU), Denmark
Claudio Soriente	NEC Laboratories Europe Madrid, Spain
Pantelimon Stanica	Naval Postgraduate School, USA
Serge Vaudenay	EPFL, Switzerland

Polina Vinogradova IOHK, Canada
Hendrik Waldner Max Planck Institute, Germany

Part II
Institutional Session

Round Table with representatives of government's Departments and other Italian public-law institutions

Moderator: TBA

Speakers:

- *Paolo Aceto*,
  Generale, Arma dei Carabinieri,

- *TBA*,
  Rappresentante della Guardia di Finanza,

- *Andrea Billet*,
  Direttore Servizio Agenzia per la Cybersicurezza Nazionale,

- *Ivano Gabrielli*,
  Direttore Polizia Postale, Ministero degli Interni.

Intervento di Paolo Aceto
Generale dell'Arma dei Carabinieri

Intervento di TBA
Rappresentante della Guardia di Finanza

Intervento di Andrea Billet
Dirigente presso l'Agenzia per la Cybersicurezza Nazionale

Intervento di Ivano Gabrielli
Direttore del Servizio Polizia Postale e delle Comunicazioni

KEYNOTE:
La De Cifris e la crittografia italiana

Barbara Masucci

University of Salerno, Italy

De Cifris Partners: Athilab

Chiara Ballari

Athilab

De Cifris Partners: Radom Power

Massimo Caccia

Random Power

De Cifris Koine – CIFRIS24 ACTA –

De Cifris Partners: ThinkQuantum

Simone Capeleto

ThinkQuantum

De Cifris Partners: FORKBOMB BV

Adrea D'Intino

De Cifris Partners: QTI SRL

Alessandra Matteis

QTI SRL

Part III
Scientific Session

Introduction to the Scientific Session

[.....]

De Cifris Koine – CIFRIS23 ACTA – https://doi.org/10.69091/koine/vol-1-M01

Boolean Functions

KEYNOTE:
Quadratic-like balanced functions and permutations

Claude Carlet
Joint work with Irene Villa

University of Paris VIII and LAGA, France
University of Bergen, Norway

Abstract. The so-called (n, m)-functions have very nice properties when quadratic, which for instance ease the study of their almost perfect nonlinearity. But quadratic functions are weak against some other attacks. It is then important to study strict superclasses sharing some of these properties. In particular, when the block ciphers have a structure of substitution-permutation network (SPN), the substitution boxes must be permutations ($m = n$). It is then essential to study superclasses of quadratic functions within the class of balanced functions. We shall introduce and study such a superclass, that of "quadratic-like balanced functions" ("permutations" when $m = n$).

The so-called (n, m)-functions (or vectorial functions) $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, when they are quadratic, that is, when all their derivatives $F(x) + F(x + a)$ are affine functions over the $\mathbb{F}_2$-vector space $\mathbb{F}_2^n$, have very nice properties, which for instance ease the study of their almost perfect nonlinearity (an important cryptographic property introduced by K. Nyberg in the framework of the resistance against differential attacks of the block ciphers using such F as a substitution box). But quadratic functions are weak against some other attacks such as higher order differential attacks and integral attacks. It is then important to study strict superclasses (of the class of quadratic functions) sharing some of the nice properties of quadratic functions.
An important feature of vectorial functions, which is required in many applications, is their balance: the preimages $F^{-1}(b)$ of all the elements of the codomain $\mathbb{F}_2^m$ must have the same size 2^{n-m} (which needs that $m \leqslant n$). In particular, when the block ciphers have a structure of substitution-permutation network (SPN), the substitution boxes must be permutations ($m = n$).
It is then essential to study superclasses of quadratic functions within the class of balanced functions. Such a superclass exists - that of balanced plateaued functions - but there is no specific relation between plateauedness and balance, and this makes this superclass moderately interesting. We need then to find other superclasses, in

which balance would play a central role. We shall introduce and study such a superclass, whose elements share with quadratic balanced functions a nice property that we shall recall. We shall call these functions quadratic-like balanced functions (and quadratic-like permutations when $m = n$). We will show that some important classes of functions have such a property:
- Feistel permutations (i.e. permutations which have the structure of a round in a block cipher having a Feistel structure),
- crooked permutations (that is, (n, n)-permutations whose derivatives have for image sets the complements of linear hyperplanes),
- more generally, balanced strongly plateaued functions (whose component functions all are partially-bent, i.e. are affine extensions of bent functions).
We will also show that all the power permutations $F(x) = x^d$, $x \in \mathbb{F}_{2^n}$, having this property must be quadratic, which will generalize a well-known similar result on power crooked functions.
The notion of quadratic-like balance is affine invariant and we shall give several constructions of quadratic-like permutations and balanced functions which lie outside the classes above, up to affine equivalence.
We shall characterize the property by the Walsh transform and study the consequences of this characterization, showing for instance that quadratic-like almost bent functions (whose nonlinearity achieves the optimum $2^{n-1} - 2^{\frac{n-1}{2}}$) are crooked.

References

1. T. Bending, and D. Fon-Der-Flaass. Crooked functions, bent functions and distance regular graphs. *Electron. J. Comb.* 5, Research paper 34 (electronic), 14 pages, 1998.
2. M. Calderini, M. Sala, and I. Villa. A note on APN permutations in even dimension. Finite Field and their Applications, 2017.
3. C. Carlet. Boolean and vectorial plateaued functions, and APN functions. *IEEE Transactions on Information Theory* 61 (11), pp. 6272-6289, 2015
4. C. Carlet. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, 2021.
5. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography, 15 (2), pp. 125-156, 1998.
6. J. F. Dillon, and H. Dobbertin. New cyclic difference sets with Singer parameters. Finite Fields and Their Applications 10, pp. 342-389, 2004.
7. G. M. Kyureghyan, The only crooked power functions are $x^{2^k+2^l}$. European Journal of Combinatorics 28 (4), pp. 1345-1350, 2007.
8. P. Langevin, and P. Véron. On the Non-linearity of Power Functions. Designs, Codes and Cryptography, 2005, 37, pp.31-43.

On second-order derivatives of Boolean functions and cubic APN permutations in even dimension

Augustine Musukwa

University of Trento, Italy

1 Introduction

We denote the finite field with two elements (0 and 1) by $\mathbb{F}$, and $\mathbb{F}^n$ is vector space of dimension n over $\mathbb{F}$. We study the functions from $\mathbb{F}^n$ to $\mathbb{F}$ which are called Boolean functions (we denote the set of these functions by B_n) and the functions from $\mathbb{F}^n$ to $\mathbb{F}^n$ which are called vectorial Boolean functions. Among other cryptographically significant vectorial Boolean functions, we study APN functions which are known to provide optimal resistance to the differential and linear attacks [23].

In this work, for a Boolean function f, we introduce a few parameters, particularly a quantity $\mathcal{M}(f)$ which is related to the behaviour of its second-order derivatives (the first-order derivative with respect to $a \in \mathbb{F}^n$ is defined as $D_a f = f(x) + f(x+a)$, and the second-order derivative with respect to $a, b \in \mathbb{F}^n$ is defined as $D_b D_a f = f(x) + f(x+a) + f(x+b) + f(x+a+b)$). The quantity $\mathcal{M}(f)$ is used to characterize partially-bent and bent functions of degrees 2 and 3. The parameter is extended to vectorial Boolean functions and it is used to characterize quadratic and cubic APN functions of degree 2 and 3. It can also be a powerful tool in studying APN permutations in even dimension.

Since we are restricted to only two pages, in this summary we do not provide the preliminaries and the results are presented without proofs.

2 Parameters for Boolean functions

First we introduce the following notation: $Z(f) = \{a \in \mathbb{F}^n \mid D_a f = 0\}$ and $U(f) = \{a \in \mathbb{F}^n \mid D_a f = 1\}$. From the two sets we define the parameter $\mathfrak{m}(f) = |Z(f)| - |U(f)|$. Furthermore, we denote $Z_a(f) = Z(D_a f)$ and $U_a(f) = U(D_a f)$ so that $\mathfrak{m}(D_a f) = |Z_a(f)| - |U_a(f)|$. We define another parameter as follows: $\mathcal{M}(f) = \sum_{a \in \mathbb{F}^n \setminus \{0_n\}} \mathfrak{m}(D_a f)$. This parameter has been used in most results.

Definition 1. *Given $f \in B_n$, we define* $\mathrm{var}(f)$ *as the smallest integer k in $\{0, \ldots, n\}$ such that there exists $g \in B_k$ with f being affine equivalent to g. We write $k = \mathrm{var}(f)$. If $\mathrm{var}(f) = n$ we say that f is* variable maximal.

We next use the defined parameters to study Boolean functions.

Theorem 1. *$|Z(\cdot)|$, $|U(\cdot)|$ and $\mathfrak{m}(\cdot)$ are invariant under affine equivalence.*

Corollary 1. *A bent Boolean function f is variable maximal.*

Proposition 1. *For any partially-bent function $f \in B_n$ with $\deg(f) = 2, 3$, we have $\mathcal{M}(f) = 2^n(2^k - 1)$, where $k = \dim V(f)$. (Note that $V(f) = \{a \in \mathbb{F} \mid D_a f$ is constant$\}$)*

Corollary 2. *Let $f \in B_n$ be a quadratic or cubic function. Then f is bent if and only if $\mathcal{M}(f) = 0$.*

Corollary 3. *For n odd, a quadratic Boolean function $f \in B_n$ is semi-bent if and only if $\mathcal{M}(f) = 2^n$.*

3 APN functions and their second-order derivatives

We extend the parameters introduced for Boolean functions to vectorial Boolean functions and we use them to characterise APN maps of low degree.

Definition 2. *For a function $F : \mathbb{F}^n \to \mathbb{F}^n$ with $n \in \mathbb{N}$, define $\mathcal{M}(F) = \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} \mathcal{M}(F_\lambda)$.*

Theorem 2. *The value $\mathcal{M}(\cdot)$ is invariant under EA-transformation.*

Theorem 3. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a function with $\deg(F) \in \{2, 3\}$. Then $\mathcal{M}(F) \geqslant 2^n(2^n - 1)$. Moreover, F is APN if and only if the equality holds.*

Corollary 4. *An APN function $F : \mathbb{F}^n \to \mathbb{F}^n$ with $\deg(F) \in \{2, 3\}$ has at most $2^n - 1$ pairs (a, λ) $(a, \lambda \neq 0_n)$ such that $D_a F_\lambda$ is constant.*

Theorem 4. *For an APN permutation $F : \mathbb{F}^n \to \mathbb{F}^n$ every nonzero component F_λ is such that $m(F_\lambda) = 0, 1$ and $Z(F_\lambda) = \{0_n\}$.*

Corollary 5. *Every nonzero component of an APN permutation is variable maximal.*

Proposition 2. *For n a positive even integer, consider $F : \mathbb{F}^n \to \mathbb{F}^n$ an APN permutation of degree 3. Then either one of the following two conditions is satisfied.*

1. *Every nonzero component F_λ is such that $\mathcal{M}(F_\lambda) = 2^n$.*
2. *There are two distinct nonzero components F_λ, F_γ such that $\mathcal{M}(F_\lambda) < 2^n$ and $\mathcal{M}(F_\gamma) \leqslant 2^n$.*

4 On cubic APN permutations over $\mathbb{F}^8$

It is known that there are no cubic APN permutations in dimension six (see Theorem 5.4 in [6]). We study the case of a possible cubic APN permutation in dimension eight. By Proposition 2, we know that at least two components f_1, f_2 are such that $\mathcal{M}(f_1), \mathcal{M}(f_2) \leqslant 2^n$, for any n. Based on this fact and the computational results in [20], on the classification of cubic functions up to linear and affine equivalence, we deduce the following.

Theorem 5. *Let F be a cubic APN permutation in 8 variables and let Λ be the set $\{\lambda \in \mathbb{F}^n \mid \mathcal{M}(F_\lambda) \leqslant 2^n\}$. Then the size of Λ is between 85 and 252.*

References

1. Berger, T.P., Canteaut, A., Charpin, P., Laigle-Chapuy. Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. IEEE Trans. Inf. Theory **52**(9), 4160-4170 (2006).
2. Beth, T., Ding, C.: On almost perfect nonlinear permutations. In: Advances in Cryptology - EUROCRYPT '93, vol 765, pp 65-76. Springer, Berlin, Heidelberg (1993).
3. Biham, E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY 4.1 (1991): 3-72.
4. Browning, K., Dillon, J., Kibler, R., McQuistan, M. APN polynomials and related codes. *Journal of Combinatorics, Information and System Science* 34 (2009): 135 –159.
5. Bosma, W., Cannon, J., Playoust, C. The Magma algebra system I: the user language, J. Symb. Comput. 24 (1997) 235–265.
6. Calderini, M., Sala, M., Villa I.: A note on APN permutations in even dimension, Finite Fields and Their Applications, **46**, 1-6 (2017).
7. Canteaut, A.: Cryptographic Functions and Design Criteria for Block Ciphers. In: Rangan C.P., Ding C. (eds) *Progress in Cryptology - INDOCRYPT 2001.* INDOCRYPT 2001. Lecture Notes in Computer Science, vol 2247, (2001), pp 1-16. Springer, Berlin, Heidelberg.
8. Canteaut, A., Duval, S., Perrin, L.: 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 Transactions on Information Theory, vol. 63, no. 11, pp. 7575-7591 (2017).
9. Canteaut, A., Perrin, L. Tian, S.: If a generalised butterfly is APN then it operates on 6 bits. Cryptogr. Commun. 11, 1147–1164 (2019).
10. Carlet, C.: Open Questions on Nonlinearity and on APN Functions. In: Koç, Ç., Mesnager, S., Savaş, E. (eds) Arithmetic of Finite Fields. WAIFI 2014. Lecture Notes in Computer Science(), vol 9061. Springer, Cham. (2015).
11. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge: Cambridge University Press (2021).
12. Carlet, C., Charpin, P., Zinoviev. V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography 15.2 (1998): 125-156.
13. Chee, S., Lee, S., Kim K.: Semi-bent Functions. In: Pieprzyk, J., Safavi-Naini, R. (eds.) Advances in Cryptology-ASIACRYPT'94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, vol 917, pp 107-118. Springer, Wollongong.(1994).

14. Cusick, T. W., Stanica, P.: Chapter 6 - Special Types of Boolean Functions, Editor(s): Thomas W. Cusick, Pantelimon Stanica, Cryptographic Boolean Functions and Applications (Second Edition), Academic Press, Pages 109-142 (2017).
15. Dillon, J. F.: Elementary Hadamard difference sets. Proceedings of Sixth S-E Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, pp.237–249 (1975).
16. Fontanari, C., Pulice, V., Rimoldi, A. and Sala, M.: On weakly APN functions and 4-bit S-Boxes. Finite Fields and Their Applications, 18(3), pp.522-528 (2012).
17. Hou, X.-D.: Affinity of permutations of $\mathbb{F}_2^n$. Discrete applied mathematics 154(2), pp.313-325 (2006).
18. Idrisova, V.: On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptogr. Commun. 11, 21–39 (2019).
19. Knudsen, L.: Truncated and Higher Order Differentials. In: 2nd International Workshop on Fast Software Encryption (FSE 1994). Leuven: Springer-Verlag. pp. 196–211 (1994).
20. Langevin, P.: Classification of RM(3,8)/RM(1,8). `http://langevin.univ-tln.fr/project/rm832/rm832.html`
21. MacWilliams, F.-J., Sloane, N.-J.-A.: The Theory of Error-Correcting Codes. Elsevier, New York (1977).
22. Musukwa, A., Sala, M., Villa, I., Zaninelli, M.: On cryptographic properties of cubic and splitting Boolean functions. Applicable Algebra in Engineering, Communication and Computing: 1-17 (2022).
23. Nyberg, K.: Differentially uniform mappings for cryptography. Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg (1993).
24. Perrin, L., Udovenko, A., Biryukov, A.: Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem. In: Robshaw, M., Katz, J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science(), vol 9815. Springer, Berlin, Heidelberg. (2016).
25. Wagner, D.: The boomerang attack. In International Workshop on Fast Software Encryption (pp. 156-170). Springer, Berlin, Heidelberg (1999).
26. Wu, C., Feng, D.: Boolean Functions and Their Applications in Cryptography. Springer, New York (2016).

Protocols and Zero-Knowledge

KEYNOTE: 20 Years of Leakage-Resilient Cryptography

Daniele Venturi

University of Roma La Sapienza, Italy

Abstract. This short extended abstract accompanies the author's invited talk at the conference CIFRIS'24, and celebrates 20 years since the publication of the seminal result on physically-observable cryptography by Micali and Reyzin at TCC'04.

1 Provable Security

One of the most important features underlying the design of modern cryptosystems is their *provable security*, as originally introduced by Goldwasser and Micali [3]. In a nutshell, provable security means that there exists a so-called reduction turning any efficient adversary breaking the security of our cryptosystem (in a well-defined threat model) into an efficient algorithm solving some mathematical task which is believed to be hard (and that mathematicians tried to solve for decades, or even hundreds of years). Example of such hard mathematical problems include, integer factoring, finding discrete logarithms over certain finite fields, and decoding random linear codes.

Of course, the actual security of our cryptosystem cannot be better than the guarantees provided by the threat model one introduces: the more the threat model captures reality accurately, the better. One important limitation of the most common and used threat models is the assumption that the attacker can only interact with the underlying algorithms in a black-box manner, meaning that the internal secrets and randomness are completely unknown to the adversary. Unfortunately, history taught us that such an assumption may be too restrictive, as there are practical attacks that allow the adversary to learn partial information about the secret key of a cryptosystem, resulting in devasting consequences on its security. These attacks are often known under the name of *side-channel* attacks, and exploit physical phenomena of real-world implementations based on time, power consumption, electromagnetic radiation, and more [5,6,1].

Motivated by this shortcoming, cryptographers started to investigate the design of cryptosystems provably resisting side-channel attacks. This line of research

was initiated by the work of Micali and Reyzin on physically-observable cryptography [7], which received the TCC test-of-time award in 2015. We refer the reader to the survey by Kalai and Micali [4] for a complete overview of results in leakage-resilient cryptography, and focus here on a selection of them.

2 Bounded Leakage Resilience

Definitions in leakage-resilient cryptography typically allow the adversary to obtain information on the secret key sk of a given cryptosystem. For concreteness, let us focus on the case of digital signatures: leakage resilience here means that no efficient attacker given the public key pk and some leakage $f(sk)$ for some adversarially-chosen leakage function f, as well as poly-many signatures $\sigma_1, \ldots, \sigma_n$ on adversarially-chosen messages $\mu_1, \ldots, \mu_n$, can forge a valid signature on a *fresh* message $\mu^* \notin \{\mu_1, \ldots, \mu_n\}$.

Clearly, in order for this to work, we must put some restriction on the function f, as if $f(sk) = sk$ no security at all is possible. One of the most basic restrictions is to assume that $|f(sk)| = \ell$, for some leakage bound $\ell \ll |sk|$. Under this restriction, one can obtain leakage resilience for a rich variety of cryptographic primitives, including storage, pseudorandom functions, encryption, message authentication codes, digital signatures, cryptographic circuits, and interactive protocols [4]. In the first part of the talk, we will review some of these results.

3 Simulation Theorems

One of the main reasons behind the widespread usage of the bounded leakage model is that formally proving the security of a cryptographic algorithm in this model is more approachable than for most other leakage models. However, bounded leakage does not directly capture real-world side-channel attacks. For example, transcripts produced via power analysis are typically much longer than the secret key under attack but, unlike bounded leakage, are inherently *noisy*. Motivated by this limitation, several models for noisy leakage have been studied in the literature. On the practical front, the most popular measures of a given leakage's "noisiness" are conditional min-entropy, statistical distance, and mutual information. For instance, if X denotes the secret key and Z is leakage from X, then the mutual information between X and Z—defined as $\mathsf{MI}(X;Z) = D_{\mathsf{KL}}(P_{XZ} \| P_X \otimes P_Z)$ where D_{KL} is the Kullback–Leibler divergence, P_{XZ} is the joint distribution of X and Z and $P_X \otimes P_Z$ is their product distribution—captures the mutual dependence between X and Z. Ideally, we would like to design cryptographic schemes that are secure against all noisy leakages Z satisfying $\mathsf{MI}(X;Z) \leqslant \delta$ for δ as large as possible.

A fundamental question is to study the connection between different leakage models, towards understanding whether cryptographic schemes formally proven secure under less realistic leakage assumptions remain secure against more realistic

ones. One way to handle such a question is to rely on so-called *simulation theorems* [2]. Given a secret distribution X on $\mathcal{X}$ and a leakage Z from X, we ask if there exists a simulator Sim which is allowed to choose any bounded leakage function $g : \mathcal{X} \to \{0,1\}^\ell$, learns $g(X)$, and, after post-processing of $g(X)$, outputs a simulated leakage Z' such that $(X, Z) \approx_\varepsilon (X, Z')$, where $\approx_\varepsilon$ means that the two joint distributions are within statistical distance at most ε of each other, for a small error term ε. In other words, no adversary can distinguish (with non-negligible advantage) between the real secret-leakage pair (X, Z) and the fake pair (X, Z') where Z' is produced with only the help of a single query of ℓ-bounded leakage. In the second part of the talk, we will review the main ideas behind some of these simulation theorems.

4 Open Problems

We conclude the talk with an overview of open problems and interesting directions for future research in the area of leakage-resilient cryptography. Perhaps, the most important such open question is to prove simulation theorems, with efficient simulation, for super-logarithmic values of the leakage bound $\ell(\lambda) = \omega(\log \lambda)$ (where λ is the security parameter). This would immediately allow to upgrade the computational security of *any* primitive in the presence of bounded leakage, to the more realistic setting of noisy leakage.

References

1. D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, *The EM Side-Channel(s)*, 2003, DOI 10.1007/3-540-36400-5_4.
2. G. Brian, A. Faonio, M. Obremski, J. L. Ribeiro, M. Simkin, M. Skórski, and D. Venturi, *The Mother of All Leakages: How to Simulate Noisy Leakages via Bounded Leakage (Almost) for Free*, 2021, DOI 10.1007/978-3-030-77886-6_14.
3. S. Goldwasser and S. Micali, *Probabilistic Encryption*, JCSS 20 (2), 1984, pp. 270–299.
4. Y. T. Kalai and L. Reyzin, *A survey of leakage-resilient cryptography*, Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, 2019, pp. 727–794.
5. P. C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, 1996, DOI 10.1007/3-540-68697-5_9.
6. P. C. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*, 1999, DOI 10.1007/3-540-48405-1_25.
7. S. Micali and L. Reyzin, *Physically Observable Cryptography (Extended Abstract)*, 2004, DOI 10.1007/978-3-540-24638-1_16.

Security Analysis of ZKPoK based on MQ problem in the Multi-Instance Setting

Delaram Kahrobaei[1,3], Ludovic Perret[4], and Martina Vigorito[2]

[1] City University of New York, USA
[2] University of Salerno, Italy
[3] New York University, USA
[4] Sorbonne University, France

The context: The Multivariate Quadratic (MQ) problem, defined below, is a traditional post-quantum hard problem.

Definition 1 (MQ problem). *Let m and n positive integers, we define by $\mathtt{MQ}(n, m, \mathbb{F}_q)$ the family of functions $\{\mathcal{F} = (f_1, \ldots, f_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m\}$ such that $\forall \ell, 1 \leqslant \ell \leqslant m$:*

$$f_\ell(x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{i,j}^{(\ell)} x_i x_j + \sum_{1 \leqslant i \leqslant n} c_i^{(\ell)} x_i + k^{(\ell)}, \text{ where } a_{i,j}^{(\ell)}, c_i^{(\ell)}, k^{(\ell)} \in \mathbb{F}_q. \quad (1)$$

Given $\mathcal{F} \in \mathtt{MQ}(n, m, \mathbb{F}_q)$ and $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{F}_q^m$, the MQ problem asks to find $\mathbf{s} \in \mathbb{F}_q^n$ such that :

$$f_1(\mathbf{s}) = v_1, \ldots, f_m(\mathbf{s}) = v_m.$$

We will call $\mathtt{MQ}_{\mathrm{H}}$ the restriction of MQ to homogeneous polynomials.

We investigate the security of a new ZKPoK based on MQ introduced in [3,4]. This new scheme, which we will call MQBG, is related to new variants of $\mathtt{MQ}_{\mathrm{H}}$ such as $\mathtt{MQ}_{\mathrm{H}}^{+}$. This problem occurs in the multi-instance setting and is defined as follows:

Definition 2 ($\mathtt{MQ}_{\mathrm{H}}^{+}$ problem). *Let m and n positive integers, we define by $\mathtt{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$ the family of functions $\{\mathcal{F} = (f_1, \ldots, f_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m\}$ such that $\forall \ell, 1 \leqslant \ell \leqslant m$:*

$$f_\ell(x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{i,j}^{(\ell)} x_i x_j, \text{ where } a_{i,j}^{(\ell)} \in \mathbb{F}_q. \quad (2)$$

Given $\mathcal{F} \in \mathtt{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$ and $\mathbf{v}_1, \ldots, \mathbf{v}_M \in \mathbb{F}_q^m$. The $\mathtt{MQ}_{\mathrm{H}}^{+}$ problem asks to find $\mathbf{s}_1, \ldots, \mathbf{s}_M \in \mathbb{F}_q^n$ such that :

$$\mathcal{F}(\mathbf{s}_1) = \mathbf{v}_1, \ldots, \mathcal{F}(\mathbf{s}_M) = \mathbf{v}_M.$$

These problems are widely used as the basis for many proposed post-quantum digital signature schemes, for example, UOV signature scheme [6] and MAYO signatures [2].

The authors of [3,4] claimed that the security of this MQBG relies on a new intermediate problem which is called Differential Multivariate Quadratic Homogeneous ($\texttt{DiffMQ}^{+}_{\mathrm{H}}$) problem in a multi-instance version that is:

Definition 3 ($\texttt{DiffMQ}^{+}_{\mathrm{H}}$ **problem).** *Let $M \geqslant 1$, m, n positive integers, $\mathcal{F} \in \texttt{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$ and $(\mathbf{u}_1, \mathbf{v}_1), \ldots, (\mathbf{u}_M, \mathbf{v}_M) \in \mathbb{F}_q^n \times \mathbb{F}_q^m$ such that $\mathcal{F}(\mathbf{u}_1) = \mathbf{v}_1, \ldots, \mathcal{F}(\mathbf{u}_M) = \mathbf{v}_M$. Given $\kappa_1, \kappa_2 \in \mathbb{F}_q^*$, the $\texttt{DiffMQ}^{+}_{\mathrm{H}}$ problem asks to find $(\mathbf{c}, \mathbf{d}_1, \mathbf{d}_2) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^n$ such that:*

$$\mathcal{F}(\mathbf{d}_1) + \mathbf{c} = \kappa_1^2 \mathbf{v}_{\mu_1} \quad \text{and} \quad \mathcal{F}(\mathbf{d}_2) + \mathbf{c} = \kappa_2^2 \mathbf{v}_{\mu_2}, \tag{3}$$

with $\mu_1, \mu_2 \in [1, \ldots, M]$.

More precisely, $\texttt{DiffMQ}^{+}_{\mathrm{H}}$ is related to the special soundness that is the property of a cryptographic protocol which ensures that if an adversary can convince a verifier of a false statement with some probability, then there exists an efficient algorithm that can extract a witness from any such convincing interaction.

In [4] it was initially claimed that $\texttt{DiffMQ}^{+}_{\mathrm{H}}$ is not easier than $\texttt{MQ}^{+}_{\mathrm{H}}$ ([4, Theorem 8]), i.e. if there exists a polynomial-time algorithm solving $\texttt{DiffMQ}^{+}_{\mathrm{H}}$ with success probability p, then there exist a poly-time algorithm solving $\texttt{MQ}^{+}_{\mathrm{H}}$ with probability $\left(1 - \frac{1}{q^{m-n}}\right) p$. This statement was then revisited in the updated version [3]. However, the problem is still defined, and the complexity was not known until now. The contribution of our work is to show that there is a polynomial-time algorithm that should be avoided in practice.

Polynomial-Time Algorithm for Solving $\texttt{DiffMQ}^{+}_{\mathrm{H}}$*:* We present a polynomial-time algorithm that solves $\texttt{DiffMQ}^{+}_{\mathrm{H}}$ with probability $O(1/q^{m-n})$. The main idea is that $\texttt{DiffMQ}^{+}_{\mathrm{H}}$ can be reduced to the problem of finding a collision on the quadratic system $\mathcal{F} \in \texttt{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$. Although $\texttt{MQ}_{\mathrm{H}}$ is hard, the problem of finding a collision is much easier in the case quadratic equations, see [1,5].

Theorem 1. *Let $\mathcal{F} \in \texttt{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$, where m and n are positive integers. Then there exists a probabilistic polynomial time algorithm that solve $\texttt{DiffMQ}^{+}_{\mathrm{H}}$ with probability $O(1/q^{m-n})$.*

The idea is consider the polar form $\mathcal{F}' : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^m$ associated to $\mathcal{F}$. Therefore this polar form is bi-linear and equal to:

$$\mathcal{F}'(\mathbf{x}, \mathbf{y}) = \mathcal{F}(\mathbf{x} + \mathbf{y}) - \mathcal{F}(\mathbf{x}) - \mathcal{F}(\mathbf{y}). \tag{4}$$

Let $(\mathbf{s}_1, \mathbf{v}_1), \ldots, (\mathbf{s}_M, \mathbf{v}_M) \in \mathbb{F}_q^n \times \mathbb{F}_q^m$ and $\mathcal{F}(\mathbf{s}_1) = \mathbf{v}_1, \ldots, \mathcal{F}(\mathbf{s}_M) = \mathbf{v}_M$ and $\kappa_1, \kappa_2 \in \mathbb{F}_q^*$. The algorithm recovers $(\mathbf{c}, \mathbf{d}_1, \mathbf{d}_2) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^n$ such that:

$$\mathcal{F}(\mathbf{d}_1) + \mathbf{c} = \kappa_1^2 \mathbf{v}_1 \quad \text{and} \quad \mathcal{F}(\mathbf{d}_2) + \mathbf{c} = \kappa_2^2 \mathbf{v}_2. \tag{5}$$

It has two main steps. In the first one, we eliminate $\mathbf{c} \in \mathbb{F}_q^m$ and we recover $(\mathbf{d}_1, \mathbf{d}_2) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ by solving a linear system. Finally we recover the $\mathbf{c} \in \mathbb{F}_q^n$ that fits the $(\mathbf{d}_1, \mathbf{d}_2)$ recovered in the first step.

References

1. L. Bettale, J. C. Faugère, and L. Perret, *Security Analysis of Multivariate Polynomials for Hashing*, Information Security and Cryptology, 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers, Lecture Notes in Computer Science 5487, Springer, 2008, pp. 115–124, DOI 10.1007/978-3-642-01440-6_11.
2. W. Beullens, *MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps*, Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers, Lecture Notes in Computer Science 13203, Springer, 2021, pp. 355–376, DOI 10.1007/978-3-030-99277-4_17.
3. L. Bidoux and P. Gaborit, *Compact Post-quantum Signatures from Proofs of Knowledge Leveraging Structure for the sfPKP, sfSD and sfRSD Problems*, Codes, Cryptology and Information Security - 4th International Conference, C2SI 2023, Rabat, Morocco, May 29-31, 2023, Proceedings, Lecture Notes in Computer Science 13874, Spinger, 2023, pp. 10–42, DOI 10.1007/978-3-031-33017-9_2.
4. L. Bidoux and P. Gaborit, *Shorter Signatures from Proofs of Knowledge for the SD, MQ, PKP and RSD Problems*, 2022, `https://arxiv.org/abs/2204.02915`.
5. J. Ding and B. Yang, *Multivariates Polynomials for Hashing*, Information Security and Cryptology, Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5, 2007, Revised Selected Papers, Lecture Notes in Computer Scienc 4990, Springer, 2007, pp. 358–371, DOI 10.1007/978-3-540-79499-8_28.
6. A. Kipnis, J. Patarin, and L. Goubin, *Unbalanced Oil and Vinegar Signature Schemes*, Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, Lecture Notes in Computer Science 1592, Springer, 1999, pp. 206–222, DOI 10.1007/3-540-48910-X_15.

Post-Quantum Cryptography

KEYNOTE: Algorithms for solving the matrix code equivalence problem

Simona Samardjiska

Radboud University, Netherlands

Abstract. In the past few years, there has been an increased interest in hard equivalence problems, especially with NIST's announcement of a fourth round for new designs of digital signatures. On a high level, such a problem can be defined as follows: Given two algebraic objects, find - if any - an equivalence that maps one object into the other. Several instantiations have been considered for cryptographic purposes, for example - Isomorphism of polynomials (Pattarin '96), Code equivalence (Biasse et al. '20), Matrix Code equivalence (Chou et al. '22), Alternating trilinear form equivalence (Tang et al.'22), Lattice isomorphism (Ducas and van Woerden '22). All of these problems are believed to be hard even for quantum adversaries. Conveniently, they can generically be used to build a Sigma protocol and further a post-quantum secure signature using the Fiat-Shamir transform. In this talk I will make a broad overview of algorithms for solving the matrix code equivalence problem and how they can be applied to related problems. In particular, I will focus on algebraic and graph-based algorithms which are currently the state-of-the-art for solving the problem. I will further argue that clever combination of the two techniques often leads to the best, and sometimes surprising results.

In the past few years, there has been an increased interest in hard equivalence problems, especially with NIST's announcement of a fourth round for new designs of digital signatures. On a high level, such a problem can be defined as follows: Given two algebraic objects, find - if any - an equivalence that maps one object into the other. Several instantiations have been considered for cryptographic purposes, for example - Isomorphism of polynomials (Pattarin '96 [14]), Code equivalence (Biasse et al. '20 [6,1]), Matrix Code equivalence (Chou et al. '22 [8]), Alternating trilinear form equivalence (Tang et al.'22 [17]), Lattice isomorphism (Ducas & van Woerden '22 [11]). All of these problems are believed to be hard even for quantum

De Cifris Koine – CIFRIS24 ACTA –

This research has been supported by the Dutch government through the NWO grant OCNW.M.21.193 (ALPaQCa)

adversaries. Conveniently, they can generically be used to build a Sigma protocol and further a post-quantum secure signature using the Fiat-Shamir transform.

For example, taking sets of k-tuples of multivariate polynomials over finete fields together with linear bijective transformations on the input and output basis of the polynomials, we obtain the building blocks of the IP signature [14] based on the IP problem of finding a secret basis change. Originally, the scheme used inhomogenous quadratic polynomials but this subclass of IP turned out to be easy to solve in practice [12]. However, we now know that the homogenous quadratic variant, also referred to as the Quadratic Maps Linear Equivalence (QMLE) problem is the hardest instance, very likely not efficiently solvable.

Recently, as a result of several optimization techniques [10,5,6,1] Patarin's construction became attractive again. It was revived through two new signature schemes based on the hardness of two problems closely related to QMLE. A signature scheme based on the hardness of the alternating trilinear form equivalence (ATFE) problem was introduced at Eurocrypt 2022 [17], whereas matrix code equivalence (MCE) was used in the more recently proposed construction called MEDS [8]. Both of these schemes, the first under the name of ALTEQ, were latter submitted to the additional round for digital signatures of the NIST standardization process for post-quantum cryptography [2,9].

In this talk I will make a broad overview of algorithms for solving the matrix code equivalence problem and how they can be applied to related problems. In particular, I will focus on algebraic and graph-based algorithms which are currently the state-of-the art for solving the problem. I will further argue that clever combination of the two technics often leads to the best, and sometimes surprising results.

For instance, I will describe the graph-based algorithms that stem from the algorithm of Bouillaguet et al. for the IP problem [4,7] to the case of MCE and ATFE. A direct adaptation of it provides an upper bound of $\tilde{\mathcal{O}}(q^{4n/3})$ for MCE [15] and $\tilde{\mathcal{O}}(q^{2n/3})$ for ATFE [17]. Using a different property for building the graph, [15] proposed an improvement for MCE resulting in a complexity of $\tilde{\mathcal{O}}(q^n)$. A similar collision based approach for ATFE but looking at low rank codewords was first considered in [17] and later improved by Beullens [3] to $\tilde{\mathcal{O}}(q^{\max(n-5)/2,n-7})$ for odd n and $\tilde{\mathcal{O}}(q^{\max(n-4)/2,n-4})$ for even n. Later, Beullens' attack [3] was used as the basis for setting parameters for ALTEQ [2]. A graph-walking approach inspired by [3] was recently proosed against the MCE problem in [13] breaking the Round 1 parameters of MEDS [9].

Parallel to the advancement of graph-based algorithms, major advancement was achieved in algebraic algorithms. Currently the best algebraic algorithms against MCE were developed in [8,9] and they take nontrivial approaches in adapting Leon's algorithm to the rank metric and modeling the problem algebraically but from a coding theory viewpoint. Using this improved algebraic modeling, and a thorough analysis of the algebraic structure the recent work [16] breaks the Round 1 parameters of ALTEQ.

References

1. Alessandro Barenghi, Jean-François Biasse, Edoardo Persichetti, and Paolo Santini. LESS-FM: fine-tuning signatures from the code equivalence problem. In Jung Hee Cheon and Jean-Pierre Tillich, editors, *PQCrypto 2021*, volume 12841 of *LNCS*, pages 23–43. Springer, 2021.
2. Markus Bläser, Dung Hoang Duong, Anand Kumar Narayanan, Thomas Plantard, Youming Qiao, Arnaud Sipasseuth, , and Gang Tang. The ALTEQ Signature Scheme: Algorithm Specifications and Supporting Documentation. NIST PQC Submission, 2023.
3. Ward Beullens. Graph-theoretic algorithms for the alternating trilinear form equivalence problem. Cryptology ePrint Archive, Paper 2022/1528, 2022. `https://eprint.iacr.org/2022/1528`.
4. Charles Bouillaguet, Pierre-Alain Fouque, and Amandine Véber. Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 211–227. Springer, 2013.
5. Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020*, volume 12492 of *LNCS*, pages 464–492. Springer, 2020.
6. Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini. LESS is More: Code-Based Signatures Without Syndromes. In Abderrahmane Nitaj and Amr Youssef, editors, *AFRICACRYPT 2020*, volume 12174 of *LNCS*, pages 45–65. Springer, 2020.
7. Charles Bouillaguet. *Algorithms for some hard problems and cryptographic attacks against specific cryptographic primitives*. PhD thesis, Université Paris Diderot, 2011.
8. Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Take your meds: Digital signatures from matrix code equivalence. Cryptology ePrint Archive, Paper 2022/1559, 2022. `https://eprint.iacr.org/2022/1559`.
9. Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Lars Ran, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. MEDS – Matrix Equivalence Digital Signature, 2023. Submission to the NIST Digital Signature Scheme standardization process.
10. Luca De Feo and Steven D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 759–789. Springer, 2019.
11. Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In *Advances in Cryptology–EUROCRYPT 2022: 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30–June 3, 2022, Proceedings, Part III*, pages 643–673. Springer, 2022.
12. Jean-Charles Faugère and Ludovic Perret. Polynomial equivalence problems: Algorithmic and theoretical aspects. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 30–47. Springer, 2006.

13. Anand Kumar Narayanan, Youming Qiao, and Gang Tang. Algorithms for matrix code and alternating trilinear form equivalences via new isomorphism invariants. In: Joye, M., Leander, G. (eds) Advances in Cryptology – EUROCRYPT 2024. Lecture Notes in Computer Science, vol 14653. Springer, Cham. https://doi.org/10.1007/978-3-031-58734-4_6
14. Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In *EUROCRYPT '96*, volume 1070 of *LNCS*, pages 33–48. Springer, 1996.
15. Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Hardness estimates of the code equivalence problem in the rank metric. Des. Codes Cryptogr. 92, 833–862 (2024). https://doi.org/10.1007/s10623-023-01338-x
16. Lars Ran, Simona Samardjiska, and Monika Trimoska. Algebraic algorithm for the alternating trilinear form equivalence problem. In Andre Esser and Paolo Santini, editors, *Code-Based Cryptography*, pages 84–103, Cham, 2023. Springer Nature Switzerland.
17. Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In *EUROCRYPT 2022*, volume 13277 of *LNCS*, pages 582–612. Springer, 2022.

Smaller public-keys for MinRank-based schemes

Antonio J. Di Scala and Carlo Sanna

Politecnico di Torino, Italy

Introduction

MinRank is a problem in linear algebra that was first introduced by Buss, Frandsen, and Shallit (1999) [11]. Roughly speaking, given $k+1$ matrices $M_0, \ldots, M_k$ of size $m \times n$ over a finite field $\mathbb{F}_q$, the decisional version of MinRank asks to determine if there exists a non-trivial linear combination of $M_0, \ldots, M_k$ whose rank does not exceed a fixed parameter r. The search version of MinRank, which is the one we will be focusing on hereafter, asks to find such a linear combination.

For several reasons, MinRank is an attractive candidate to build post-quantum cryptographic primitives. First, MinRank is completely based on simple linear algebra operations, which can be implemented easily and efficiently. Second, the hardness of MinRank is supported by a long line of research: MinRank is an NP-complete problem and, due to its relevance in cryptanalysis, algorithms for solving it have been extensively studied, to the extent that random instances of MinRank are expected to be hard [4,5,6,9,13,14,19,21]. Finally, there are no known quantum algorithms to solve MinRank that go beyond straightforward quantum search applications.

Several digital signature schemes based on MinRank have been proposed, namely: a scheme due to Courtois (2001) [12], MR-DSS (2022) [7], MIRA (2023) [3] (see also [16]), and MiRitH (2023) [1] (see also [2]). In particular, MIRA and MiRitH have been submitted to the NIST Post-Quantum Cryptography Standardization Process.

In all these schemes, the public key is a random instance of MinRank, the secret key is the solution of such an instance, and the signing and verification algorithms together are a non-interactive zero-knowledge proof of knowledge of the solution. While the secret key can be easily compressed as a seed of λ bits, where λ is the security parameter, compressing the public key is less obvious.

Courtois [12, Section 5.1] proposed an algorithm, which we call KeyGen1, that compresses the public key in $\lambda + mn \log q$ bits, where log is the logarithm in base 2. This method was improved in MR-DSS [7, Section 4.4] by reducing the compressed public key to $\lambda + (mn - k) \log q$ bits. This improvement, which we call KeyGen2, is employed by MIRA [3, Section 2.4.1], while MiRitH uses KeyGen1 [1, Section 3.2].

Our contribution

We propose a new key-generation algorithm for MinRank-based schemes, which we call KeyGen3, with a compressed public key of $\lambda + (m(n-r)-k)\log q$ bits. (Note that $k < m(n-r)$. In fact, all parameter sets satisfy the stronger inequality $k < (m-r)(n-r)$, in order to make the MinRank problem *overdetermined*.)

Table 1 provides a comparison of the sizes of the public keys of the three key-generation algorithms, for the parameter sets proposed for MiRitH [1, Table 1]. As it can be seen, the public-key size of KeyGen3 is about 50% of that of KeyGen2, and sits in the range of 328–676 bits for security levels of 128–256 bits.

	parameters					public key (bits)		
λ	q	m	n	k	r	KeyGen1	KeyGen2	KeyGen3
128	16	15	15	78	6	1,028	716	356
128	16	16	16	142	4	1,152	584	328
192	16	19	19	109	8	1,636	1,200	592
192	16	19	19	167	6	1,636	968	512
256	16	21	21	189	7	2,020	1,264	676
256	16	22	22	254	6	2,192	1,176	648

Table 1: Comparison of the sizes of the public keys, for the parameter sets proposed for MiRitH [1, Table 1].

Furthermore, we provide a rigorous proof that the security of KeyGen3 reduces to the security of KeyGen1 with a negligible loss. For instance, if we take $q = 16$ as in Table 1 then, roughly speaking, our main theorem says that the set of keys generated by KeyGen3 is equivalent (via an efficient transformation) to a large subset of the keys generated by KeyGen1, where "large" means more than 56% of the total. Since the MinRank problem is supposed to be hard to solve on average, considering a large subset of all the possible instances remains hard to solve on average. More precisely, KeyGen3 has a security loss of less than $\log_2(1/0.56) \approx 0.836$ bits, compared to KeyGen1.

Acknowledgements

The authors are members of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of the Politecnico di Torino. This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

References

1. G. Adj, S. Barbero, E. Bellini, A. Esser, L. Rivera-Zamarripa, C. Sanna, J. Verbel, and F. Zweydinger, *MiRitH: MinRank in the Head*, Submission to NIST, 2023, https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/MiRitH_spec-web.pdf.
2. G. Adj, L. Rivera-Zamarripa, and J. Verbel, *MinRank in-the-Head*, Progress in Cryptology - AFRICACRYPT 2023, Springer Nature Switzerland, 2023, pp. 3–27.
3. N. Aragon, L. Bidoux, J. J. Chi-Domínguez, T. Feneuil, P. Gaborit, R. Neveu, and M. Rivain, *MIRA: a Digital Signature Scheme based on the MinRank problem and the MPC-in-the-Head paradigm*, 2023, arXiv preprint https://arxiv.org/abs/2307.08575.
4. M. Bardet and M. Bertin, *Improvement of algebraic attacks for solving superdetermined MinRank instances*, Lecture Notes in Computer Science, vol. 13512, 2022, pp. 107–123.
5. M. Bardet, P. Briaud, M. Bros, P. Gaborit, and J. P. Tillich, *Revisiting algebraic attacks on MinRank and on the rank decoding problem*, 2022, Cryptology ePrint Archive, Paper 2022/1031 https://eprint.iacr.org/2022/1031.
6. M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J. P. Tillich, and J. Verbel, *Improvements of algebraic attacks for solving the rank decoding and MinRank problems*, Advances in cryptology—ASIACRYPT 2020. Part I, Lecture Notes in Computer Science, vol. 12491, Springer, 2020, pp. 507–536.
7. E. Bellini, A. Esser, C. Sanna, and J. Verbel, *MR-DSS—Smaller MinRank-based (ring-)signatures*, Post-quantum cryptography, Lecture Notes in Computer Science, vol. 13512, Springer, 2022, pp. 144–169.
8. D. J. Bernstein, T. Chou, and P. Schwabe, *McBits: Fast Constant-Time Code-Based Cryptography*, Cryptographic Hardware and Embedded Systems - CHES 2013, Springer, 2013, pp. 250–272.
9. L. Bettale, J. C. Faugère, and L. Perret, *Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic*, Designs, Codes and Cryptography. An International Journal 69 (1), 2013, pp. 1–52.
10. W. Beullens, *Improved cryptanalysis of UOV and Rainbow*, Advances in cryptology—EUROCRYPT 2021. Part I, Lecture Notes in Computer Science, vol. 12696, Springer, 2021, pp. 348–373.
11. J. F. Buss, G. S. Frandsen, and J. O. Shallit, *The computational complexity of some problems of linear algebra*, Journal of Computer and System Sciences 58 (3), 1999, pp. 572–596.
12. N. T. Courtois, *Efficient zero-knowledge authentication based on a linear algebra problem MinRank*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Computer Science, vol. 2248, Springer, 2001, pp. 402–421.
13. J. C. Faugère, F. Levy-dit-Vehel, and L. Perret, *Cryptanalysis of MinRank*, Advances in cryptology—CRYPTO 2008, Lecture Notes in Computer Science, vol. 5157, Springer, 2008, pp. 280–296.
14. J. C. Faugère , M. Safey El Din, and P. J. Spaenlehauer, *Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology*, ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, ACM, 2010, pp. 257–264.

15. J. C. Faugère, M. Safey El Din, and P. J. Spaenlehauer, *On the complexity of the generalized MinRank problem*, Journal of Symbolic Computation, vol. 55, 2013, pp. 30–58.
16. T. Feneuil, *Building MPCitH-based Signatures from MQ, MinRank, Rank SD and PKP*, 2022, Cryptology ePrint Archive, Paper 2022/1512 `https://eprint.iacr.org/2022/1512`.
17. S. D. Fisher and M. N. Alexander, *Classroom Notes: Matrices over a finite field*, American Mathematical Monthly 73 (6), 1966, pp. 639–641.
18. P. Gaborit, O. Ruatta, and J. Schrek, *On the complexity of the rank syndrome decoding problem*, Institute of Electrical and Electronics Engineers. Transactions on Information Theory 62 (2), 2016, pp. 1006–1019.
19. A. Kipnis and A. Shamir, *Cryptanalysis of the HFE public key cryptosystem by relinearization*, Advances in cryptology—CRYPTO '99 (Santa Barbara, CA), Lecture Notes in Computer Science, vol. 1666, Springer, 1999, pp. 19–30.
20. C. Tao, A. Petzoldt, and J. Ding, *Efficient key recovery for all HFE signature variants*, Advances in cryptology—CRYPTO 2021. Part I, Lecture Notes in Computer Science, vol. 12825, Springer, 2021, pp. 70–93.
21. J. Verbel, J. Baena, D. Cabarcas, R. Perlner, D. Smith-Tone, *On the complexity of "superdetermined" MinRank instances*, Post-quantum cryptography, Lecture Notes in Computer Science, vol. 11505, Springer, 2019, pp. 167–186.

Investigation of Metabelian Platform Groups for Protocols Based on the (Simultaneous) Conjugacy Search Problem.

Delaram Kahrobaei[1,2,3,5], Carmine Monetta[4], Ludovic Perret[6], Maria Tota[4], and Martina Vigorito[4]

[1] University of York, UK
[2] Queens College, City University of New York, USA
[3] Tandon School of Engineering, New York University, USA
[4] University of Salerno, IT
[5] Initiative for the Theoretical Sciences, City University of New York, USA
[6] Sorbonne University, France

The context: The field of group-based cryptography began with the seminal work of Anshel, Anshel and Goldfeld in 1999 when they proposed a Commutator Key-Exchange protocol related on the difficulty of solving Simultaneus Conjugacy Search Problem in certain classes of groups, namely braid groups [1]. The search for a platform group for this protocol has been an active area including several cryptanalysis. In general to be a suitable platform group there are certain properties that the platform must satisfy, for instance we need fast computation of the products and fast comparison of the elements. Indeed the group has to be finitely presented, to allow fast computation. Finally the problem on which the protocol is based should be hard in the underling platform. Then a good candidate could be a polycyclic groups. In fact polycyclic groups are natural generalizations of cyclic groups and they have been used in the classical crytosystems such as RSA [9]. Actually Eick and Kahrobaei in [2] introduced a new line of investigation for cryptograpghy which has been called polycyclic group-based cryptography. More precisely, they proposed such groups as platform for the Commutator Key-Exchange protocol, also known as Anshel-Anshel-Goldfeld (a.k.a. AAG) [1], as well as for the non-commutative Diffie-Hellman Key-Exchange protocol (a.k.a. Ko-Lee) [5]. The security of these protocols is based on the difficulty of solving the Simultaneous Conjugacy Search Problem (SCSP) and the Conjugacy Search Problem (CSP), respectively, in the underlying platform group. Their argument is based on experimental results for the CSP for certain metabelian polycyclic groups arising from field extensions. These groups are not virtually nilpotent, hence the CSP cannot be solved using the analysis provided in [8]. Nevertheless, some of these groups must be avoided as platform since, in [6], Kotov and Ushakov cryptanalysed SCSP for some groups of this type. A connected work is due to Gryak, Kahrobaei and Martinez Perez who investigated another class

of metabelian groups. Indeed, in [7] they obtain a complexity result concerning the CSP which is proved to be at most exponential for the analyzed class of groups.

Our contribution: In this paper we go further to the results FBA in [6] and we analyze the complexity of CSP and SCSP for some other classes of metabelian groups. We noticed that whereas the CSP seems to be at most exponential in [7], the SCSP and CSP with some extra restrictions are much easier and we will show it in an alternative way. In particular the families of metabelian groups we are interested in are of the form $G = M \ltimes N$, with both groups M and N abelian. This kind of groups are metabelian and arise quite naturally in linear algebra and ring theory.

Example 1. Let $V(+, \cdot)$ be a vector space over a field F. Take the group M as the multiplicative group F^* of F and the group N as the additive group of V. If $\lambda \in F^*$ and $v \in V$, the action of λ maps v to $v \cdot \lambda$. Hence $G = F^* \ltimes V$ has the same structure of the general group we considered before. Similarly we could start with a module over a commutative unitary ring.

Specifically, for a particular example of these metabelian groups we have proved the following theorems, which could be applied also when G is as described in Example 1:

Theorem 1. *Let $G = M \ltimes N$, where $M \cong \mathbb{Z}^n$ and $N = \mathbb{Z}[m_1^{\pm 1}, \ldots, m_n^{\pm 1}]$ (as additive groups), with $m_1, \ldots, m_n$ positive integers, then there exists a polynomial-time algorithm that solves SCSP, which implies that is possible to break Commutator Key-Exchange protocol for such a group G.*

Theorem 2. *Let $G = M \ltimes N$, where $M \cong \mathbb{Z}^n$ and $N = \mathbb{Z}[m_1^{\pm 1}, \ldots, m_n^{\pm 1}]$ (as additive groups), with $m_1, \ldots, m_n$ positive integers, then there exists a polynomial-time algorithm that solves CSP, which implies that is possible to break Diffie-Hellmann Key-Exchange protocol for such a group G.*

References

1. I. Anshel, M. Anshel, and D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Let. 6, 287–291, 1999.
2. B. Eick and D. Kahrobaei, *Polycyclic groups: A new platform for cryptology?*, 2004.
3. D. Kahrobaei, R. Flores and M. Noce, *Group-based Cryptography in the Quantum Era*, Notices of the American Mathematical Society, 752–763, 2023.
4. D. Kahrobaei, R. Flores, M. Noce, M. Habeeb, and C. Battarbee, *Applications of Group Theory in Cryptography*, American Mathematical Society, The Mathematical Surveys and Monographs series of the American Mathematical Society, 2024.
5. K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, *New public-key cryptosystem using braid groups*, Advances in cryptology, CRYPTO 2000, vol. 1880, 166–183, 2000.

6. M. Kotov and A. Ushakov, *Analysis of a certain polycyclic-group-based cryptosystem*, Journal of Mathematical Cryptology, vol. 9, 161–167, 2015.
7. J. Gryak, D. Kahrobaei, and C. Martinez-Perez, *On the conjugacy problem in certain metabelian groups*, Glasgow Mathematical Journal, Cambridge University Press **61**, Issue 2, 251–269, 2019.
8. C. Monetta and A. Tortora, *The multiple conjugacy search problem in virtually nilpotent polycyclic groups*, Advances in Group Theory and Applications, vol. 13, 61-70, 2022.
9. R. Rivest, A. Shamir and L. Adelman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM., vol. 2, 463-474, 1978.

Public-Key Cryptography

First-degree prime ideals of composite extensions

Giordano Santilli[1] and Daniele Taufer[2]

[1] Agenzia per la Cybersicurezza Nazionale
[2] KU Leuven

Let $\theta \in \mathbb{C}$ be an algebraic integer, i.e. the complex root of a monic integer polynomial. It is known that principal ideals generated by elements of the form $e + d\theta$ in the ring $\mathbb{Z}[\theta]$, for coprime integers e and d, can be factored only by means of prime ideals of prime norm [3]. These ideals of degree 1, therefore called *first-degree prime ideals*, have been exploited for designing the celebrated General Number Field Sieve algorithm [4]. Such a routine, which is nowadays the best non-quantum method for factoring large integers, requires decomposing a huge quantity of ideals of type $(e + d\theta) \subset \mathbb{Z}[\theta]$, and employing relations among them to retrieve the integer factorization [1].

When θ is a root of a biquadratic polynomial, the problem of computing the first-degree primes dividing $(e + d\theta)$ was proved to be better solved, in all but exceptional cases, in quadratic subfields [5]. The solution goes as follows: if $f \in \mathbb{Z}[x]$ is the minimal polynomial of θ, one can represent first-degree prime ideals in $\mathbb{Z}[\theta]$ as pairs (t, p), where p is a prime integer (namely, the norm of the considered ideal), and $t \in \mathbb{F}_p$ is a root of $f \bmod p$ [3]:

$$\ker(\mathbb{Z}[\theta] \to \mathbb{F}_p,\ \theta \mapsto t) \quad \longleftrightarrow \quad (t, p).$$

Then, one constructs every such (t, p) as a *combination* of first-degree primes in the underlying quadratic fields:

$$(r, p), \quad (s, p) \quad \xrightarrow{\text{Combination}} \quad (r + s, p).$$

As simple as this construction is, it is proven to span the utmost majority of ideals of $\mathbb{Z}[\theta]$ with a prime norm. In addition, it respects the divisibility of ideals $(e + d\theta)$, therefore it can be conveniently applied for factoring them.

The limit of the above approach is that biquadratic fields are special extensions that have been widely investigated for theoretical reasons, but rarely appear in computational practice. Moreover, although it has proved to be more efficient, the computation in two quadratic fields is not significantly faster than those in the biquadratic extension they generate. In the present work [6], we prove that the same idea can actually be applied to composite fields of *any* degree, turning it into a general and more applicable tool in computational algebra. Besides, we also prove that the practical advantage depends on the smoothness of the degree extensions,

which makes it resounding in the case of large extensions obtained by chains of smaller ones. In the same paper, we provide both theoretical and computational evidence for such an improvement.

More generally, [6] establishes a novel framework for studying first-degree prime ideals and their divisibility of principal ideals. In fact, from a theoretical purview, we prove that this approach deeply relies on the description of the minimal polynomial of extension fields as subsequent resultants of the underlying minimal polynomials. This construction always works when the underlying number fields are *linearly disjoint*, which is known to be a weak assumption satisfied by every pair of reasonably uncorrelated fields. Furthermore, the edge cases are completely characterized: we show that, in prescribed rare circumstances, this approach can fail for two fundamentally different reasons:

- it may fail to read *every* first-degree prime ideal in the underlying field, starting from the composite one, or
- the divisibility in the underlying fields is not necessarily carried over the composite one.

We provide examples for every pathological situation, although we argue that such cases almost never occur, especially when the considered number fields are normal and with coprime degrees. Thus, despite their theoretical interest, these edge cases are irrelevant for computational purposes, as we experimentally verify that it is barely possible to find any of them for large norms. Moreover, even when some of the exceptional hypotheses are met, the lack of correspondence involves only sporadic ideals, while all the others still arise from combinations and respect divisibility. The Magma [2] code employed for the current work is publicly available at [7].

In conclusion, in the suborder $\mathbb{Z}[\theta]$ of composite extensions of linearly disjoint number fields, we proved that first-degree prime ideals can be read (almost) entirely from the relative norms inside their minimal subfields. Moreover, we showed that the correspondence by combination preserves the divisibility of ideals $(e + d\theta) \subset \mathbb{Z}[\theta]$, with a few numerical exceptions. Those are novel results, whose theoretical implications and computational applications certainly deserve further exploration.

References

1. D.J. Bernstein, A.K. Lenstra, *A General Number Field Sieve implementation*, in The Development of the number field sieve, Springer, 1993, pp. 103–126.
2. W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24, 1997, pp. 235–265.
3. J.P. Buhler, H.W. Lenstra, C. Pomerance, *Factoring integers with the number field sieve*, in The Development of the number field sieve, Springer, 1993, pp. 50–94.
4. A.K. Lenstra, H.W. Lenstra, M.S. Manasse, J.M. Pollard, *The number field sieve*, in The Development of the number field sieve, Springer, 1993, pp. 11–42.

5. G. Santilli, D. Taufer, *First-degree Prime Ideals of Biquadratic Fields Dividing Prescribed Principal Ideals*, Mathematics 8 (9), 2020.
6. G. Santilli, D. Taufer, *First-degree prime ideals of composite extensions*, ArXiv: 2111.04660 (2024).
7. G. Santilli, D. Taufer, *Magma implementation*, available at `https://github.com/DTaufer/First-degree-prime-ideals/blob/main/MagmaCode.m`.

A Novel Related Nonce Attack for ECDSA

Marco Macchetti and Nils Amiet

Kudelski Security, Switzerland

Introduction. Digital signatures are nowadays ubiquitous and find application in secure communication protocols, code authentication, public key infrastructures and block-chain technologies. Control of funds deposited in any digital wallet is eventually based on the capability of its owner to prove ownership and sign transactions using an associated private key in a digital signature scheme. One of the most widely adopted digital signature standards, based on elliptic curve cryptography (ECC), is ECDSA [1]. Due to the high performance and small signature and key size, ECDSA has been adopted in many applications, from TLS to Bitcoin. A study [11] conducted in early 2021 on the top market-cap 100 blockchains showed that 74 coins use ECDSA as digital signature scheme (over the **secp256k1** curve [4]).

The generation of an ECDSA signature is arguably a fragile process, requiring the creation and use of cryptographically strong random values; it is understandable that its security has been widely scrutinized and that attacks exploiting bad implementations have been extensively published [9], [5], [10], [2]. Even if the ECDSA signature generation is performed securely, if the nonce values k are not properly generated in a random way, attacks become possible. An example would be if the k values are biased, that is if their distribution over the interval $[1, n-1]$ is not uniform. for example if they contain known prefixes, suffixes or common bit sequences [6], or if they are generated using non cryptographic PRNGs [3],[8],[2]. This latter case is particularly interesting; if nonces are generated using Linear Congruential generators (LCGs), the signatures can be likely used to mount an attack by means of Lattice Reduction algorithms [7], and the signer's key can be obtained.

The biases used in [7], [3] and exploited so far in the literature can be seen as simple relations between the nonce bits, or linear relations between the full nonce values. Up to our knowledge, there are no published studies on cases where the nonce values are related in a more complicated way, for instance by means of quadratic, cubic or higher-degree algebraic relationships. This is the goal of this work, and is motivated by the fact that examples of non-cryptographic PRNGs include quadratic and cubic congruential generators [12].

Our contributions. We advance the state of the art by proposing a novel attack that exploits high-degree relationships among the random values (nonces) used to generate several signatures, allowing to retrieve the signer's private key. Our method is not exploiting any side channel information coming from the signature genera-

tion process, but is rather a cryptanalytic attack that can be run, under certain assumptions, on a relatively small set of signatures generated by a private key.

In our investigations, we make the assumption that nonces used to generate several ECDSA signatures are subject to an unknown polynomial relationship modulo n, where n is the order of the curve's generator point; more precisely, we suppose that they satisfy a recurrence polynomial equation of arbitrary degree and unknown coefficients modulo n. In this case it is very easy to recover the private key using only few signatures, without the need of lattice reduction.

The first step we need to perform is to find a way to get rid of the unknown coefficients involved in the recurrence equation; to this purpose, we devise a recursive algorithm that is able to rewrite the unknown recurrence relation as a polynomial involving only differences of nonces. Then, we can use the relationships between the nonces and the private key given by the second half of each signature to rewrite the polynomial only in terms of the private key. Finally, we show that we can use known algorithms to find the roots of the polynomial; the private key will always be obtained as a root of the polynomial. The attack works on all prime curves currently standardized and in use for ECDSA (including Bitcoin curve **secp256k1**) and up to our knowledge, it is the first to exploit relationships of degrees higher than linear.

Cases where nonces are generated with Linear Congruential Generators (LCG), quadratic or cubic generators with unknown coefficients modulo n, are special cases of this general category of relationships. After showing how to attack nonces generated with an arbitrary recurrence relation, we then prove that even sets of fully random nonces allow the attacker to retrieve the private key when the set is completed by one additional nonce that follows the (unknown) recurrence relation given by the random nonces taken in a given order (we refer to this as the *rogue nonce* example). When a sufficient number of signatures are generated with a given private key, there will always be a reordering of the signatures that make the recurrence attack work, leading to compromise of the private key. However, we are not able to find this ordering faster than brute-force.

We also show how to perform attacks in the case where the LCG uses a modulo which is different from the order of the curve; if the LCG multiplier is small enough, we can write suitable point equations and employ a dictionary-based approach (thus requiring pre-computation) to retrieve the private key from few signatures (2 if the LCG coefficients are known). Based on preliminary trials, we speculate that multipliers up to 44-bit length could be attacked using rainbow tables when the modulo of the LCG has approximately the same bit length of the curve order.

Future work. Our attack could be extended to cover Schnorr signatures. It would also be interesting to devise generic techniques that would allow retrieval of the private key in the case where the modulo used by the recurrence relation is different from the order of the curve, improving our preliminary results; this seems an interesting case for known LCG, QCG and CCG such as the ones referenced in [12]. Even if it would probably be necessary to make further assumptions, for instance that

the moduli should be co-prime, we consider this as the most interesting evolution of the work presented here.

References

1. *FIPS186-5, Digital Signature Standard (DSS)*, National Institute of Standards and Technologies, 2023, available at `https://csrc.nist.gov/publications/detail/fips/186/5/final`.
2. D. F. Aranha, F. R. Novaes, A. Takahashi, M. Tibouchi, and Y. Yarom, *LadderLeak: Breaking ECDSA with Less than One Bit of Nonce Leakage*, Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020, pp. 225–242, DOI 10.1145/3372297.3417268.
3. J. Breitner and N. Heninger, *Biased Nonce Sense: Lattice Attacks Against Weak ECDSA Signatures in Cryptocurrencies*, Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers, Lecture Notes in Computer Science 11598, pp. 3–20, DOI 10.1007/978-3-030-32101-7_1.
4. D. R. L. Brown, *SEC 2: Recommended elliptic curve domain parameters*, 2010, `http://www.secg.org/sec2-v2.pdf`.
5. E. De Mulder, M. Hutter, M. E. Marson, and P. Pearson, *Using Bleichenbacher"s Solution to the Hidden Number Problem to Attack Nonce Leaks in 384-Bit ECDSA*, Cryptographic Hardware and Embedded Systems - CHES 2013, pp. 435–452, ISBN 978-3-642-40349-1.
6. J. C. Faugère, C. Goyet, and G. Renault, *Attacking (EC)DSA Given Only an Implicit Hint*, Selected Areas in Cryptography, 2013, pp. 252–274, ISBN 978-3-642-35999-6.
7. Google, *Project Paranoid – checks for weaknesses in ECDSA generation*, available at `https://github.com/google/paranoid_crypto/blob/main/docs/ecdsa_signature_tests.md`.
8. N. Heninger, *RSA, DH, and DSA in the Wild*, IACR Cryptol. ePrint Arch., 2022, `https://eprint.iacr.org/2022/048`.
9. N. A. Howgrave-Graham and N. P. Smart, *Lattice Attacks on Digital Signature Schemes*, Designs, Codes and Cryptography 23, 2001, pp. 283–290.
10. J. Jancar, V. Sedlacek, P. Svenda, and M. Sys, *Minerva: The curse of ECDSA nonces (Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces)*, IACR Transactions on Cryptographic Hardware and Embedded Systems 4, 2020, pp. 281–308, DOI 10.13154/tches.v2020.i4.281-308.
11. Nash, *Cryptography behind the top 100 cryptocurrencies*, `http://ethanfast.com/top-crypto.html`.
12. M. O. Saarinen, *SP 800–22 and GM/T 0005–2012 Tests: Clearly Obsolete, Possibly Harmful*, 2022 IEEE European Symposium on Security and Privacy Workshops, pp. 21-37, DOI 10.1109/EuroSPW55150.2022.00011.

Application of Mordell–Weil lattices with large kissing numbers to acceleration of multi-scalar multiplication on elliptic curves

Dmitrii Koshelev ⋆

University of Lleida, Spain

It is not a secret that elliptic curves E over finite fields $\mathbb{F}_q$ of huge characteristics p are actively used in discrete logarithm cryptography. Multi-scalar multiplication (MSM) in the $\mathbb{F}_q$-point group $E(\mathbb{F}_q)$ is widely recognized as a very slow operation. To be more precise, it is about computing the sum $\sum_{i=1}^{N} n_i P_i$ for given $N \in \mathbb{N}$ "basis" points $P_i \in E(\mathbb{F}_q)$ and integers $n_i \in \mathbb{Z}$. At the same time, MSM is actually a ubiquitous primitive in advanced protocols of elliptic curve cryptography. Therefore, there is a vital need among implementers to speed up the given primitive.

As a confirmation of these words, one can mention the relatively recent ZPRIZE 2022 competition [1] (see also ZPRIZE 2023 [2]). Among its objectives was accelerating MSM on certain elliptic $\mathbb{F}_q$-curves $E_b\colon y^2 = x^3 + b$ (of j-invariant 0). The money rewards of this competition were quite tempting (the total prize was \$4,415,000), which indicates the importance of the topic. As is well known, $j = 0$ curves are the most attractive in pairing-based cryptography. Furthermore, they enjoy the most efficient group operation (at least among prime-order curves). That is why curves E_b are a popular choice for implementation of discrete logarithm-based protocols, even if they do not deal with pairings.

There are numerous algorithms of MSM (see, e.g., [3,4,5] and references therein). All of them in one way or another are reduced to precomputing auxiliary points of the form $P_v := \sum_{i=1}^{N} v_i P_i$ with various integer vectors $v = (v_i)_{i=1}^{N}$. The points P_v are then utilised (depending on the concrete n_i) in the main part of an MSM algorithm, allowing to avoid a lot of repeating elliptic curve additions. By the way, $P_i = P_{e_i}$, where $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ are the standard basis vectors of the lattice $\mathbb{Z}^N$.

In fact, the points P_v become less useful whenever the vectors v are long with respect to a certain norm on $\mathbb{Z}^N$. In this situation, P_v seem to be too redundant points in the sense that we cannot often apply them during multi-scalar multiplication. The author decided to work with the 1-norm $|v|_1 = \sum_{i=1}^{N} |v_i|$ to stay with little naturals. Besides, it is the most suitable to reflect the "complexity" of the points P_v. Indeed, if $|v_i| \leqslant 2$ and more frequently $|v_i| \leqslant 1$ (as it turns out in this paper), then

De Cifris Koine – CIFRIS24 ACTA –

⋆ https://www.researchgate.net/profile/dimitri-koshelev

The author was supported by Ethereum Foundation.

the 1-norm almost coincides with the minimal number of additions on E necessary for computing P_v given v_i and P_i. Thus, it is sufficient to focus on vectors $v \in \mathbb{Z}^N$ that lie in the ball of some small radius $R \in \mathbb{N}$, i.e., $|v|_1 \leqslant R$. In particular, they have to possess maximum R non-zero coordinates.

For elliptic curves having an $\mathbb{F}_q$-endomorphism τ of degree close to 1, the famous GLV (Gallant–Lambert–Vanstone) decomposition can be applied in addition to accelerate MSM even more. As a consequence, MSM algorithms exploiting GLV are based rather on the auxiliary points

$$P_{(v,u)} := P_v + \tau(P_u) = \sum_{i=1}^{N} v_i P_i + u_i \tau(P_i)$$

with coefficients $u_i \in \mathbb{Z}$ that equally constitute the short vector $u := (u_i)_{i=1}^N$. By abuse of notation, instead of $P_{(v,u)}$ let's write just P_v with $v \in \mathbb{Z}^{2N}$ such that $v_{N+i} = u_i$.

Of course, having a huge amount of available memory or a wide communication channel, the desired points P_v can be found once and for all to regularly restore them from the given memory or channel. However, this solution is vulnerable to the constant danger that a malicious entity will perform a fault attack, somehow replacing one or several points in such a way that this breaks a cryptosystem. On the other hand, it is much easier to protect only basic information storing in a small piece of memory (or establish it over a reliable, but slow channel) from which every point P_v can be safely (re)generated. It is clear that the described strategy, applied directly to the points, is too expensive in any sense of the word.

The recent works [12,11] are devoted to the problem of generating efficiently the "basis" points P_i. In these works it is suggested to express $N = (N \operatorname{div} n)n + (N \bmod n)$ for a little $n \in \mathbb{N}$. Besides, we are given n linearly independent points $P_i(t)$ from the *Mordell–Weil (MW) group* $\mathcal{E}(F)$ of a certain non-trivial twist $\mathcal{E}$ of E over the function field $F := \mathbb{F}_q(t)$. In the literature $\mathcal{E}$ is often called *isotrivial elliptic surface*. Then, n "basis" points can be obtained at once as the specialization of $P_i(t)$ at an element $t \in \mathbb{F}_q$. Transparently changing $t \in \mathbb{F}_q$, nothing prevents from applying the same procedure N div n (plus one if $n \nmid N$) times to obtain N points. In fact, $\mathcal{E}(F)$ has the structure of a Euclidean lattice modulo the torsion subgroup $\mathcal{E}(F)_{tor}$. The corresponding (positive definite) quadratic form $\widehat{h} \colon \mathcal{E}(F) \to \mathbb{Q}_{\geqslant 0}$ is said to be *canonical height*. However, this lattice structure previously played only a minor role in the cryptographic context under consideration.

The present work extends the above generation method to a considerable proportion of the points P_v, not exclusively P_i. It is proposed to pick MW lattices (of rank r) with large *kissing* (a.k.a. *Newton*) *number* k. By definition, it is the number of *the shortest* (i.e., *minimal*) non-zero lattice points. The norm of the F-point $P_v(t) := \sum_{i=1}^{r} v_i P_i(t)$, where $v = (v_i)_{i=1}^r \in \mathbb{Z}^r$, is an indicator of how quickly $P_v(t)$ can be evaluated at elements of $\mathbb{F}_q$. Indeed, the degrees of the point coordinates

are proportional to the norm. And the more minimal points we have, the greater performance gain takes place. That is why we are interested in large k with respect to r, that is, in maximizing the quantity $\delta := \log_2(k)/r$. It can be seen that the generation of P_i from [12,11] corresponds to the case when $\mathcal{E}(F)$ is realized as the trivial lattice $\mathbb{Z}^r$, because e_i are its unique minimal vectors up to sign.

The task of constructing arbitrary lattices having large kissing numbers is one of the most classical tasks in mathematics. It has been carefully studied for several centuries. Established lower and upper bounds on k in the first dimensions can be found in any lattice database like [6,13]. In turn, asymptotic results as $r \to \infty$ are well surveyed, e.g., in [15]. In that article Vlăduţ constructs a *k-asymptotically good family* of lattices for which the kissing number grows exponentially, that is, $\limsup_{r\to\infty} \delta > 0$. Unfortunately, this inequality probably does not hold for families of MW lattices, making them always *k-asymptotically bad*.

The last drawback is slightly mitigated for supersingular elliptic surfaces $\mathcal{E}$, because for them, δ decreases more slowly. In a series of articles [7,8,9] Elkies thoroughly studies MW lattices of such surfaces in characteristic 2. For moderate ranks, he (re)discovers lattices with the greatest known kissing numbers. Among the obtained lattices there is in particular the 24-dimensional *Leech lattice* Λ_{24} whose $k = 196560$, the optimal kissing number for $r = 24$. Regarding an odd characteristic p, it is worth mentioning Shioda's remarkable article [14] about certain supersingular surfaces E_{p+1} of j-invariant 0. Their MW lattices have the non-constant parameters $r = \Theta(p)$ and $k = \Omega(p^2)$. Therefore, for p of a cryptographic size, k is an order of magnitude greater than r. However, we cannot employ the given results in discrete logarithm cryptography, because supersingular elliptic curves E are known to be weaker than ordinary ones, especially for little p.

Fortunately, at least for even ranks $r \leqslant 8$, it is still possible to achieve the optimal kissing numbers through the MW lattices of ordinary elliptic surfaces, although we are forced to restrict ourselves to $j = 0$. By the way, in the extreme case $r = 8$, the largest $k = 240$. It is about the classical *root lattice* E_8, which is wonderful (in many senses) to the same extent as Λ_{24}. For other constant ordinary j-invariants, the author does not find in the literature examples of elliptic surfaces whose MW lattices enjoy quite large kissing numbers, not to mention the optimal ones. The situation when k is not substantially greater than r does not merit separate attention. As a consequence, we do not lose much, dealing hereafter only with curves E_b.

In the end, it is worth saying that the full version of the current article is available on the web page [10].

Acknowledgements. The author expresses his gratitude to Antonio Sanso and Justin Drake from Ethereum Foundation for motivation (and help in searching for financial support) they provided to complete this article. Besides, the author was contacted by Victor Miller with appreciation for the previous work [11], which also encouraged to continue research in this direction.

References

1. *ZPRIZE 2022 competition*, available at `https://github.com/z-prize`.
2. *ZPRIZE 2023 competition*, available at `https://www.zprize.io`.
3. R. M. Avanzi, *The complexity of certain multi-exponentiation techniques in cryptography*, Journal of Cryptology 18, 2005, pp. 357–373.
4. D. J. Bernstein, *Pippenger's exponentiation algorithm*, available at `https://cr.yp.to/papers/pippenger-20020118-retypeset20220327.pdf`, 2002.
5. G. Botrel and Y. El Housni, *Faster Montgomery multiplication and multi-scalar-multiplication for SNARKs*, Transactions on Cryptographic Hardware and Embedded Systems (TCHES) (3), 2023, pp. 504–521.
6. H. Cohn, *Kissing numbers*, `https://cohn.mit.edu/kissing-numbers`.
7. N. D. Elkies, *Mordell–Weil lattices in characteristic* 2*, I: Construction and first properties*, International Mathematics Research Notices (8), 1994, pp. 343–361.
8. N. D. Elkies, *Mordell–Weil lattices in characteristic* 2*, II: The Leech lattice as a Mordell–Weil lattice*, Inventiones Mathematicae 128 (1), 1997, pp. 1.8.
9. N. D. Elkies, *Mordell–Weil lattices in characteristic* 2*, III: A Mordell–Weil lattice of rank* 128, Experimental Mathematics 10 (3), 2001, pp. 467–473.
10. D. Koshelev, *Application of Mordell–Weil lattices with large kissing numbers to acceleration of multi-scalar multiplication on elliptic curves*, `https://eprint.iacr.org/2023/1384`, 2023.
11. D. Koshelev, *Generation of two "independent" points on an elliptic curve of j-invariant* $\neq 0, 1728$, `https://eprint.iacr.org/2023/785`, 2023.
12. D. Koshelev, *Generation of "independent" points on elliptic curves by means of Mordell–Weil lattices*, Mathematical Cryptology 4 (1), 2024, pp. 11–22.
13. G. Nebe and N. Sloane, *LATTICES*, `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES`.
14. T. Shioda, *Mordell–Weil lattices and sphere packings*, American Journal of Mathematics 113 (5), 1991, pp. 931–948.
15. S. Vlâduţ, *Lattices with exponentially large kissing numbers*, Moscow Journal of Combinatorics and Number Theory 8 (2), 2019, pp. 163–177.

Theoretical Cryptography

KEYNOTE:
Low Latency Designs: Primitives and Beyond

Gregor Leander

Ruhr University Bochum, Germany

Abstract. In this talk, I will explore the current advancements in low-latency cryptographic primitives, focusing on their design, challenges, and practical applications.

Latency is a fundamental consideration when designing symmetric cryptographic primitives, yet achieving minimal latency presents a unique set of challenges compared to other performance metrics. At its core, the quest for a low-latency cipher involves determining the minimum computational effort required to maintain secure encryption—an open question that remains unresolved in the cryptographic community. Beyond its theoretical significance, low latency is critical for practical applications.

1 Block ciphers

Recent advances in cache encryption and pointer authentication have led to the development of new cryptographic primitives with unconventional parameters, particularly featuring extremely short block sizes. Two notable examples are BibBip [1] and SCARF [2], which require fresh design strategies and introduce new models for potential attackers. This underscores the ongoing evolution of low-latency cryptographic research. Several low-latency (tweakable) block ciphers have been created to address these emerging demands, including PRINCE [3], PRINCEv2 [4], MANTIS [5], QARMA [6], QARMAv2 [7], and SPEEDY [8]. Applications also come in the form of authenticated encryption schemes [9]. With the exception of SPEEDY, these ciphers generally follow the Substitution-Permutation Network (SPN) structure, utilizing 4-bit S-boxes for the non-linear layers and almost Maximum Distance Separable (MDS) matrices for the linear layers. Most support a 64-bit block size, while some extend to 128 bits. A key innovation introduced by PRINCE is the α-reflection property, which allows for efficient low-latency implementations of both encryption and decryption, setting a benchmark for further developments in this area.

De Cifris Koine – CIFRIS24 ACTA –

2 Memory Encryption

Memory encryption, commonly used in high-end smart cards, is another domain where low-latency cryptographic primitives play a vital role. Such primitives are also critical in hardware-assisted security mechanisms like pointer authentication (as seen in IBM's SecureBlue, Intel's SGX, and AMD's SEV), secure caches, and specialized hardware instructions designed to defend against software-based attacks. In these scenarios, reducing latency is crucial for maintaining system performance while ensuring strong security. However, low-latency decryption circuits are not always required. Instead, applications often necessitate encrypting larger block sizes—exceeding 128 bits—without introducing significant delays. To meet these requirements, SPEEDY was designed with large low-latency S-boxes optimized for such cases. Although these innovations offer promising solutions, the field remains under-explored, opening up opportunities for further research and development.

References

1. Anonymous, *BipBip: A Low-Latency Tweakable Block Cipher with Small Dimensions*, IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2023, No. 1, pp. 326–368, 2023, DOI: 10.46586/tches.v2023.i1.326-368.
2. F. Canale, T. Güneysu, G. Leander, J. P. Thoma, Y. Todo, and R. Ueno, *SCARF – A Low-Latency Block Cipher for Secure Cache-Randomization*, in Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, USA, pp. 1937–1954, 2023.
3. J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçın, *PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications*, in Advances in Cryptology – ASIACRYPT 2012, Springer, pp. 208–225, 2012.
4. D. Božilov, M. Eichlseder, M. Knežević, B. Lambin, G. Leander, T. Moos, V. Nikov, S. Rasoolzadeh, Y. Todo, and F. Wiemer, *PRINCEv2: More Security for (Almost) No Overhead*, in Selected Areas in Cryptography: 27th International Conference, Halifax, NS, Canada (Virtual Event), Revised Selected Papers, pp. 483–511, 2020.
5. C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, *The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS*, in Advances in Cryptology – CRYPTO 2016, Springer, pp. 123–153, 2016.
6. R. Avanzi, *The QARMA Block Cipher Family*, IACR Transactions on Symmetric Cryptology, Vol. 2017, No. 1, pp. 4–44, 2017, DOI: 10.13154/tosc.v2017.i1.4-44.
7. R. Avanzi, S. Banik, O. Dunkelman, M. Eichlseder, S. Ghosh, M. Nageler, and F. Regazzoni, *The QARMAv2 Family of Tweakable Block Ciphers*, IACR Transactions on Symmetric Cryptology, Vol. 2023, No. 3, pp. 25–73, 2023.
8. G. Leander, T. Moos, A. Moradi, and S. Rasoolzadeh, *The SPEEDY Family of Block Ciphers: Engineering an Ultra Low-Latency Cipher from Gate Level for Secure Processor Architectures*, IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2021, No. 4, pp. 510–545, 2021, DOI: 10.46586/tches.v2021.i4.510-545.
9. B. Chakraborty and M. Nandi, *The mF mode of authenticated encryption with associated data*, Journal of Mathematical Cryptology, vol. 16, no. 1, pp. 73–97, 2022.

Polynomial functional encryption schemes

Maria Ferrara, Paolo Santonastaso, Antonio Tortora, and Ferdinando Zullo

Università degli Studi della Campania "Luigi Vanvitelli", Italy

In recent years, *functional encryption* has proved very useful in several contexts such as cloud services, digital payments, digital identity verification, and IoT device management, as well as in all scenarios where it can be very advantageous to provide functional access over encrypted data.

The concept of functional encryption was introduced in [4,11]. It captures the notions of *Identity-Based Cryptography* [12] and *Attribute-Based Encryption* [9], and also extends public-key encryption by introducing the use of certain functionalities. The main feature of functional encryption schemes is that the key generation algorithm enables the creation of functional keys associated with a specific function F. When such functional keys are used to decrypt a ciphertext, the protocol outputs the function evaluation of the associated function F applied to the data.

The first construction of functional encryption scheme is based on *inner product* [1]. In this case, for a given ciphertext $\mathbf{x}$ and a secret key $\mathbf{y}$, the protocol returns the inner product $\langle \mathbf{x}, \mathbf{y} \rangle$. Over the years, there have been several examples of functional encryption protocols that differ from each other in the chosen functionalities. We suggest [10] for a detailed survey.

One of the main generalizations of inner-product functional encryption scheme is the quadratic scheme, first introduced in [3]. The main feature of these schemes is that the functionality $\mathcal{F}$ returns, for a given ciphertext $\mathbf{x}$, a secret key $\mathbf{y}$ and a matrix A, the product $\mathbf{x}A\mathbf{y}^\top$. After that, several quadratic FE protocols have been developed (see for instance [2,5,13,6,8]), increasing both the security and the efficiency of computations, and making the FE quadratic scheme a useful tool for applications in different contexts, including quadratic networks and privacy-enhanced machine learning models.

In this talk, motivated by the construction of practically efficient functional encryption scheme supporting more than linear functionalities, we describe a new functional encryption scheme whose functionalities are polynomials. Such scheme is an extension of the quadratic encryption scheme proposed in [7].

Precisely, our set of functionalities consists of all polynomials in the variables $x_1, \ldots, x_n$, whose monomials contain at most two different variables and whose degrees are bounded by certain integers α and β.

Based on these functionalities, we propose the construction of an FE scheme, where the ciphertext size is linear in $(\alpha + \beta)n$. The scheme turns is proven to be secure in the Generic Bilinear Group Model.

Keywords: functional encryption · quadratic scheme · bilinear pairing.

References

1. M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval, *Simple functional encryption schemes for inner products*, IACR International Workshop on Public Key Cryptography, Springer, 2015, pp. 733–751.
2. S. Agrawal, R. Goyal, and J. Tomida, *Multi-input quadratic functional encryption from pairings*, Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part IV 41, Springer, 2021, pp. 208–238.
3. C. E. Z. Baltico, D. Catalano, D. Fiore, and R. Gay, *Practical functional encryption for quadratic functions with applications to predicate encryption*, Annual International Cryptology Conference, Springer, 2017, pp. 67–98.
4. D. Bohen, A. Sahai, and B. Waters, *Functional encryption: Definitions and challenges*, Theory of Cryptography: 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings 8, Springer, 2011, pp. 253–273.
5. S. Chen, A. Modi, S. Agrawal, and A. Khisti, *Quadratic Functional Encryption for Secure Training in Vertical Federated Learning*, 2023 IEEE International Symposium on Information Theory (ISIT), 2023, pp. 60–65.
6. Q. Chu, L. Lin, C. Qian, and J. Chen, *Registered Functional Encryption for Quadratic Functions from MDDH*, Cryptology ePrint Archive, 2024.
7. E. Dufour-Sans, R. Gay, and D. Pointcheval, *Reading in the dark: Classifying encrypted digits with functional encryption*, Cryptology ePrint Archive, 2018.
8. R. Gay, *A new paradigm for public-key functional encryption for degree-2 polynomials*, IACR International Conference on Public-Key Cryptography, Springer, 2020, pp. 95–120.
9. V. Goyal, O. Pandey, A. Sahai, and B. Waters, *Attribute-based encryption for fine-grained access control of encrypted data*, Proceedings of the 13th ACM conference on Computer and communications security, 2006, pp. 89–98.
10. C. Mascia, M. Sala, and I. Villa, *A survey on functional encryption*, Advances in Mathematics of Communications 17 (5), 2023, pp. 1251–1289.
11. A. O'Neill, *Definitional issues in functional encryption*, Cryptology ePrint Archive, 2010.
12. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology: Proceedings of CRYPTO 84 4, Springer, 1985, pp. 47–53.
13. J. Tomida, *Unbounded quadratic functional encryption and more from pairings*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 543–572.

Modern Techniques in Somewhat Homomorphic Encryption Schemes

Massimo Giulietti, Paolo Martinelli, and Marco Timpanella

University of Perugia, Italy

1 Context

The concept of homomorphic encryption was introduced by Rivest, Adleman, and Dertouzos in 1978 [9]. It enables computations on encrypted data without requiring decryption. This capability has profound implications for data privacy and secure computation. Homomorphic encryption schemes are categorized into three main types: Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and Fully Homomorphic Encryption (FHE).

PHE supports unlimited operations of a single type (e.g., either addition or multiplication), which is useful in specific applications like secure voting systems or financial computations. SWHE allows for various operations but with a limited number of each type, offering a balance between operational flexibility and efficiency. FHE, realized through Gentry's breakthrough in 2009, permits unlimited operations of any type, enabling complex computations on encrypted data and opening new possibilities in cloud computing and privacy-preserving machine learning [4].

Before Gentry's work, SWHE schemes like Polly Cracker and the Boneh-Goh-Nissim (BGN) scheme laid important groundwork. Polly Cracker supported both addition and multiplication but suffered from impractical ciphertext growth [8]. In contrast, the BGN scheme allowed unlimited additions and a single multiplication while maintaining constant ciphertext size, making it a practical choice for specific applications [1]. These early schemes highlighted the potential and challenges of homomorphic encryption, setting the stage for future developments.

2 Contribution

This paper emphasizes the transition from classic SWHE schemes to modern approaches utilizing lattice-based problems, such as Learning With Errors (LWE). LWE, introduced by Regev, is central to both SWHE and FHE due to its security reductions to hard lattice problems, which are conjectured to be resistant to quantum attacks [7]. This makes LWE-based schemes particularly attractive for constructing secure and efficient homomorphic encryption systems.

De Cifris Koine – CIFRIS24 ACTA –

One of the notable advancements in this area is the Brakerski-Vaikuntanathan (BV) scheme, which avoids the use of ideal lattices and instead relies on standard LWE assumptions [3]. The BV scheme achieves FHE through a process called bootstrapping, which transforms a somewhat homomorphic scheme into a fully homomorphic one. Bootstrapping involves refreshing the ciphertext to reduce noise, thereby enabling more operations without increasing error.

Further enhancements in efficiency and performance have been achieved by schemes based on Ring-LWE (RLWE) and NTRUEncrypt. These schemes leverage the algebraic structure of polynomial rings to transfer lattice problems into a more efficient domain, allowing for practical implementations of homomorphic encryption. RLWE-based schemes, such as FV and BGV, are notable for their improved efficiency and security in a post-quantum context [6,2]. NTRUEncrypt, on the other hand, is distinguished by its efficient key generation and encryption processes, which make it suitable for a wide range of applications [5].

3 Conclusion

This paper has provided an overview of the evolution of somewhat homomorphic encryption schemes, highlighting significant algorithms and their impacts on cryptography. From foundational work like BGN to modern LWE-based methods, SWHE continues to shape secure computing paradigms, offering practical solutions for privacy-preserving data processing. The advancements in SWHE, particularly those leveraging lattice-based techniques, are paving the way for more secure and efficient cryptographic systems in the era of post-quantum cryptography.

The continued development of SWHE schemes is crucial for advancing data privacy and security, particularly as computational demands grow and quantum computing becomes a tangible threat. Future research will likely focus on optimizing these schemes for specific applications, reducing computational overhead, and enhancing scalability. As such, SWHE remains a vibrant and essential area of research within the broader field of cryptography.

References

1. D. Boneh, E.J. Goh, and K. Nissim, *Evaluating 2-DNF formulas on ciphertexts*, Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2. Springer Berlin Heidelberg, 2005, pp. 325–341.
2. Z.Brakerski, and V. Vaikuntanathan, *Leveled fully homomorphic encryption without bootstrapping*, ITCS, pp. 309-325.
3. Z.Brakerski, and V. Vaikuntanathan, *Efficient fully homomorphic encryption from (standard) LWE*, SIAM Journal on Computing, 2014, pp.831–871.

4. C. Gentry, *Fully homomorphic encryption using ideal lattices*, Proceedings of the forty-first annual ACM symposium on Theory of computing, 2009, pp.169-178.
5. J. Hoffstein, and J. Pipher, and J.H. Silverman, *NTRU: A ring-based public key cryptosystem*, Algorithmic number theory, 1998, pp. 267-288.
6. V. Lyubashevsky, C. Peikert, and O. Regev, *On ideal lattices and learning with errors over rings*, Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. Springer Berlin Heidelberg, 2010.
7. O. Regev, *Lattices in computer science*. arXiv preprint `arXiv:0906.5343`, 2009.
8. E. Rieffel, and W. Polak, *The theory and practice of homomorphic encryption*, IBM Research, 2011.
9. R.L. Rivest, L. Adleman, and M.L. Dertouzos, *On data banks and privacy homomorphisms*, Foundations of secure computation 4.11, 1978, pp. 169-180.

Applied Cryptography

Dynamic-FROST: Schnorr Threshold Signatures with a Flexible Committee

Annalisa Cimatti[1], Francesco De Sclavis[2], Giuseppe Galano[2,3], Sara Giammusso[2], Michela Iezzi[2], Antonio Muci[2], Matteo Nardelli[2], and Marco Pedicini[1]

[1] Roma Tre University, Italy
[2] Bank of Italy*, Italy
[3] University of Pisa, Italy

Threshold signatures allow any subgroup of t signers out of n participants to generate a signature which cannot be forged by any subgroup with fewer than t members. They offer scalability and confidentiality: the length of the aggregated signature remains constant and does not increase with t or n, and the identity of actual signers remains confidential, as it is not disclosed by the aggregated signature. Among threshold signature schemes, FROST [5] leverages the additive property of Schnorr signatures to produce a joint one that looks like a simple, single Schnorr signature. Furthermore, FROST has many desirable properties for decentralized applications: it constructs signatures so that no central dealer is required to generate and distribute keys or to sign; it achieves Existential Unforgeability under Chosen-Message Attack (EUF-CMA); it achieves efficient communication by reducing the protocol to just two rounds.

Motivation for Dynamic-FROST. FROST signatures have a fixed committee and a fixed threshold t. It might be interesting for some applications to allow the committee or the threshold to change without changing the group secret. For example, advanced self-custodial cryptocurrency wallets might require a FROST-powered dynamic threshold signature that enables users to alter the set of signers, but without moving funds to a new address, i.e., without modifying the group public key through a blockchain transaction. In 2023, the Human Rights Foundation announced it would award 1 bitcoin to any mobile wallet that successfully implements such a feature [4]. Threshold signatures can also be employed by a committee of validators in a permissioned blockchain to authenticate new blocks, as outlined in [1]. In this scenario, the composition of the validators' committee might evolve over time (e.g., due to governance adjustments), and thus the set of signers or the threshold would need to be updated accordingly. In such cases, changing the group public key would require upgrading all participants' nodes, otherwise newly signed blocks would be considered invalid.

De Cifris Koine – CIFRIS24 ACTA –

* All views are those of the authors and do not necessarily reflect the position of Bank of Italy.

CHURP Proactive Secret Sharing. To change the shares without modifying the group secret, we employ CHURP [6], a Dynamic Proactive Secret Sharing scheme (DPSS). The basic idea is to generate a two-variable polynomial which has two different degrees in the two variables: the lower-degree variable is used to distribute polynomial shares, which are used to perform signatures; the higher-degree one is used to pass a set of polynomials to a new committee, which can be used to generate new shares, so that both the committee and the threshold can be changed. The phase during which the shares are proactivized is the *handoff* and it is periodically executed at fixed intervals called *epochs*.

Our contribution. We present a novel protocol called *Dynamic FROST* (D-FROST), which combines FROST with CHURP to accomodate dynamic committees and threshold changes in a FROST threshold signature. The idea behind CHURP derives from a technique outlined in [3], and is based on two-variable polynomials, while FROST uses one-variable ones. To combine these two approaches, we create a bridge between the two protocols and prove the resulting scheme's security properties. To blend FROST and CHURP together, after FROST Key Generation, the committee transitions to a *steady state*, i.e., a state in which CHURP can be executed. After CHURP is executed, FROST signatures can be made with the newly generated shares. Then, at the beginning of every epoch, CHURP's handoff is executed again, and new FROST signatures can be performed; there is no need to repeat the key generation or the transition to a steady state. To the best of our knowledge, this is the first protocol that allows Schnorr-based threshold signatures with a dynamic committee and a dynamic threshold without changing the group public key. We provide insight into how the resulting protocol inherits both FROST's and CHURP's properties: the signature is still EUF-CMA secure, and proactivizing the shares does not reveal additional information to malicious participants. Further details can be found in [2].

References

1. M. Benedetti, F. De Sclavis, M. Favorito, G. Galano, S. Giammusso, A. Muci, and M. Nardelli, *Certified Byzantine Consensus with Confidential Quorum for a Bitcoin-derived Permissioned DLT*, Proc. of the 5th Distributed Ledger Technology Workshop, 2023.
2. A. Cimatti, F. De Sclavis, G. Galano, S. Giammusso, M. Iezzi, A. Muci, M. Nardelli, and M. Pedicini, *Dynamic-FROST: Schnorr Threshold Signatures with a Flexible Committee*, 2024, Cryptology ePrint Archive, Paper 2024/896, `https://eprint.iacr.org/2024/896`.
3. A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, *Proactive Secret Sharing Or: How to Cope With Perpetual Leakage*, Proc. of CRYPTO '95, Springer-Verlag, 1995, pp. 339–352.
4. HRF *Human Rights Foundation Bounties*, 2023, available at `https://hrfbounties.org/` (Accessed on July 16, 2024).

5. C. Komlo and I. Goldberg, *FROST: Flexible Round-Optimized Schnorr Threshold Signatures*, Selected Areas in Cryptography, Springer, 2021, pp. 34-65.
6. S. K. D. Maram, F. Zhang, L. Wang, A. Low, Y. Zhang, A. Juels, and D. Song, *CHURP: Dynamic-Committee Proactive Secret Sharing*, Proc. of ACM SIGSAC CCS '19, ACM, 2019, pp. 2369–2386.

BTLE: Atomic Swaps with Time-Lock Puzzles

Barbara Fadi[1], Enrico Guglielmino[2], Nadir Murru[3], and Claudio Schifanella[1]

[1] Università di Torino, Italy
[2] Politecnico di Torino, Italy
[3] Università di Trento, Italy

With the emergence of numerous projects based on blockchain, another problem came to the surface: the problem of communication between these different distributed systems. Formally, given two blockchains, the problem consists in the ability to operate transactions between one blockchain and another. This problem is generally referred to as Cross Chain Communication [5,2]. The most used method today to achieve synchronicity between two blockchains is based on Hashed Time-Lock Contract (HTLC) [3]. While heavily used, this is not the only method to achieve synchronicity: another method is based on time-lock puzzles. The method proposed by Rivest et al. [4] aims to obtain time-bounded encryption: the goal is to obtain a method to make a message remain encrypted only for a predictable amount of time. A time-lock puzzle is also described as a "time capsule" for a message. In our case, the time-lock puzzle is used by Alice and Bob to reveal part of a private key to obtain the counterpart funds while maintaining security. For example, if Alice behaves dishonestly, Bob is able to redeem her funds, knowing that Alice cannot steal them before a certain time defined by Bob himself in the time-lock puzzle. Unfortunately, however, there are few systems to implement a time-lock puzzle other than Rivest's method. In this paper1 we propose a new method to obtain time-lock puzzles starting from Rivest's method, laying the groundwork for further study to create new puzzles in different environments. As pointed out in Zamyatin et al [5], most decentralized coin-transfer methods proposed so far in the literature involve only two parties. This works for a single exchange, but makes it difficult to implement the proposed method in a context similar to online exchanges. In fact, in the case of an online exchange, there are many participants who intend to operate the same exchange, at the same time and at the same rate while competing for first place. This is a many-1 setting, instead of a 1-1 as in the case of Alice and Bob explained before. A visual representa- tion of the difference can be seen in Figure 1. Another assumption generally made and implicit in the methods proposed in literature is that these par- ties already know each other before making the exchange. In reality this is a very strong assumption and that makes it difficult to implement the proposed system retaining the same security guarantees. To face this problem, a cen- tralization tweak is operated during the implementation where the algorithm of connection and knowledge of the two participants is operated on a

De Cifris Koine – CIFRIS24 ACTA –

central server. In the context of markets, this connection algorithm is called matching algorithm. It is necessary to study methods that give the possibility to exchange funds in a multitude of contexts without requiring that the participants know each other beforehand, especially at a time when traditional financial methods are moving towards decentralized finance. For these reasons, our solution is broadcasted, meaning it deal with multiple participants concurrently in a many-1 environment. Therefore it is a Broadcast Time-Lock Exchange (BTLE). Our contributions in this context are the following:

- We propose a off-line and decentralized matching algorithm
- We propose a decentralized exchange method (i.e., one that works with- out the help of a trusted third party) using the time-lock puzzle as a synchronization tool
- We introduce a new type of time-lock puzzle based on the Pell conic [1] and we explain how to extend it to become a Verifiable Delay Function
- We compare the time-lock puzzle proposed by Rivest et al. and the one mentioned before
- We propose an implementation of both the decentralized matching algorithm and the decentralized exchange protocol2
- We prove the security of the method in the hybrid ideal/real world simulation in the presence of static malicious adversaries
- We conducted an analysis of the method in terms of time

References

1. E. Bellini and N. Murru, *An Efficient and Secure RSA-like Cryptosystem Exploiting Rédei Rational Functions over Conics*, Finite Fields and Their Applications 39, 2016, pp. 179–194, 10.1016/j.ffa.2016.01.011.
2. V. Buterin, *Chain Interoperability*, R3 Research Paper, 2016.
3. M. Herlihy, *Atomic Cross-Chain Swaps*, Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, ACM, 2018, pp. 245–254, 10.1145/3212734.3212736.
4. R. L. Rivest, A. Shamir, D. A. Wagner, *Time-Lock Puzzles and Timed-Release Crypto*, 1996.
5. M. Zamani, M. Movahedi, and M. Raykova, *RapidChain: Scaling Blockchain via Full Sharding*, Proceedings of the 2018, ACM, SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, pp. 931–948, 10.1145/3243734.3243853.

Part IV
Workshops

WORKSHOP
FCiR - Financial Cryptography in Rome 2024

Organizers: Michela Iezzi and Massimiliano Sala

KEYNOTE: Secure and Private Data Sharing in Financial Institutions

Carsten Maple

University of Warwick, United Kingdom

Abstract. Financial institutions are increasingly relying on data to inform strategy and operations but are hampered from sharing this information within and beyond their organisation for a range of reasons. This talk will present some of the use cases for information sharing and present recent work in Privacy Enhancing Technologies, including Homomorphic Encryption, that has facilitated such information exchange.

KEYNOTE: Progress on Private Computation

Christian Rechberger

Graz University of Technology, Austria

Abstract. Encrypting all kinds of traffic on the internet is ubiquitous since about a decade, that 'lock icon' in some corner in our browser windows is a symbol of that. The invention and development of public key cryptography in the decades before was a major driver behind this development. The elephant in the room: In order to compute on the transmitted data, it needs to be decrypted, hence forgoing many of the protections at that point. New inventions and developments in cryptography are about to close this gap: Homomorphic encryption, secure multiparty computation, or zero-knowledge proofs. Huge efficiency improvements have already been achieved, and more improvements are in the pipeline. Open-source solutions are maturing. Commercialization, albeit in its infancy, is in progress. We review some of these developments and sketch the road ahead.

De Cifris Koine – CIFRIS24 ACTA –

Layer-2 Innovations for Scalable Blockchain Payments

Giuseppe Galano

Bank of Italy, Italy

Abstract. The work explores Layer-2 innovations designed to enhance the scalability of payments within Bitcoin's distributed ledger technology. By leveraging potential future advancements in blockchain capabilities, more sophisticated second-layer solutions can be envisioned, addressing the challenges of traditional off-chain protocols while maintaining security. The discussion centers on the most promising proposals and their trade-offs.

De Cifris Koine – CIFRIS24 ACTA –

Decentralized Finance: Labyrinth

Amit Chaudhary

Labyrinth Technology, UK

Abstract. We propose a middleware solution designed to facilitate seamless integration of privacy using zero-knowledge proofs within various multi-chain protocols, encompassing domains such as DeFi, gaming, social networks, DAOs, e-commerce, and the metaverse. Our design achieves two divergent goals: to preserve consumer privacy while achieving finance regulation compliance.

In [1,2] we face the problems of achieving privacy in blockchain applications while simultaneously providing guarantees that all legal requirements are met. We summarize here our findings and we invite the readers to try our free open-source prototypes at `https://www.labyrinthprotocol.tech`.

Achieving privacy in blockchain applications presents unique challenges - often requiring trade-offs between user experience and privacy. The transparent nature of conventional blockchains reveals all of the transaction data, including addresses, assets involved, amount, smart-contract data, and timestamps, out to the public. It is analogous to using a regular bank account and revealing all private financial information, deterring the mass adoption of blockchain and digital asset technology. As this space continues to evolve and more institutional and individual users engage in activities on these applications, privacy will become a paramount concern creating the biggest hurdle for achieving mainstream adoption. Individuals contemplating the adoption of blockchain-based payment systems may exhibit considerable hesitance if their salaries or other confidential financial details, such as payments for medical services and their online purchases, are accessible to the public. This demand for privacy will also be from social networking platforms, decentralized lending protocols, philanthropic platforms, e-commerce, gaming, and other protocols where users want to prioritize safeguarding the privacy of their information. While there is a clear need for privacy solutions, regulatory scrutiny of privacy protocols necessitates action to develop practical and fair measures that deter bad actors from engaging in on-chain illicit activity. Selective Deanonymization lays out a method for allowing traceability. Particularly, an instantiation of involuntary deanonymization can prove to be a flagship regulation-compliant technique, that can be used when a malicious actor refuses to comply with the law. In our two papers and in our prototype,

De Cifris Koine – CIFRIS24 ACTA –

we propose a privacy-preserving solution with solid regulatory compliance using zero-knowledge proofs and threshold cryptography having the following features:

- A general purpose multi-chain privacy solution spanning across multiple EVM chains.
- Available with simple, composable and flexible plug-and-play middleware solution via an SDK.
- Secure with built-in compliance solution with con- crete AML practices.
- Providing a seamless user-experience using account abstraction and wallet integrations.

1 Limitations in current architecture

At present most widely used programmable blockchains (e.g. EVM based chains such as Ethereum, Polygon, Optimism, Arbitrum) offer benefits such as permissionless nature, decentralization, and security, but these blockchains do not offer privacy. Alternative blockchain networks have been aiming to create solutions from scratch, to eliminate the pitfalls but fail to near the activity and value of mentioned public chains. This necessitates a solution to multiple problems on the public chain itself.

2 Labyrinth

To tackle problems, as discussed above, Labyrinth offers a packaged solution that acts as a privacy middleware with built-in compliance. Privacy and compliance-related complexity are abstracted away by providing the developers with an SDK that facilitates a plug-and-play solution. As a consequence, we give back to the protocols and developers their freedom to innovate, so that they can focus on solving their core problem instead of worrying about user privacy or compliance

References

1. N. Sahu, M. Gajera, A. Chaudhary, and H. Ivy-Law, *Balancing Blockchain Privacy and Regulatory Compliance by Selective De-Anonymization*, arXiv preprint arXiv:2311.08167, 2023. Available: https://arxiv.org/pdf/2311.08167.pdf.
2. N. Sahu, M. Gajera, and A. Chaudhary, *zkFi: Privacy-Preserving and Regulation Compliant Transactions using Zero Knowledge Proofs*, June 2023. Contacts: nvnx@zkfi.tech, mitul@zkfi.tech, amit@zkfi.tech.

Confidential Knowledge Graphs through Synthetic Augmentation

Luigi Bellomarini, Costanza Catalano, Andrea Coletta, and Michela Iezzi

Bank of Italy, Italy

Abstract. Sharing Knowledge Graphs (KGs) between organisations is essential to set up effective business processes in the financial domain, yet this should be done without disclosing privacy-sensitive data. In this work, we show that existing literature offers techniques to anonymize graphs, but does not support the presence of derived knowledge, like in the case of KGs. We investigate poten tial approaches for developing privacy-preserving techniques using synthetically augmented KGs.

De Cifris Koine – CIFRIS24 ACTA –

WORKSHOP
ReAdPQC - Recent Advances in Post-Quantum Cryptography 2024

Organizers: Giulio Codogni, Roberto La Scala, Edoardo Persichetti, and Federico Pintore

KEYNOTE: Post-Quantum Signatures from Secure Multiparty Computation

Thibauld Feneuil

CryptoExperts, France

Abstract. The MPC-in-the-Head (MPCitH) paradigm is a versatile framework to design zero-knowledge proofs and post-quantum signatures, by relying on secure multi-party computation (MPC) techniques. It has recently been improved in a series of works which makes it a practical and tunable tool. This paradigm has been utilized in 9 out of the 40 candidates selected for the first round of the recent NIST call for additional post-quantum signatures. In this talk, I will provide a general introduction to MPCitH, discuss the latest MPCitH techniques, and show how they can be used to build efficient post-quantum signatures.

De Cifris Koine – CIFRIS24 ACTA –

The Regular Multivariate Quadratic Problem

Rocco Mora
Joint work with Antoine Joux

CISPA Helmholtz Center for Information Security, Germany

Abstract. In this talk, we introduce a new NP-complete variant of the multivariate quadratic problem. The computational challenge involves finding a solution to an algebraic system that meets the "regular" constraint, meaning that each block of the solution vector contains only one nonzero entry. Following this, we adapt and compare various techniques of cryptanalysis to study the asymptotic complexity of the average instance.

The MQ problem and its use in cryptography. The problem of solving a multivariate quadratic system over a finite field takes the name of Multivariate Quadratic (MQ) problem and is known to be NP-complete. It also seems to be hard on average for a wide range of parameters, but despite its evident difficulty, numerous algorithms have been developed to solve it. The MQ problem is fundamental in cryptography, especially in the post-quantum realm. It serves as the foundation for designing multivariate public key cryptosystems, which form one of the most promising quantum-resistant alternatives. In particular, it has emerged over the years as being remarkably well-suited to the construction of digital signatures. It is even more pervasive in algebraic cryptanalysis, which has a crucial impact on many different families of primitives. Indeed, algebraic attacks consist of modeling a cryptographic problem in terms of a polynomial system and breaking the former by finding a solution for the latter.

A new variant of the MQ problem. We present here a new variant of the MQ problem. Whilst the polynomial equations are sampled at random and do not present any particular structure, the solution is required to have a regular shape. Concretely, if the solution is a vector of $n = lw$ variables split into w blocks each of length l, then it must have exactly one nonzero entry for each block. The NP-completeness of the multivariate quadratic problem is preserved when adding the regular condition to the solution.

The same regular constraint was originally introduced in the context of code-based cryptography in [1]. Indeed, [1] proposed a family of cryptographic hash functions based on the provably secure regular syndrome decoding problem. More recently, the same problem received new attention thanks to its introduction in

De Cifris Koine – CIFRIS24 ACTA –

secure computation to design MPC-protocols [8], pseudorandom correlation generators [3] and a digital signature from MPC-in-the-head [5]. These works suggest that also the RMQ problem could be used for similar constructions.

Our contribution. After introducing the computational problem and overviewing its main features, we mainly focus on the study of the asymptotic complexity of the average RMQ instance in the setting of the uniqueness bound. Differently from regular syndrome decoding [7], the RMQ problem is not affected by ISD techniques. Instead, we analyzed the most important families of techniques for solving boolean systems and adapted them to take advantage of the regularity of the solution. On one side, we explore the algebraic algorithms related to Gröbner basis computation [6,2] by modeling the regular constraint as additional equations to be satisfied, reviewing different ways of hybridization and estimating the solving degree, in a similar fashion to what has been done for the code-based counterpart in [4]. On the other hand, we investigate how the research line of probabilistic polynomial methods initiated with [9] applies and can be optimized to our context. We also show how an RMQ instance can be transformed into a standard MQ one with fewer variables and analyze the complexity of solving the new system. Finally, we provide comparisons among all the algorithms examined. Despite the improvements presented, we conclude that the problem remains difficult in practice in the average case for many interesting parameters and therefore it is potentially suitable for cryptographic purposes.

References

1. D. Augot, M. Finiasz, and N. Sendrier, *A family of fast syndrome based cryptographic hash functions*, Progress in Cryptology–Mycrypt 2005: First International Conference on Cryptology in Malaysia, Kuala Lumpur, Malaysia, September 28-30, 2005. Proceedings 1, Springer, 2005, pp. 64–83.
2. M. Bardet, J. C. Faugère, B. Salvy, and P. J. Spaenlehauer, *On the complexity of solving quadratic boolean systems*, Journal of Complexity 29 (1), Elsevier, 2013, pp. 53–75.
3. E. Boyle, G. Couteau, N. Gilboa, and Y. Ishai, *Compressing vector OLE*, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 896–912.
4. P. Briaud and M. Øygarden, *A new algebraic approach to the regular syndrome decoding problem and implications for PCG constructions*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 391–422.
5. E. Carozza, G. Couteau, and A. Joux, *Short signatures from regular syndrome decoding in the head*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2023, pp. 532–563.
6. N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2020, pp. 392–407.

7. A. Esser and P. Santini, *Not just regular decoding: asymptotics and improvements of regular syndrome decoding attacks*, Annual International Cryptology Conference, Springer, 2024, pp. 183–217.
8. C. Hazay, E. Orsini, P. Scholl, and E. Soria-Vazquez, *TinyKeys: A new approach to efficient multi-party computation*, Journal of Cryptology 35 (2), Springer, 2022.
9. D. Lokshtanov, R. Paturi, S. Tamaki, R. Williams, and H. Yu, *Beating brute force for systems of polynomial equations over finite fields*, Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, 2017, pp. 2190–2202.

MinRank Attacks in Multivariate Cryptography

Ryann Cartor

Clemson University, USA

Abstract. This talk focuses on the cryptanalysis of post-quantum cryptography schemes, particularly focusing on multivariate and rank-metric code-based cryptosystems. As quantum computing advances, these schemes have gained attention for their unique performance characteristics, but they are vulnerable to MinRank attacks, which have exposed critical security flaws. The MinRank problem, central to these attacks, has been effectively used to break several prominent cryptosystems. This presentation will examine two distinct MinRank-based attacks on the multivariate encryption scheme HFERP, offering new insights into cryptanalytic techniques and their implications for the future of post-quantum cryptography. The discussion highlights the necessity of continuous cryptanalysis and innovation in developing quantum-resistant cryptosystems.

As the National Institute of Standards and Technology (NIST) continues its efforts to standardize post-quantum cryptographic algorithms, there is a growing need to explore diverse cryptographic schemes that can withstand the challenges posed by quantum computing. Among the potential candidates, multivariate cryptography and rank-metric code-based schemes have gained attention for their unique performance characteristics. Multivariate schemes are known for their fast encryption times and relatively short ciphertexts, while rank-metric code-based schemes offer efficient key sizes and operations compared to their hamming-weight counterparts, while still boasting strong security assumptions. However, both types of cryptosystems have been significantly impacted by MinRank attacks, leading to critical vulnerabilities and necessitating a thorough re-evaluation of their security.

The MinRank problem, which is central to these attacks, involves finding linear combinations of given matrices such that the resulting matrix has a rank lower than a specified threshold. Despite being NP-hard, recent algorithmic advancements, especially in [2], have made the MinRank problem a powerful tool for cryptanalysis. This technique has been successfully applied to break several prominent cryptosystems, including Rainbow [3], GeMSS [1], RQC, and ROLLO [2].

In this talk, we will focus on the cryptanalysis of the multivariate encryption scheme HFERP [4]. The HFERP central maps combine multiple types of equations, including those shaped like HFE, Rainbow, and random quadratic polynomials [5].

De Cifris Koine – CIFRIS24 ACTA –

This cryptanalysis introduces two different MinRank attacks. The first attack uses a "divide and conquer" approach and uses insights from the Simple Attack [3], which previously broke the Rainbow scheme. Interestingly, while the Simple Attack applied MinRank techniques in one direction, our attack uses these techniques in an orthogonal manner, opening a new dimension of cryptanalytic potential. Additionally, we apply support minors techniques on a MinRank instance where the coefficients are drawn from the big field, a method previously effective against other multivariate big field schemes [6].

This talk will provide a comprehensive review of the MinRank problem and its use in cryptanalysis, followed by an in-depth discussion of our two distinct MinRank-based attacks on HFERP. We will also explore the broader implications of these findings for multivariate cryptography and suggest new directions for future research in post-quantum cryptography. Our results underscore the importance of continuous cryptanalysis and the need for diverse approaches in the development of quantum-resistant cryptosystems.

References

1. J. Baena, P. Briaud, D. Cabarcas, R. A. Perlner, D. Smith-Tone, and J. A. Verbel, *Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow*, Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III, Lecture Notes in Computer Science 15309, Springer, 2022, pp. 376–405, DOI `https://doi.org/10.1007/978-3-031-15982-4_13`.
2. M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J. P. Tillich, and J. A. Verbel, *Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems*, Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I, Lecture Notes in Computer Science 12491, Springer, 2020, pp. 507–536, DOI `https://doi.org/10.1007/978-3-030-64837-4_17`.
3. W. Beullens, *Breaking Rainbow Takes a Weekend on a Laptop*, Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II, Lecture Notes in Computer Science 13508, Springer, 2022, pp. 464–479, DOI `https://doi.org/10.1007/978-3-031-15979-4_16`.
4. M. Cartor, R. Cartor, H. Furue, and D. Smith-Tone, *Improved Cryptanalysis of HFERP*, Public-Key Cryptography - PKC 2024 - 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15-17, 2024, Proceedings, Part I, Lecture Notes in Computer Science 14601, Springer, 2024, pp. 413–440, DOI `https://doi.org/10.1007/978-3-031-57718-5_14`.
5. Y. Ikematsu, R. A. Perlner, D. Smith-Tone, T. Takagi, and J. Vates, *HFERP - A New Multivariate Encryption Scheme*, Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings,

Lecture Notes in Computer Science 10786, Springer, 2018, pp. 396–416, DOI https://doi.org/10.1007/978-3-319-79063-3_19.

6. C. Tao, A. Petzoldt, and J. Ding, *Efficient Key Recovery for All HFE Signature Variants*, Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I, Lecture Notes in Computer Science 12825, Springer, 2021, pp. 70–93, DOI https://doi.org/10.1007/978-3-030-84242-0_4.

Attack-based encryption using isogenies

Luciano Maino

University of Bristol, UK

Isogeny-based cryptography is one of the most promising branches of post-quantum cryptography. Arguably, the most important isogeny-based cryptosystem is SIDH, which was proposed by De Feo, Jao, and Plût [3]. Despite having ideal features such as efficiency and compactness, this cryptosytem was proven to be completely insecure in [2,8,12].

The attacks in [2,8,12] also introduced a new tool in cryptography: a new way to represent isogenies. Using this tool, we designed a public-key encryption (PKE) mechanism, which we called FESTA, for *Fast Encryption from Supersingular Torsion Attacks* [1]. The core idea is to leverage the SIDH attacks to design a trapdoor function and then apply the OAEP transform to build an IND-CCA secure PKE.

In the trapdoor formulation, the trapdoor key is an isogeny $\varphi_A \colon E_0 \to E_A$, together with a random special matrix $\mathbf{A}$. The public parameters are the codomain E_A and the image of a large torsion basis (P_b, Q_b) under φ_A. Before being revealed, the points $(\varphi_A(P_b), \varphi_A(Q_b))$ are scaled by the matrix $\mathbf{A}$.

The input of the trapdoor function is given by two isogenies $\varphi_1 : E_0 \to E_1$ and $\varphi_2 : E_A \to E_2$, and a random special matrix $\mathbf{B}$. Its output is obtained by computing the images of the torsion basis on E_0 and E_A under φ_1 and φ_2, respectively, and scaling them both with the matrix $\mathbf{B}$; see fig. 1. The matrices $\mathbf{A}$ and $\mathbf{B}$ are special in the sense that they commute; this is the case, for instance, for diagonal matrices.

The commutativity of the matrices is what enables the trapdoor inversion: applying the inverse matrix $\mathbf{A}^{-1}$ to scale the points on E_2 yields the correct images of the torsion points on E_1 under the isogeny $\psi := \varphi_2 \circ \varphi_A \circ \widehat{\varphi}_1$. Hence, we can use the SIDH attacks to recover the input $(\varphi_1, \varphi_2, \mathbf{B})$.

The efficiency of the trapdoor inversion depends on the performance of the SIDH attacks. The main ingredient of such attacks is the computation of isogenies between products of elliptic curves. The parameters in FESTA are chosen in such a way that we only need to compute two-dimensional isogenies between products of elliptic curves. In particular, such isogenies are of a special form, namely chains of $(2, 2)$-isogenies. Efficient algorithms to compute these isogenies have been shown in [4]. The key concept behind these algorithms is the use of the so-called *theta model*.

The performance of FESTA was later improved by Nakagawa and Onuki in [8]. More recently, some of the ideas in [8] were used in [1] to significantly improve SQIsign [5].

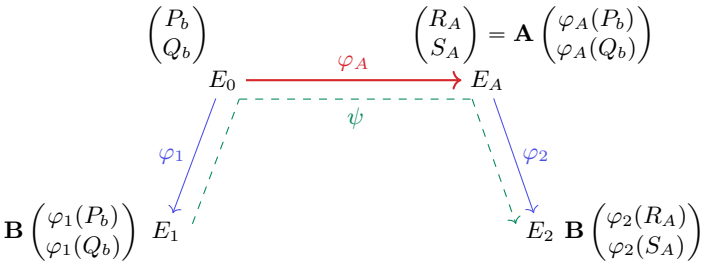


Fig. 1: The FESTA trapdoor function. The parameter generation computes the isogeny ϕ_A, while the trapdoor function evaluation consists of evaluating the isogenies ϕ_1 and ϕ_2. The inversion algorithm recovers the isogeny $\psi = \varphi_2 \circ \varphi_A \circ \widehat{\varphi}_1$.

References

1. A. Basso, P. Dartois, L. de Feo, A. Leroux, L. Maino, G. Pope, , D.Robert, B. Wesolowski, *SQIsign2D-West The Fast, the Small, and the Safer*, Cryptology ePrint Archive, Paper 2024/760, to appear in Asiacrypt 2024, 2024, `https://eprint.iacr.org/2024/760`.
2. A. Basso, L. Maino, G. Pope, *FESTA: Fast Encryption from Supersingular Torsion Attacks*, International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2023, Part VII, Singapore: Springer Nature Singapore, 2023, `https://doi.org/10.1007/978-981-99-8739-9_4`.
3. W. Castryck and T. Decru, *An efficient key recovery attack on SIDH*, Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science 14008, pp. 423–447, Springer, 2023, `https://doi.org/10.1007/978-3-031-30589-4_15`.
4. P. Dartois, L. Maino, G. Pope, and D. Robert, *An Algorithmic Approach to* $(2,2)$*-isogenies in the Theta Model and Applications to Isogeny-based Cryptography*, Cryptology ePrint Archive, Paper 2023/1747, to appear in Asiacrypt 2024 (2023), `https://eprint.iacr.org/2023/1747`.
5. L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, *SQISign: Compact postquantum signatures from quaternions and isogenies*, Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science 12491, pp. 64–93, Springer, 2020, `https://doi.org/10.1007/978-3-030-64837-4_3`.
6. D. Jao and L. De Feo, *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*, Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science, 12491, pp. 64–93. Springer, 2020, `https://doi.org/10.1007/978-3-030-64837-4_3`.
7. L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski, *A Direct Key Recovery Attack on SIDH*, Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science 14008, pp. 448–471, Springer, 2023, `https://doi.org/10.1007/978-3-031-30589-4_16`.

8. K. Nakagawa and H. Onuki, *QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras*, Cryptology ePrint Archive, Report 2023/1468, 2023, https://eprint.iacr.org/2023/1468.
9. D. Robert, *Breaking SIDH in Polynomial Time*, Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science 14008, pp. 472–503, Springer, 2023, https://doi.org/10.1007/978-3-031-30589-4_17.

SQIsign2D-West: The Fast, the Small, and the Safer

Andrea Basso[1,2], Pierrick Dartois[3,4], Luca De Feo[2], Antonin Leroux[5,6], Luciano Maino[1], Giacomo Pope[1,7], Damien Robert[3,4], and Benjamin Wesolowski[8]

[1] University of Bristol, Bristol, United Kingdom
[2] IBM Research Europe, Zürich, Switzerland
[3] Univ. Bordeaux, CNRS, INRIA, IMB, UMR 5251, F-33400 Talence, France
[4] INRIA, IMB, UMR 5251, F-33400, Talence, France
[5] DGA-MI, Bruz, France
[6] IRMAR - UMR 6625, Université de Rennes, France
[7] NCC Group, Cheltenham, United Kingdom
[8] ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France

SQI [5,3] is a signature scheme based on the conjectured hardness of computing endomorphism rings of supersingular curves. A candidate in the NIST post-quantum cryptography standardisation process, it features the smallest combined size of public key and signature, but it also exhibits one the slowest performances among all candidates.

The SIDH attacks [2,8,12] shook the foundations of isogeny-based cryptography by showing that any isogeny can be efficiently recovered from its evaluation on a sufficiently large torsion subgroup. Although they marked the end of SIDH/SIKE [3,6] and related schemes, it was not long before the same technique was put to constructive use, notably in the encryption schemes FESTA [1] and QFESTA [9], and in the SQIsignHD [4] variant of SQIsign. The key to all these applications is to *embed* an isogeny of elliptic curves into an isogeny between *higher-dimensional abelian varieties*. The number of dimensions used for the embedding is a key parameter for efficiency: Robert [11] shows that 8 dimensions are always enough, however the cost of representing the higher-dimensional objects grows *exponentially* with the dimension, thus all practical constructions strive to limit the embedding dimension. For example, FESTA and QFESTA manage to restrict themselves to two-dimensional isogenies.

In the same vein, SQIsignHD consists of two sub-variants. The first, Rigorous-SQIsignHD, uses eight-dimensional isogenies and strives for the best possible provable security but is deemed unpractical. The second, FastSQIsignHD, uses four-dimensional isogenies and compromises on the security proof to achieve the best possible efficiency: the result is a signature scheme with smaller signatures than SQIsign, similarly sized public keys, and significantly faster signing times, but, realistically, *slower verification* owing to the complexity of the four-dimensional representation.

Our contributions. The question of whether it is possible to obtain an improvement over SQIsign by using only two-dimensional isogenies was left open in [4],

Table 1: Parameter sizes and performance of SQIsign2D–West. Average running times computed using an Intel Xeon Gold 6338 (Ice Lake, 2GHz) using finite field arithmetic optimised for the x64 architecture, turbo boost disabled.

	Sizes (bytes)		Timings (ms)		
	Public key	Signature	Keygen	Sign	Verify
NIST I	66	148	30	80	4.5
NIST III	98	222	85	230	14.5
NIST V	130	294	180	470	31.0

where a short paragraph commented on the apparent difficulty of this task. We answer this question in the affirmative by introducing SQIsign2D–West.

To achieve this we introduce new tools for computing higher-dimensional isogeny representations in the context of supersingular elliptic curves:

- An algorithm, a simple extension of [9, Algorithm 2], to evaluate a random elliptic isogeny of given degree by embedding it in a two-dimensional isogeny;
- An algorithm, inspired by [10], to translate a quaternion ideal into a two-dimensional representation of the corresponding elliptic curve isogeny. Combined with an algorithm to sample uniformly random quaternion ideals of given norm, it lets the signer uniformly generate isogenies to be transmitted to the verifier.

We give concrete parametrisations of SQIsign2D–West for NIST security levels I, III and V, and implement them, using both generic and optimised modular arithmetic. With key and signature sizes as reported in table 1, it is comparable to SQIsignHD in terms of bandwidth. Our benchmarks highlight a consistent improvement over SQIsign across the whole spectrum, slightly slower signing performance than FastSQIsignHD but much faster than SQIsign, and *the fastest verification* among all variants of SQIsign. Because prime characteristics in the shape required by SQIsign-2D–West are abundant, our variant, unlike SQIsign, does not need a costly search for a "SQIsign-friendly" prime and thus scales seamlessly to high security levels.

Our security proof shows that the security of SQIsign2D–West reduces to the problem of computing the endomorphism ring of a random supersingular curve, in a security model where the attacker is given (classical) access to an oracle computing (higher-dimensional representations of) uniformly random isogenies from a given curve. Hence, compared to SQIsignHD, SQIsign2D–West manages to blend the efficiency gains of FastSQIsignHD with security guarantees similar to Rigorous-SQIsignHD.

References

1. Basso, A., Maino, L., Pope, G.: FESTA: Fast encryption from supersingular torsion attacks. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part VII. LNCS, vol. 14444, pp. 98–126. Springer, Singapore (Dec 2023). https://doi.org/10.1007/978-981-99-8739-9_4
2. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 423–447. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_15
3. Chavez-Saab, J., Santos, M.C., De Feo, L., Eriksen, J.K., Hess, B., Kohel, D., Leroux, A., Longa, P., Meyer, M., Panny, L., Patranabis, S., Petit, C., Rodríguez Henríquez, F., Schaeffler, S., Wesolowski, B.: SQIsign. Tech. rep., National Institute of Standards and Technology (2023), available at `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`
4. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQIsignHD: New dimensions in cryptography. In: Joye, M., Leander, G. (eds.) EUROCRYPT 2024, Part I. LNCS, vol. 14651, pp. 3–32. Springer, Cham (May 2024). https://doi.org/10.1007/978-3-031-58716-0_1
5. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part I. LNCS, vol. 12491, pp. 64–93. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64837-4_3
6. Jao, D., Azarderakhsh, R., Campagna, M., Costello, C., De Feo, L., Hess, B., Jalali, A., Koziel, B., LaMacchia, B., Longa, P., Naehrig, M., Renes, J., Soukharev, V., Urbanik, D., Pereira, G., Karabina, K., Hutchinson, A.: SIKE. Tech. rep., National Institute of Standards and Technology (2022), available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions`
7. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.Y. (ed.) Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011. pp. 19–34. Springer, Berlin, Heidelberg (Nov / Dec 2011). https://doi.org/10.1007/978-3-642-25405-5_2
8. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 448–471. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_16
9. Nakagawa, K., Onuki, H.: QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras. In: Reyzin, L., Stebila, D. (eds.) CRYPTO 2024, Part V. LNCS, vol. 14924, pp. 75–106. Springer, Cham (Aug 2024). https://doi.org/10.1007/978-3-031-68388-6_4
10. Page, A., Robert, D.: Introducing clapoti(s): Evaluating the isogeny class group action in polynomial time. Cryptology ePrint Archive, Report 2023/1766 (2023), `https://eprint.iacr.org/2023/1766`
11. Robert, D.: Evaluating isogenies in polylogarithmic time. Cryptology ePrint Archive, Report 2022/1068 (2022), `https://eprint.iacr.org/2022/1068`
12. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 472–503. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_17

WORKSHOP
TAC - Topics in Applied Cryptography 2024

Organizers: Riccardo Longo, Alessandro Tomasi, Chiara Spadafora, Silvio Ranise, and Stefano Berlato

KEYNOTE: Transparency, trust and accountability

Filippo Valsorda

Transparency logs (tlogs) are a powerful tool that makes it possible to bring accountability where it is unpractical to improve trust.

A transparency log is an append-only Merkle tree with mechanisms in place to ensure that all parties in an ecosystem have consistent views of the tree. In particular, clients are guaranteed that any entry for which they verify a compact inclusion proof will reach monitors in a timely manner.

A specific instance of a log is abstractly defined by three properties:

- What are the entries?
- Who can add entries to the log?
- Who monitors log entries?

Transparency logs shine when only the log operator can append entries to them, as it allows the operator to become accountable for the contents of the log. This works even for data that's otherwise unauthenticated.

It's useful to think of tlogs as delivering for data the same accountability that open source delivers for software: just like it's possible for a project to produce a release containing a backdoor, it is possible for the log operator to inject illegitimate data, but both actions are discoverable and come at a reputational cost. This makes tlogs especially well-suited to verify data necessary for the operation of open-source client software. In this talk we'll look at examples and discuss the threat models for which tlogs fit best as a solution.

Fundamentally, transparency logs must prevent split-views, where different entities are presented different, inconsistent views of the tree, to hide or tamper with entries. The solutions for this are either after-the-fact gossip, or witness cosigning. Unfortunately, any kind of after-the-fact auditing is ineffective if compromise of the log integrity can lead to compromise of the client system (e.g. if a tlog is used to secure software updates) because the auditing system can be defused as a consequence of system compromise. That makes witness cosigning, where third-party entities provide cosignatures on the Merkle tree heads after verifying they are consistent, the only solution for certain tlog applications. A public witness ecosystem is practically hard to build and foster, as it requires long-term commitments

from trustworthy operators. In this talk we'll discuss our design for lightweight witness implementations, the checkpoint format which already enables interoperability between different tlog and witness implementations, and how a healthy witness ecosystem can make it extremely easy to deploy new log applications.

To ease deployment, it is also convenient to bundle everything needed to verify the inclusion of some data in a transparency log: a cosigned Merkle tree head, an inclusion proof, and a leaf entry. Such an artifact is produced upon submission and is verifiable offline, making it possible to deploy tlog-based solutions anywhere digital signatures are in use. In this talk we'll present this "spicy signature" format, and discuss how it allows bringing accountability to any signature verification.

Tlogs are a concrete implementation of what's commonly called a bullettin board in the literature. Certificate Transparency (CT) pioneered and popularized the use of transparency logs, but also presents a model that is not very reusable due to its peculiar PKI context, and the technology has markedly improved since. In conclusion, we'll look at modern applications of transparency logs, in particular in the context of package ecosystems and key transparency systems. Finally, we'll discuss applications to cryptosystems that require a broadcast channel, such as distributed key generation, and to key recovery mechanisms.

Lova - A Novel Framework for Verifying Mathematical Proofs with Incrementally Verifiable Computation

Noel Elias

University of Texas, USA

Introduction: The efficient verification of proofs and computations has been a long-term foundational problem within Computer Science. Proof systems that efficiently verify computations in different contexts have become key components in many new domains. For example, with machine learning models it is absolutely essential to be able to provide a proof of accurate training and verifiable inferencing [6]. Using such a certificate promotes model transparency as users can verify a model's parameters and features instead of utilizing its predictions through a black box. Additionally, in a Blockchain context, the verification of proofs and computations can also be used to authenticate different transactions while maintaining a decentralized and anonymous network [3].

With the rise of Zero-Knowledge proofs [4], many efficient solutions have been proposed to solve this problem. One of the solutions commonly used are SNARKs (Succinct Non-interactive Argument of Knowledge) [1]. In essence, SNARKs enable a "prover" to succinctly prove a statement to a "verifier" in an efficient manner. More specifically, SNARKs enable untrusted provers to be able to demonstrate knowledge of some witness ω to the verifier. This witness ω could be any statement that can be converted to a computational trace. In addition, SNARKs not only offer succinct proofs but also non-interactive and optionally zero-knowledge proofs.

These SNARKs can even be taken a step further and be utilized for verifying the proofs of proofs. Thus a verification circuit of another inner SNARK can be converted to be a witness ω for an outer SNARK: recursive SNARKs [2]. By utilizing compatible SNARKs, one can significantly increase the efficiency and memory costs of such a proof generation.

So at an initial glace, SNARKs seem to solve the problem of verifying mathematical proofs. However, the problem complexity increases when such proofs become dynamic and are simply repeated executions of the same function over and over

again. This is not ideal and is the motivation for the cryptographic idea of Incrementally Verifiable Computation (IVC) [8].

At a high level, IVC suggests breaking a proof for such a program into its respective iterative sub-steps. To verify each sub-step i we show the following proof π_i: (1) we can verifiably arrive at s_{i-1} starting from the original state s_0 AND (2) $F(s_{i-1}) = s_i$ is computed correctly. Utilizing combinations of these cryptographic checks we can efficiently verify recursive proofs.

Problem: Currently, there is a lack of viable implementations and general methodologies to be able to efficiently and dynamically verify a basic mathematical logic proof. In particular, there are currently no common-place IVC implementations to verify mathematical proofs for individual correctness and sequential order. In addition, most IVC tools do not work for non-linear systems or for verifying proofs with differing non-repeated steps. So, state-of-the-art IVC protocols like Nova [5] are not immediately applicable to verifying mathematical proofs which can be non-linear and contain many different proof steps. Thus, Lova proposes a general framework to solve these problems while dynamically and efficiently verifying logic proofs using the state-of-the-art Nova system for incrementally verifiable computation

Contributions At a high level, Lova introduces a novel method to accomplish this verification of non-linear and non-homogeneous mathematical proofs utilizing the following pipeline. The mathematical proofs are first formatted and sliced into independent sections: each with the statements, logic rules, and previous lines that were utilized. Next, the mathematical proof slices are converted into a system of linear constraints based on a proof circuit. Utilizing a novel multiplexing circuit, each instance calculates the necessary sums for all logic rules before conducting the necessary checks for the current logic step as indicated by a private input signal. Lastly, each of these linear instances is folded utilizing Nova and converted into a "recursive SNARK". To provide further proof compression, this SNARK is then utilized to form another compressed SNARK using the Spartan SNARK proof system [7]. The full code implementation can be found at https://github.com/noelkelias/lova.

To summarize, Lova provides an end-to-end efficient IVC framework as a solution to mathematical proof verification (see Appendix A for Lova's applications). Particularly, Lova expands upon the existing Nova proof system to allow for the efficient verification of mathematical proofs that are non-linear and heterogeneous (non-identical proof steps). More formally, the novelty of the Lova framework can be described as follows:

- A mechanism to splice and encode mathematical proofs into independent, verifiable, and Nova-friendly proof sequences. These proof sequence are self-contained with the necessary public and private inputs.
- An method to create conditional code segments without breaking the linearity of R1CS instances.

- A system of algorithms to verify a variety of linear and non-linear mathematical logic rules.
- A novel multiplexing circuit design which even allows for non-homogeneous (non-identical) proof steps to be efficiently verified together in a single succinct Nova proof.
- The incorporation of Nova recursive SNARKs with existing SNARK technologies resulting in an end-to-end proof generation pipeline.

The attached Lova framework implementation addresses the current lack of IVC implementations utilizing Nova SNARKs and provides solutions for Nova's theoretical shortcomings. Thus, the Lova framework can be used as a stepping stone to understand how to adapt Nova-based IVC techniques for universal succinct proof verification.

References

1. E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, *Snarks for c: Verifying program executions succinctly and in zero knowledge*, Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, Springer, 2013, pp. 90–108.
2. N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, *Recursive composition and bootstrapping for snarks and proof-carrying data*, Proceedings of the forty-fifth annual ACM symposium on Theory of computing, 2013, pp. 111-120.
3. K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li, and Y. Yang, *A secure and verifiable data sharing scheme based on blockchain in vehicular social networks*, IEEE Transactions on Vehicular Technology 69 (6), 2002, pp. 5826–5835.
4. U. Fiege, A. Fiat, and A. Shamir, *Zero knowledge proofs of identity*, Proceedings of the nineteenth annual ACM symposium on Theory of computing, 1987, pp. 210–217.
5. A. Kothapalli, S. Setty, and I. Tzialla, *Nova: Recursive zero-knowledge arguments from folding schemes*, Annual International Cryptology Conference, Springer, 2022, pp. 359–388.
6. S. Lee, H. Ko, J. Kim, and H. Oh, *vcnn: Verifiable convolution neural network based on zk-snarks*, IEEE Transactions on Dependable and Secure Computing, 2024.
7. S. Setty, *Spartan: Efficient and general-purpose zksnarks without trusted setup*, Cryptology ePrint Archive, Paper 2019/550, 2019, `https://eprint.iacr.org/2019/550`.
8. P. Valiant, *Incrementally verifiable computation or proofs of knowledge imply time/space efficiency*, Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, Springer, 2008, pp. 1–18.

Work in progress: HASHTA AI - Share and compute securely your data

Amit Chaudhary

University of Warwick, UK

Abstract. The rise of Artificial Intelligence has once more shown the world that the value of data grows dramatically as they are shared and aggregated. We propose a system based on a public blockchain in which everyone can selectively share their data for trusted and confidential computation, knowing that only the intended recipients will have access. We believe that only such a system can allow for an unplugged growth of AI technology, because it fairly guarantees all actors of an AI ecosystem: data providers, model providers, training providers, model users.

The marginal value of data grows with their aggregation, because only when a computation is performed on a large quantity of data some unexpected interesting correlations can be found. This is even more true with the advent of AI models trained and fine-tuned on large amount of data. AI is changing our world by emulating human actions and decisions by accurate predictions, human-like pattern recognition, and natural language processing. This AI capability has revolutionised human-machine interaction by accelerating the automation of tasks (driverless cars, games - chess [1] and [2], Go [3]), medical discoveries [4] (protein folding: [5] and [12], gene markings), and human-like assistance (chatGPT [14], and other models [10] and [13]).

On the other hand, (lawful) massive data collection requires data owners to actively share their data. Sharing data may lead to loss of confidentiality and/or privacy, which are risks preventing most people from doing it. This is unfortunate because reluctant data owners cannot benefit from the increased value of their data that would come with their sharing.

In a nutshell, people would prefer to share their data, especially for massive computations that can be very profitable. Still, they refrain from doing it because they fear some information leakage and privacy loss. This is dramatically true in the AI scenario, where several types of actors are involved, each with specific tasks and requirements. The main actors are: (training) data providers, model providers and (model) training providers.

De Cifris Koine – CIFRIS24 ACTA –

Data providers are concerned with the integrity and authentication of their data, the usage of their data (data providers might have ethical, communal or other restraints) and their confidentiality.
Similarly, model providers are concerned with the integrity and authentication of their models, as well as their usage. While most models are public, it is also possible that some providers want to keep their models as confidential as possible.
Finally, training providers require integrity, authentication (and confidentiality) of the output of their training. Besides, actors may wish to delegate the heaviest computations to third parties, still retaining all previous security requirements.
We can thus summarize the main problem that we want to address with HASHTA AI and which needs to be solved (in our opinion) to reach unimpeded AI development: to let *everyone selectively share their data for trusted and confidential computation, knowing that only the intended recipients will have access to them.*

1 Addressing the problem

To understand how we plan to address our problem, we describe some other problems and see how their solutions actually bring us, step by step, closer to our goal.
First, let us suppose that a group of friends wants to make their own digital currency, but in such a way that they do not need to trust anyone to keep their balances (or, equivalently, their transaction history). Thus, they need a (digital) location where balances are kept *immutable* (to tampering) and where the currency's users can check them freely. This problem was solved by blockchain technology with the introduction of "public ledgers" [15] and [16]. The main point in public ledgers that is relevant for us and that makes people trust a public ledger is the so-called *economic security* [18], [19] and [20], as follows: *for the rationally-behaving system providers (miners and such), it is more convenient (economically speaking) to follow the protocol rather than to cheat.*
Second, our friends with a public ledger want to use some data on their ledger as input to perform computations, but in a way that the sequence of operations is executed exactly as planned. Indeed, they may upload a precise description of their program (*smart contract*) on the (immutable) ledger to avoid ambiguity. Still, *system providers must be driven via economic incentives to execute it correctly.* This problem was partially solved in Ethereum [22], even if with a substantial computational cost that led quickly to saturation and scalability problems. A more satisfying solution was found with "rollups" e.g. Arbitrum [17], that is, with actors collecting requests sent to the (smart contract) ledger and afterwards sending a merged computation output to the ledger (possibly with proofs of its correctness). Again, *these actors follow the prescribed protocol or incur economic penalties.* Yet, different rollups [21], [25], [23] and [24] (ZK rollups, optimistic and others) provide different levels of assurance, with higher levels being more expensive and less efficient.

Finally, people realised that any kind of data, in principle, could be stored in a way immutable to tampering, not only inputs and outputs of programs. However, such a system must let people retrieve their data at will, as well as provide proof of availability. Once more, solutions have been found (Lazy Ledger [6], Avail [7]) under the generic name of *data availability* (DA), where the providers of DA platforms [7], [8] and [11] *follow the prescribed protocol or lose their economic reward.* Some solutions try also to include delegated computations, such as DFINITY [9].

Having quickly reviewed past solutions, it is clear that any successful solution to our problem (which also includes data privacy) must provide a level of trust to the data owners similar to the level of trust assigned to a public blockchain, a smart-contract platform or a DA system. In other words, the data owners must feel that their data will not be disclosed outside the scope for which they are sharing it. This level of trust is not enough, high as it is, for the AI scenario, where confidential computation must also be guaranteed, because several of its actors cannot afford any data leakage.

Therefore, our solution must be designed so that *if its system providers (who handle the data shared by their owners) disclose and compute data in an agreed-upon way (including confidential computation, when requested), then they are rewarded; otherwise, they are punished (in economic terms).* This provides the level of *technological* trust appropriate to the AI context.

2 Future work

Following a short period of welcome dissemination and discussions, we will describe in an upcoming white paper the technological/economic/cryptographic details of HASHTA and its inner working. We believe the final result will be satisfactory and timely for current challenges, such as massive training/inference of AI models that depends on the selected disclosure of confidential personal data.

References

1. Tomašev, Nenad, Ulrich Paquet, Demis Hassabis, and Vladimir Kramnik. "Assessing Game Balance with AlphaZero: Exploring Alternative Rule Sets in Chess." arXiv preprint arXiv:2009.04374 (2020).
2. Silver, David, et al. "Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm." arXiv preprint arXiv:1712.01815 (2017).
3. Silver, David, et al. "Mastering the game of Go with deep neural networks and tree search." Nature 529, no. 7587 (2016): 484–489.
4. Rajpurkar, Pranav, Emma Chen, Oishi Banerjee, and Eric J. Topol. "AI in health and medicine." Nature Medicine 28, no. 1 (2022): 31–38. doi:10.1038/s41591-021-01614-0.

5. Jumper, John, et al. "Highly accurate protein structure prediction with AlphaFold." Nature 596, no. 7873 (2021): 583–589.
6. Al-Bassam, Mustafa. "LazyLedger: A Distributed Data Availability Ledger With Client-Side Smart Contracts." arXiv preprint arXiv:1905.09274 (2019).
7. Accessed 05-07-2024. https://www.availproject.org/.
8. Accessed 05-07-2024. https://celestia.org/.
9. "DFINITY." https://dfinity.org/.
10. Touvron, Hugo, et al. "LLaMA: Open and Efficient Foundation Language Models." arXiv preprint arXiv:2302.13971 (2023). https://arxiv.org/abs/2302.13971.
11. "EigenDA." eigenda.xyz. https://www.eigenda.xyz/. [Accessed 05-07-2024].
12. Jumper, John, et al. "Highly accurate protein structure prediction with AlphaFold." *Nature* 596.7873 (2021): 583-589.
13. Anil, Rohan, et al. . "PaLM 2 Technical Report." *arXiv preprint* (2023): 2305.10403. https://arxiv.org/abs/2305.10403.
14. Bubeck, Sébastien, et al. "Sparks of Artificial General Intelligence: Early experiments with GPT-4." *arXiv preprint* (2023): 2303.12712. https://arxiv.org/abs/2303.12712.
15. "Bitcoin P2P e-cash paper." *metzdowd.com*. Accessed 05-07-2024. https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.
16. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Cryptography Mailing list at https://metzdowd.com* (2008).
17. Kalodner, Harry, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. "Arbitrum: Scalable, private smart contracts." In *27th USENIX Security Symposium (USENIX Security 18)*, pp. 1353–1370. USENIX Association, 2018. https://www.usenix.org/conference/usenixsecurity18/presentation/kalodner.
18. Leshno, Jacob, Rafael Pass, and Elaine Shi. "Can open decentralized ledgers be economically secure?" *Cryptology ePrint Archive, Paper 2023/1516* (2023). https://eprint.iacr.org/2023/1516.
19. Budish, Eric, Andrew Lewis-Pye, and Tim Roughgarden. "The Economic Limits of Permissionless Consensus.". https://arxiv.org/abs/2405.09173.
20. Deb, Soubhik, Robert Raynor, and Sreeram Kannan. "STAKESURE: Proof of Stake Mechanisms with Strong Cryptoeconomic Safety." *arXiv:2401.05797* (2024). https://arxiv.org/abs/2401.05797.
21. Thibault, Louis Tremblay, Tom Sarry, and Abdelhakim Senhaji Hafid. "Blockchain Scaling Using Rollups: A Comprehensive Survey." *IEEE Access* 10 (2022): 93039-93054. DOI: 10.1109/ACCESS.2022.3200051.
22. *Ethereum Whitepaper | ethereum.org*. Accessed July 4, 2024. https://ethereum.org/en/whitepaper/.
23. StarkWare. *ethSTARK Documentation*. Cryptology ePrint Archive, Paper 2021/582, 2021. https://eprint.iacr.org/2021/582.
24. Ulrich Haböck, David Levit, and Shahar Papini. *Circle STARKs*. Cryptology ePrint Archive, Paper 2024/278, 2024. https://eprint.iacr.org/2024/278.
25. Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. *PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge*. Cryptology ePrint Archive, Paper 2019/953, 2019. https://eprint.iacr.org/2019/953.

Work in progress: Extensible Decentralized Verifiable Refreshable Secret Sharing Protocol with Extension to Threshold Access Trees for Wallet Key Recovery

Sara Montanari

University of Trento and FBK, Italy

Motivations: The safeguarding of private keys is a critical challenge, particularly for the general public, as the loss of these keys can lead to the inaccessibility of valuable assets. Traditional methods of entrusting keys to third-party custodians introduce significant risks and may not be viable for many users, while secret sharing schemes allow trust to be distributed among several providers. In fact, Secret Sharing is used in wallet key management to enhance the security and accessibility of private keys by splitting the key into multiple shares distributed among different participants or providers. No single participant holds the entire key, so access to the wallet requires a minimum number of shares to reconstruct the key. An example of application is presented in [6], where a decentralized wallet model based on Shamir Secret Sharing is explained from an engineering perspective. This approach reduces the risk of key loss or theft, as the key is never fully exposed in one place. It also enables decentralized management, where trust is distributed across multiple entities, ensuring that even if some shares are compromised, the key remains secure.

State of the art: The starting point is a recently proposed cryptographic key recovery scheme, detailed in [1] that leverages distributed secret sharing based on the Shamir Secret Sharing technique. In particular, the protocol is a totally decentralized version of [5], where a subset of participants plays the role of dealer. Moreover, it allows for the addition of new parties after the initial secret sharing and the possibility of having offline participants. Strategies for making a secret sharing protocol extensible are present in the state of the art, but they often require the presence of a dealer and are therefore centralized. The protocol also includes the verifiability property, meaning that the added participant can verify the correctness of the received share, thanks to the use of commitment schemes.

My contribution: In my work, I analyzed the introduction of a refresh phase to the protocol, ensuring *proactive security*, i.e. the maintenance of security thresholds over time. Proactive security is based on the consideration that if the information stored by participants to share a secret remains unchanged throughout the system's

De Cifris Koine – CIFRIS24 ACTA –

lifetime, an adversary could eventually breach enough participants to recover the secret, as explained in [4]. To counteract this risk, proactive security introduces the concept of dividing time into periods known as *epochs*. At the start of each epoch, the shares held by participants are updated, although the shared secret itself remains constant. This approach enhances protection for long-lived secrets, forcing the adversary to start its attack afresh with each new period.

I considered a *snapshot*, *mobile* and *adaptive* adversary. A snapshot adversary captures and analyzes a single point in time or a specific snapshot of the system's state; an adaptive adversary can adapt their strategy based on the information gathered during the protocol's execution, and in particular a mobile adversary can move among players over time but can only control a limited subset of players at any given moment.

The first method for refreshing the shares involves generating and adding a polynomial with a zero constant term to the Shamir polynomial, while the second method involves regenerating the Shamir polynomial while keeping the constant term fixed. These two strategies are shown to be equivalent and proactive-secure against the snapshot, mobile and adaptive adversary model.

The third method involves periodically updating the matrix that encodes the secret; this can be understood by observing the parallelism between MDS codes and secret sharing. This strategy, together with proactive security against the snapshot, mobile and adaptive adversary model, achieves also forward secrecy against an adversary that steals a sufficient number of old shares. However, unlike the first two methods, it is shown to be insecure against a *continuous-shot*, *non-mobile*, *adaptive* adversary.

Finally, I extended the protocol to integrate more complex access structures among parties, such as groups of participants being more powerful than others and collaborative relationships between them. Access structures define the specific sets of participants who are authorized to reconstruct a secret. Any *monotone access structure* can be realized by a linear secret sharing scheme, as shown in [2]. Moreover, the most general structure, encompassing all others, is the *threshold access tree*: participants are represented as leaves in a tree, and each internal node has a threshold that specifies the minimum number of child nodes that must be satisfied to activate that node. For this reason, I focused on extending the Secret Sharing protocol to threshold access trees, exploiting also the theory of *monotone span programs*, as explained in [3].

References

1. M. Battagliola, R. Longo and A. Meneghetti, *Extensible Decentralized Secret Sharing and Application to Schnorr Signatures*, Cryptology ePrint Archive, 2022.
2. A. Beimel, *Secure Schemes for Secret Sharing and Key Distribution*, Israel Institute of Technology, 1996.

3. Z. Liu, Z. Cao, and D. S. Wong, *Efficient Generation of Linear Secret Sharing Scheme Matrices from Threshold Access Trees*, Cryptology ePrint Archive, 2010.
4. V. Nikov and S. Nikova, *On Proactive Secret Sharing Schemes*, Springer Lecture Notes in Computer Science (LNCS), 2004.
5. T. P. Pedersen, *Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing*, Advances in Cryptology — CRYPTO '91, Spriner, 1992.
6. R. Soltani, U. T. Nguyen and A. An, *Decentralized and Privacy-Preserving Key Management Model*, 2020 International Symposium on Networks, Computers and Communications (ISNCC), 2020.

Improving Security and Performance of Cryptographic Access Control with Trusted Execution Environments

Stefano Berlato

FBK, Italy

1 Context and Problem

Cloud-hosted data can be subject to many threats, such as *honest but curious* cloud providers — which may profit from stored data [3] — other cloud tenants (e.g., leveraging isolation issues), misconfigurations of cloud services, and malicious insiders (e.g., physically accessing facilities). Cryptographic Access Control (CAC) addresses these threats by applying cryptography at client-side over sensitive data — guaranteeing end-to-end confidentiality and integrity — while enforcing fine-grained CAC policies through a careful distribution of cryptographic keys to authorized users. However, the revocation of access privileges from users in CAC yields significant performance overhead, as it typically requires renewing all cryptographic keys associated with the revoked privileges and re-encrypting the affected data, possibly resulting in thousands of cryptographic computations [2]. Many researchers employ Trusted Execution Environments (TEEs) for securing access to cloud-hosted data. However, these TEEs usually act as policy decision and enforcement points and do not synergize with CAC. To the best of our knowledge, we are the first to leverage TEEs to hide keys from users in CAC to mitigate the (otherwise unsustainable) performance overhead due to keys renewal and re-encryption resulting from revocations.

2 Design

Our design for integrating TEEs in CAC considers the 4 entities commonly found in CAC [1]: the **proxy** which interfaces users with data by performing cryptographic computations (e.g., en/decryption), the Reference Monitor (**RM**) which mediates users' Access Control (AC) requests to add and write data, the Metadata Manager (**MM**) which securely stores policy-related metadata, and the Data Manager (**DM**), or cloud, which stores encrypted data. The proxy runs on users' devices and it is the only entity accessing cryptographic keys. Thus, to effectively hide keys from users,

De Cifris Koine – CIFRIS24 ACTA –

we deploy the part of the proxy performing cryptographic computations within a TEE — packaged as a trusted application — ensuring secure communication and the integrity of the TEE and the proxy code through remote attestation. Our design consists of 4 phases, as listed below.

Onboarding (*i*): users install the proxy on TEE-equipped devices and generate public/private keys within the TEE. The TEEs create a remote attestation report including the public keys and send it to an attestation authority that, after successful verification, adds the users' public keys to the CAC policy in the MM.

Write (*ii*): the proxy in the TEE encrypts data with a newly generated symmetric key. The encrypted data are sent to the RM and the DM, while the symmetric key is encrypted with the public key of the recipient users fetched from the MM.

Read (*iii*): recipient users decrypt encrypted symmetric keys fetched from the MM with their private keys to decrypt the encrypted data fetched from the DM.

Revocation (*iv*): deleting encrypted symmetric keys from the MM is enough, as they were never directly accessed by users nor cached by the proxy in the TEE — in other words, there is no need for keys renewal or data re-encryption.

3 Open Research Directions

In the context of CAC, there are concerns about potential collusion between malicious users and cloud providers, which could lead to unauthorized access to data. TEEs are used to mitigate this risk by ensuring that cryptographic computations are executed within a secure environment, preventing keys from being exposed. However, even if a client-side TEE (like in our design) can be considered more secure than a TEE used at cloud-side – as it may be subject to tampering from the cloud provider — our design still requires trust in the TEE's manufacturer and the attestation authority, as compromised TEEs or false attestations could introduce vulnerabilities. We also plan to provide a proof-of-concept implementation of our design and evaluate its performance.

References

1. S. Berlato, R. Carbone, A. J. Lee, and S. Ranise, *Formal modelling and automated trade-off analysis of enforcement architectures for cryptographic access control in the cloud*, ACM Transactions on Privacy and Security, 2021.
2. W. C. Garrison, A. Shull, S. Myers, and A. J. Lee, *On the practicality of cryptographically enforcing dynamic access control policies in the cloud*, 2016 IEEE Symposium on Security and Privacy (SP), 2016.
3. E. Ramirez, J. Brill, M. K. Ohlhausen, J. D. Wright, and T. McSweeny, *Data brokers: A call for transparency and accountability*, CreateSpace Independent Publishing Platform, 2014.

Work in progress: On the combination of Searchable Encryption and Attribute-based encryption

Enrico Sorbera
Joint work with Valeria Vicard

FBK, Italy

Our work has been carried out in the context of outsourcing the storage of encrypted data to a cloud, still allowing users to perform searches over the encrypted document collection. Additionally, the set of results obtained from a search must correspond to the documents that are in accordance with the user's query and for which the user has access rights.

This objective is achievable by combining **Searchable Symmetric Encryption** (SSE) [5], which allows for a selective search over the files, with **Attribute-based Encryption** (ABE) [2] [4], for providing fine-grained access control and confidentiality security services.

By studying this problem, we were quick to realize that just a handful of solutions were available in the literature and we focused on the schemes presented by Nils Löken in collaboration with Johannes Blömer, known as SEAC [3] and dSEAC [1]. The protocols described in such papers allow a `Data Owner` (DO) to upload a batch of documents to a cloud, indicating for each element of the batch a (potentially) different set of keywords and an access policy describing it. Consequently, a `Data User` (DU), by specifying a keyword, a list of attributes, and a key for ABE corresponding to those attributes, could present a query to the server, which has to follow a path pre-computed by the DO, to find the documents answering the request. The main features of these protocols are: **verifiability**, which allows users to check that the server indeed abides by its protocols, **fork consistency**, which ensures that any divergence in the view of the data seen by different clients is detectable and traceable. Additionally, she provides **data confidentiality**, thanks to the combination of SE and ABE, and **forward privacy**, meaning that the server is unable to determine that a new document contains any given keyword, even if that keyword has been searched for before.

Nevertheless, there are additional features not deployed in SEAC and dSEAC. First and foremost, we would like to permit more expressiveness in queries, allowing a DU to search for multiple keywords at the same time. For example, by inserting $\{kw_1, kw_2\}$ as a set of keywords in a query, we would like to obtain all documents that contain at least both of them. Additionally, we would like to differentiate the documents according to some parameters that are not considered sensible, and for that reason, that do not need to be protected via any cryptographic measure.

Given the nature of these new parameters, we are going to refer to them as public keywords, in contraposition to the private ones, needed for the search. For clearness, we introduce the notation KW_{pr} to refer to the set of private keywords, whereas the set of public keywords is denoted as KW_{pu}.

Starting from the previous observations, we decided to extend and modify SEAC and dSEAC protocols in two divergent but non-mutually exclusive ways, so that it is up to the organization who deploys the system to select one of them or their combination.
In particular, our first proposal, **"dSEAC with public keys"**, consists of having the server encounter a series of structures, that are intended to act as filters for the search. The first filter contains a node for each of the private keywords, kw_{pr}. Crossing this structure, the server can locate the list of documents labeled by kw_{pr}, without knowing the keyword itself. The second filter is subsequently used by the server to access, among the documents outputted by the first filters, only the ones labeled by the public keywords in the query. Finally, the resulting list of documents is further filtered based on their access policy, so that the user receives only those documents for which she possesses the right attributes.
It is worth noticing that this new schema guarantees all the properties described in dSEAC and just adds a layer of public keywords, that are also the only additional leakage of the protocol.

The second proposal we developed, **"dSEAC allowing search on multiple keywords"**, is intended again as a form of precomputation of all possible paths to solutions that the Cloud Provider could take. But, contrary to SEAC and dSEAC, the first modification we brought was to move the layer enforcing ABE to the head of the structure. The incentive to do so comes from the need to obtain more efficiency: in this way, we could reduce the total amount of ABE encryptions, which is the computationally heaviest cryptographical primitive. Afterward, we focused on the filter containing the private keywords $L \subset KW_{pr}$. Here is where the major work was done, as we desire to have the possibility to look for documents that are described by a set of keywords L' such that $L \subset L'$. This is achievable by designing a structure that responds differently, according to the specific query performed by the user.

This new solution also ensures that it is possible for the Cloud Provider to predict in advance if one or more private keywords were used in the construction of the pseudo-random function.

In conclusion, as we touched on previously, the entire structure is modular and could be adjusted to suit the preferences of the organization that deploys the system. As a matter of fact, we proved how, with small modifications in the content of the filters, it is possible to invert the order of the ABE filter and the private keywords filter. Similarly, it is possible to generate a version of our scheme that uses both a filter for multiple private keywords, as well as a structure to allow searches over a

number of public keywords, enforcing both features, while preserving the leakage profile and the security of the schemes.

This work was partially supported by the project "METAfora: Metodologie e tecnologie di rappresentazione per il metaverso" (CUP code B69J23000190005), funded by the Italian Ministero delle Imprese e del Made in Italy and coordinated by BIT4ID S.r.l.

References

1. J. Blömer and N. Löken, *Dynamic Searchable Encryption with Access Control*, Foundations and Practice of Security: 12th International Symposium, FPS 2019, Toulouse, France, November 5–7, 2019, Revised Selected Papers, Springer-Verlag, 2019, pp. 308–324, DOI `https://doi.org/10.1007/978-3-030-45371-8_19`, ISBN 978-3-030-45370-1.
2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, *Attribute-based encryption for fine-grained access control of encrypted data*, Association for Computing Machinery, 2006, pp. 86–98, DOI `https://doi.org/10.1145/1180405.1180418`.
3. N. Löken, *Searchable Encryption with Access Control*, Proceedings of the 12th International Conference on Availability, Reliability and Security 24 (6), Association for Computing Machinery, 2017, ISBN 9781450352574, DOI `https://doi.org/10.1145/3098954.3098987`.
4. A. Sahai and B. Waters, *Fuzzy Identity-Based Encryption*, Advances in Cryptology – EUROCRYPT 2005, Springer, 2005, pp. 457–473, DOI `http://link.springer.com/10.1007/11426639_27`.
5. D. Song, D. Wagner, and A. Perrig, *Practical techniques for searches on encrypted data*, 2000 IEEE Symposium on Security and Privacy (SP), 2000, pp. 44–55, DOI 10.1109/SECPRI.2000.848445.

WORKSHOP
NTC - Number Theory for Cryptography
2024

Organizers: Federico Accossato, Gessica Alecci, Danilo Bazzanella, Laura Capuano, Giuseppe D'Alconzo, Simone Dutto, Nadir Murru, and Giordano Santilli

Hessians of elliptic curves: isogenies and graphs

Federico Pintore[1]
Joint work with Marzio Mula[2] and Daniele Taufer[3]

[1] University of Trento, Italy
[2] Universität des Bundeswehr München, Germany
[3] KU Leuven

Abstract. The determinant of the Hessian matrix of an elliptic curve E with nonzero j-invariant yields another elliptic curve $\mathrm{Hess}(E)$. We consider the map that sends a j-invariant in a finite field $\mathbb{F}_q$ to the j-invariant of the corresponding Hessian curve. This map defines a dynamical system, i.e. a functional graph which we call Hessian graph, whose structure is remarkably regular. In this talk we will justify the regularities of the graphs, by showing that the Hessian transformation is nothing but a 3-isogeny on a prescribed elliptic curve.

Let $\mathbb{K}$ be a field of characteristic different from 2 and 3. The *Hessian variety* associated with a projective hypersurface $V(F) \subseteq \mathbb{P}^n(\mathbb{K})$ is the zero locus of the determinant $\mathrm{Hess}(F)$ of the Hessian matrix of the homogeneous polynomial $F \in \mathbb{K}[x_1, \ldots, x_n]$. This classical construction enjoys several geometric properties, whose study began with the seminal works by Hesse [5,6] and has continued to the present day [3]. When F is a cubic in the projective plane (i.e. $n = 2$ and $\deg(F) = 3$), then $\mathrm{Hess}(F)$ is, in turn, a cubic homogeneous polynomial. Moreover, if the plane cubic defined by F is also smooth (i.e. elliptic), its Hessian has proven to be a crucial tool for investigating its arithmetic properties [8,7].

It is a natural question to ask, for a given elliptic curve E, what is the relation between E and $\mathrm{Hess}(E)$, and, more generally, $\mathrm{Hess}^{(\ell)}(E)$ where ℓ is a positive integer. This question motivates the study of the dynamical system defined by the Hessian transformation: by representing the isomorphism class of E by its j-invariant $j \in \mathbb{P}^1(\mathbb{K})$, one can view Hess as a rational function on $\mathbb{P}^1(\mathbb{K})$. We will simply refer to the corresponding functional graph as the *Hessian graph*. The study of this graph has already been undertaken by several authors in the case $\mathbb{K} = \mathbb{C}$ or $\mathbb{K} = \mathbb{R}$ [1,2] and it falls within a much broader field of research regarding the dynamics of rational functions. To date, the structure and symmetries of the Hessian graphs have not yet been fully investigated.

In a joint work with Marzio Mula and Daniele Taufer, we develop a new approach for studying the Hessian of elliptic curves, and we employ it to establish several novel

properties of such transformation. More in details, for a given $k \in \mathbb{K}^*$, we consider the elliptic curve E_k defined by

$$E_k \ : \ y^2 = x^3 + \frac{k}{4}.$$

We show that the Hessian transformation ascends to a degree-3 endomorphism ψ_k of E_k, whose kernel is $\{\infty, \pm(0, \sqrt{k}/2)\}$. This implies that, over arbitrary fields, not only does the Hessian graph enjoy properties shared by group automorphisms [4], but it also inherits distinctive features from the arithmetic of the curve E_k. Moreover, the results actually apply to a larger family of rational maps, namely those defined for $k \in \mathbb{K}^*$ by

$$\Lambda_k \ : \ \mathbb{P}^1(\mathbb{K}) \to \mathbb{P}^1(\mathbb{K}), \quad [u : v] \to [u^3 + kv^3 : -3u^2v],$$

of which the Hessian transformation constitutes a relevant instance. In fact, the map Λ_{108} is precisely the map describing the Hessian transformation of the Hesse pencil $X^3 + Y^3 + Z^3 + \lambda XYZ$ [1]. Concretely, given the canonical first projection π, we prove that one can compute Λ_k via the commuting diagram

$$\begin{array}{ccc} E_k & \xrightarrow{\psi_k} & E_k \\ {\scriptstyle \pi^{-1}}\uparrow & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1(\mathbb{K}) & \xrightarrow{\Lambda_k} & \mathbb{P}^1(\mathbb{K}). \end{array}$$

In addition, the double application of ψ_k is proved to be the scalar multiplication by -3 on the curve E_k, which provides an efficient way of computing the iterated Hessian:

$$\Lambda_k^{(2m)}(\lambda) = \pi\big((-3)^m \pi^{-1}(\lambda)\big).$$

Furthermore, we prove that the same model, but specialised for $k = -6912$, can also be used to lift the Hessian action at the level of j-invariants of the considered elliptic curves. More generally, it can be used to study the whole family of dynamical systems defined, for $k \in \mathbb{K}^*$, by

$$\mathbb{P}^1(\mathbb{K}) \to \mathbb{P}^1(\mathbb{K}), \quad [u : v] \mapsto [(u + kv)^3 : -27uv^2].$$

In fact, we prove that the latter rational map can also be read from the action of ψ_k, although a cubing operation is needed.

Furthermore, we exhibit a concrete use case of this model by leveraging the dynamics of ψ_k to describe Hessian graphs over finite fields $\mathbb{F}_q$. We prove that the functional graph of ψ_k on the points of $E_k(\mathbb{F}_{q^2})$ is extremely regular, as every periodic element is the root of isomorphic complete ternary trees. In particular, when $q \equiv 2 \pmod 3$, the cubing operation is invertible so this regularity is fully inherited

by the Hessian graph, whose global structure is therefore determined. If $q \equiv 1 \pmod 3$, the functional graph over the model curve still exhibits strong regularity properties, but reading the corresponding Hessian graph from its structure is more challenging. As a consequence, the regularity in the latter case is weaker.

References

1. M. Artebani and I. V. Dolgachev, *The Hesse pencil of plane cubic curves*, L'Enseignement Mathématique 55 (3), 2009, pp. 235-273.
2. F. Catanese and E. Sernesi, *Geometric Endomorphisms of the Hesse moduli space of elliptic curves*, 2024, ArXiv: 2309.00113.
3. C. Ciliberto, G. Ottaviani, J. Caro, and J. Duque-Rosero, *The general ternary form can be recovered by its Hessian*, 2024, ArXiv: 2406.05382, https://arxiv.org/abs/2406.05382.
4. B. E. de Klerk and J.H. Meyer, *Functional graphs of abelian group endomorphisms*, Journal of Discrete Mathematics 345 (2), 2022, ISSN 0012-365X, DOI 10.1016/j.disc.2021.112691, https://www.sciencedirect.com/science/article/pii/S0012365X21004040.
5. O. Hesse, *Über die Bedingung, unter welcher eine homogene ganze Function von n unabhängigen Variabein durch lineäre Substitutionen von n andern unabhängigen Variabein auf eine homogene Function sich zurückführen läßt, die eine Variable weniger enthält*, Journal fur die Reine und Angewandte Mathematik 1851 (42), 1851, pp. 117–124, DOI 10.1515/crll.1851.42.117, https://www.scopus.com/inward/record.uri?eid=2-s2.0-80052794541&doi=10.151.
6. O. Hesse, *Zur Theorie der ganzen homogenen Functionen*, Journal fur die Reine und Angewandte Mathematik 1859 (56), 1859, pp. 263–269, DOI 10.1515/crll.1859.56.263, https://www.scopus.com/inward/record.uri?eid=2-s2.0-80052794320&doi=10.1515.
7. M. Sala and D. Taufer, *Elliptic Loops*, Journal of Pure and Applied Algebra 227 (12), 2023, ISSN 1873-1376, DOI 10.1016/j.jpaa.2023.107417, https://doi.org/10.1016/j.jpaa.2023.107417.
8. M. Stanojkovski and C. Voll, *Hessian Matrices, Automorphisms of p-Groups, and Torsion Points of Elliptic Curves*, Mathematische Annalen 381 (1), 2021, pp. 593–629, ISSN 1432-1807, DOI 10.1007/s00208-021-02193-8, https://doi.org/10.1007/s00208-021-02193-8.

Proving knowledge of an isogeny using modular polynomials

Marzio Mula.
Joint work with T. den Hollander, S. Kleine, D. Slamanig, and S. A. Spindler.

Universität des Bundeswehr München, Germany

Abstract. Given a small prime l and a prime p of cryptographic size, a cyclic isogeny of degree l^r between two supersingular j-invariants $j, j' \in \mathbb{F}_{p^2}$ can be represented as a sequence of j-invariants $j = j_0, j_1, ..., j_r = j'$ such that each pair (j_i, j_{i+1}) is a root of the lt-h classical modular polynomial $\Phi_l(X, Y)$. For $l = 2$, previous work by Cong, Lai, and Levin shows how this representation can be effectively expressed — by means of a suitable arithmetization — in the setting of generic proof systems (such as zk-SNARKs) to prove the knowledge of a 2-smooth cyclic isogeny in a non-interactive way. In this talk, we discuss some possible optimizations of their method, using an alternative family of modular polynomials — called canonical modular polynomials — and leveraging some additional techniques to improve the arithmetization. Finally, we explore the scalability of the resulting proof system for different small primes.

1 Context

More than twenty years have passed since the seminal works by Couveignes [1], Rostovstev, and Stolbunov [2] have introduced the idea of using maps between elliptic curves, called *isogenies*, for cryptographic purposes. Although their original attempts seemed too inefficient to compare with concurrent cryptosystems, later efforts in this direction [3,4] gave birth to a rich, and still lively, branch of cryptography. A strong reason for researchers to push into in this field is that the main problem on which it is based – namely, recovering a secret isogeny between two given elliptic curves – is considered hard even for quantum computers. Moreover, compared with other proposals for post-quantum cryptography, isogenies enjoy shorter parameters which though come at the price of slower performance.

In this work we are particularly interested in (non-interactive) zero-knowledge proofs of knowledge of secret isogenies. They are a central tool for many cryptographic applications in which some party needs to prove that it is behaving honestly and/or its public key is well-formed. To do so, a possible approach analyzed by Cong,

Lai and Levin in [5] is to prove the isogeny relation by means of a general-purpose (non-interactive) zero-knowledge proof system, such as a zk-SNARK. The idea is to consider the (classical) ℓ^{th} modular polynomial $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$, for which the following property holds: two curves E and E' are ℓ-isogenous if and only if their j-invariants satisfy $\Phi_\ell(j(E), j(E')) = 0$. Consequently, when aiming to prove a walk in the ℓ-isogeny graph from some starting curve E to some curve E', one can efficiently represent it as a sequence of successive steps, i.e. a sequence of j-invariants $j_1, j_2, \ldots, j_{k-1}$ such that

$$\begin{aligned} \Phi_\ell(j(E), j_1) &= 0, \\ \Phi_\ell(j_i, j_{i+1}) &= 0 \quad \text{for all } i \in [k-2], \\ \Phi_\ell(j_{k-1}, j(E')) &= 0, \end{aligned}$$

where we write $[m] \coloneqq \{1, 2, \ldots, m\}$ for $m \in \mathbb{Z}$.

Cong, Lai and Levin then use this relation for the specific case $\ell = 2$ to construct a rank-1 constraint system (R1CS), which is a very popular arithemtization method in state-of-the-art zk-SNARKs. Then they plug this into a number of existing plausibly post-quantum proof systems such as Aurora [6], Ligero [7], and Limbo [8].

2 Our contribution

The results in [5] show that the efficiency of this general-purpose approach when compared with the recent tailor-made approach in [9] achieves an order of magnitude improvement over proof and verification times, with slightly worse but still comparable proof sizes. Moreover, compared to existing tailor-made solutions, this approach provides a stronger notion of soundness.

In our work we ask whether this can be optimized when targeting R1CS and whether the approach can be generalized to prove the knowledge of isogenies of degree ℓ^k for primes $\ell > 2$.

We answer these questions affirmatively for $\ell \in \{2, 3, 5, 7, 13\}$ by switching from classical modular polynomials, as considered by Cong, Lai and Levin, to canonical modular polynomials, which are sparser and enjoy smaller coefficients. We also apply further techniques to improve the arithmetization. Along the way, we advance the understanding of canonical modular polynomials by exploring their connection with the classical ones. Our main mathematical result is the following.

Theorem 1. *Let $\ell \in \{2, 3, 5, 7, 13\}$, let K be a field of characteristic $char(K) \neq \ell$ and let $j_0, j_1 \in K$. Then there are exactly as many non-equivalent ℓ-isogenies $j_0 \to j_1$ as there are roots $f \in \overline{K}^\times$ of the canonical polynomial $\Phi^c_\ell(X, j_0)$ (counted*

with multiplicity) that also satisfy $\Phi_\ell^c(\ell^s/f, j_1) = 0$. *In particular,* j_0 *and* j_1 *are* ℓ*-isogenous if and only if the system*

$$\begin{cases} \Phi_\ell^c(X, j_0) = 0, \\ \Phi_\ell^c(\ell^s/X, j_1) = 0 \end{cases}$$

has a solution $f \in \overline{K}^\times$.

The above result is the key ingredient of our work, as it allows us to rephrase the isogeny relation in terms of canonical modular polynomials:

$$\mathcal{R}_{\ell^k-\text{ModRoot}} = \Bigg\{ \left((E, E'), (j_i)_{i\in[k-1]}, (f_i)_{i\in[k]}\right) \mid \Phi_\ell^c(f_1, j(E)) = 0 \wedge \Phi_\ell^c(\ell^s/f_k, j(E')) = 0 \bigwedge_{i\in[k-1]} \Phi_\ell(f_{i+1}, j_i) = 0 \bigwedge_{i\in[k-1]} \Phi_\ell^c(\ell^s/f_i, j_i) = 0 \Bigg\}.$$

3 Conclusions

By replacing classical modular polynomials with the canonical ones and applying some further tricks in the arithmetization, we show that we can improve over Cong, Lai and Levin by 25% for isogenies over $\mathbb{F}_{p^2}$ and obtain a 36% improvement over $\mathbb{F}_p \times \mathbb{F}_p$, with an optimized arithmetization to support any proof system, for the constraints and the variable count. For the number of non-zero entries in the constraint matrices, the improvement is close to 50%. For larger $\ell \in \{3, 5, 7, 13\}$, a case not covered by Cong, Lai and Levin, our techniques (when reducing the k for degree ℓ^k according to a fixed security parameter 2^λ and comparing to $\ell = 2$) lead to even better improvements.

References

1. Jean-Marc Couveignes. Hard homogeneous spaces. *Cryptology ePrint Archive, Report 2006/291*, 2006. `https://eprint.iacr.org/2006/291`.
2. Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *Cryptology ePrint Archive, Report 2006/145*, 2006. `https://eprint.iacr.org/2006/145`.
3. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 19–34, Tapei, Taiwan, November 29 – December 2 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-25405-5_2.

4. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-03332-3_15.
5. Kelong Cong, Yi-Fu Lai, and Shai Levin. Efficient isogeny proofs using generic techniques. In Mehdi Tibouchi and Xiaofeng Wang, editors, *ACNS 23: 21st International Conference on Applied Cryptography and Network Security, Part II*, volume 13906 of *Lecture Notes in Computer Science*, pages 248–275, Kyoto, Japan, June 19–22, 2023. Springer, Heidelberg, Germany. doi:10.1007/978-3-031-33491-7_10.
6. Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nicholas Spooner, Madars Virza, and Nicholas P. Ward. Aurora: Transparent succinct arguments for R1CS. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 103–128, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-17653-2_4.
7. Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight sublinear arguments without a trusted setup. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017: 24th Conference on Computer and Communications Security*, pages 2087–2104, Dallas, TX, USA, October 31 – November 2, 2017. ACM Press. doi:10.1145/3133956.3134104.
8. Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, and Titouan Tanguy. Limbo: Efficient zero-knowledge MPCitH-based arguments. In Giovanni Vigna and Elaine Shi, editors, *ACM CCS 2021: 28th Conference on Computer and Communications Security*, pages 3022–3036, Virtual Event, Republic of Korea, November 15–19, 2021. ACM Press. doi:10.1145/3460120.3484595.
9. Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part II*, volume 14005 of *Lecture Notes in Computer Science*, pages 405–437, Lyon, France, April 23–27, 2023. Springer, Heidelberg, Germany. doi:10.1007/978-3-031-30617-4_14.

Lattices and Cryptography, an Overview

Stefano Barbero

DISMA Politecnico di Torino, Italy
stefano.barbero@polito.it

Abstract. Lattices play an important role in several branches of Mathematics, such as Algebra and Number Theory, becoming also very relevant in Cryptography in the last two decades. The aim of this talk is to explore how and why they acquired this importance, giving a concise but comprehensive overview. Starting from basic definitions and properties, we focus on some of the most important problems involving lattices. We consider these problems, their hardness and what algorithms we know to tackle them. Finally, we take a sharp look at the applications of lattices in Cryptography, especially in the Post Quantum scenario.

A concise, but comprehensive, overview on lattices and their relevance in Cryptography should start from the role they play in several branches of Mathematics, such as Algebra and Number Theory. An emblematic example is the sphere packing problem and its relation with codes [4], [11]. But lattices not only are an interesting way to tackle some algebraic or number theoretic questions, they also introduce some interesting and hard problems. Considering n-dimensional lattices, two well-known important problems, are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). We have some tools to deal with them: the Gaussian heuristic for the length of the shortest vector, the Lenstra–Lenstra–Lovász (LLL) algorithm for basis reduction [8],[9], and the Babai closest vertex algorithm [3]. In particular, the LLL algorithm is a fundamental tool in cryptanalyzing many schemes which admit a certain lattice modelling, e. g., it is the pillar of the Coppersmith method [5], used in attacks on RSA when parts of the secret key are known. Although the LLL algorithm could output an almost reduced lattice basis in polynomial time, the hardness of several lattice problems has been pointed out. First, the 1996 seminal work of Aijtai [1] showed that SVP is NP–hard under randomized reductions. He also introduced a family of one–way functions based on the Short Integer Solution (SIS) problem, giving actually rise to lattice cryptography. Then several other results, such as the NP-hardness of CVP, highlighted that some lattice problems are average–case hard [10] and very likely secure also against quantum computers. These facts led to an increasing use of lattices in the design of cryptographic schemes and digital signatures. The related history dates back to 1996, not only for the work of

Aijtai, but also for NTRU, developed in 1996 [7], [8], and improved over time and often combined with some other lattice–related problems such as Learning With Errors (LWE). Nowadays, we can consider the lattice based first group of winners of the NIST competition [12]. Crystal, in its versions Kyber and Dilithium [2], relies on hard problems over module lattices, i. e., lattices that "lies" between the ones used in the definitions of the LWE problem and those used for the Ring-LWE problem. Falcon [6] is a digital signature scheme that works over NTRU lattices and it is based on the hardness of SIS.

References

1. M. Ajtai, *Generating hard instances of lattice problems.* STOC'96: Proceedings of the Twenty–Eighth annual ACM symposium on Theory of computing. Philadelphia, Pennsylvania, United States: ACM. 99–108 (1996). doi:10.1145/237814.237838
2. R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, *Crystals: Cryptographic Suite for Algebraic Lattices* online at https://pq-crystals.org/index.shtml
3. L. Babai, *On Lovász lattice reduction and the nearest lattice point problem.* Combinatorica, 6(1):1–13, 1986.
4. J. H. Conway and N. J. A. Sloane, *Lattices and Groups* Grundlehren der Mathematischen Wissenschaften, vol. 290 (3rd ed.), Springer–Verlag Berlin, New York, 1999.
5. D. Coppersmith, *Finding a Small Root of a Univariate Modular Equation* Advances in Cryptology – EUROCRYPT '96. Lecture Notes in Computer Science. Vol. 1070. pp. 155–165, 1996. doi:10.1007/3-540-68339-9_14.ISBN978-3-540-61186-8
6. P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, *Falcon: Fast–Fourier Lattice–based Compact Signatures over NTRU* online at https://falcon-sign.info/
7. J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A Ring Based Public Key Cryptosystem* Algorithmic Number Theory (ANTS III) L NCS 1423 267–288 Springer-Verlag, Berlin, 1998.
8. J. Hoffstein, J. Pipher, and J.H. Silverman, *An Introduction to Mathematical Cryptography.* Springer New York, 2008.
9. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients.* Math. Ann., 261(4):515–534, 1982.
10. D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems.* The Kluwer International Series in Engineering and Computer Science, 671. Kluwer Academic Publishers, Boston, MA, 2002.
11. G. Nebe and N. J. A. Sloane, *A Catalogue of Lattices* online at https://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/
12. NIST Selected Algorithms 2022 online at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

A Note on the P-values Distribution in NIST SP 800-22 Rev. 1a Statistical Tests

Guglielmo Morgari[1]
Joint work with Vittorio Bagini[2], Danilo Bazzanella[3], and Alessandro Giacchetto

[1] Telsy SPA, Italy
[2] Fondazione Ugo Bordoni, Italy
[3] Politecnico di Torino, Italy
guglielmo.morgari@telsy.it

Cryptography is vital in securing sensitive information and maintaining privacy in today's digital world. Though sometimes underestimated, randomness plays a key role in cryptography, generating keys and other unpredictable material. Hence, high-quality random number generators are a crucial element in building a secure cryptographic system, making it essential to construct robust validation systems to verify their quality. This task is typically done by means of hypothesis tests (see [4]), which, given a random sequence, allow to assess the plausibility of a *null hypothesis* on the random data generation process. The null hypothesis is typically that the generated sequences are made of uniformly distributed and statistically independent bits.

In practice, a real value (*test statistic*) is calculated for the sequence being analyzed, according to the test definition. A *p-value* is then determined, representing the probability of observing a test statistic as extreme as, or more extreme than, the one observed, assuming the null hypothesis is true. The obtained p-value is then compared with a predefined value α (known as the *significance level*) to decide whether to accept or reject the null hypothesis. The significance level α thus represents the probability of a Type I error, which occurs when the null hypothesis is actually true but the test rejects it. Common values for α are 0.01 and 0.05.

Since p-values can in turn be seen as random variables, determined by the probability distribution associated with the null hypothesis, in our work we consider their distribution. In the context of random number generators, this distribution is inherently discrete but in the literature it is commonly approximated by continuous distributions for ease of handling.

However, we have shown that the mentioned approximation can lead to subtle errors, specifically due to the difference between the continuous and discrete cases. While in the continuous case, if the null hypothesis is true, p-values are uniformly distributed, this property does not hold in the discrete case, where at best one can achieve the *discrete uniformity* property. Some papers (see for example [2,8]) mention this point but do not explore its implications.

On the contrary, extending our previous work [5,3], we have first theoretically demonstrated that, for a generic test, it is extremely unlikely that the associated p-values satisfy the property of discrete uniformity. Then we have experimentally analyzed the collection of hypothesis tests proposed by NIST in the well-known *SP800-22 Rev. 1a* document [1], which (though recently subject to criticism, e.g., [7]) is the *de facto* standard tool to evaluate the quality of random number generators, observing that in some tests the obtained p-values distribution is quite far from being uniform.

This fact is relevant since, in its document [1], NIST relies exactly on the uniform distribution of p-values as a criterion to assess the validity of the null hypothesis. More precisely, given a collection of sequences produced by the generator under analysis, one of the criteria proposed by NIST consists in dividing the probability range (0,1] in K=10 equal sub-intervals, then computing the p-value for each sequence, counting the number of p-values falling in each sub-interval and finally determining if they can be deemed uniformly distributed, through the application of the well-known χ^2 test to the frequencies observed for the sub-intervals. The described procedure constitutes a hypothesis test itself, where the null hypothesis is the uniform distribution of the p-values computed from the individual sequences. Our simulations have shown that the rejection ratio of χ^2 values produced according to the NIST procedure under the null hypothesis (using a CSPRNG to generate strong random-looking sequences) is in line with expectations.

However, the choice to divide the probability range into K=10 sub-intervals is arbitrary. For investigative purposes, we have slightly modified the NIST procedure, by considering K=100 sub-intervals, which, assuming the p-value distribution is uniform, appears to be an equally valid choice. Moving to the modified version we have observed that the rejection ratio is much higher than expected for the tests whose p-value distribution is further from uniformity. We believe that this observation can be explained by the wrong assumption of discrete uniformity of p-values used by NIST in building the procedure. Moreover, it may also contribute to justify why NIST decided to set K as low as 10, thus minimizing the effects of the discretization, and to set the significance level of the procedure to $\alpha = 0.0001$. This value for α is surprisingly low (as also noted in [6]) and is clearly inconsistent with the more common $\alpha = 0.01$ used throughout the entire document [1] for different, but related, criteria. In fact, such a low α significantly increases the success rate for collections of sequences produced under the null hypothesis, whereas our simulations have shown that using a more standard value for α would cause an unacceptably high rejection ratio in the modified procedure. Finally we emphasize that the choice of NIST to lower the Type-I error probability (α) in the above mentioned procedure leads to a higher Type-II error probability, which is undesirable in cryptography as it increases the risk of incorrectly accepting a flawed generator.

References

1. L. E. Bassham III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, and others, *Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications*, National Institute of Standards & Technology, 2010, https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final.
2. C. Blocker, J. Conway, L. Demortier, J. Heinrich, T. Junk, L. Lyons, and G. Punzi, *Simple Facts about P -Values*, 2006, https://hep-physics.rockefeller.edu/~luc/technical_reports/cdf8023_facts_about_p_values.pdf.
3. A. Giacchetto, *Generatori di numeri aleatori: relazioni tra test di casualità*, Politecnico di Torino, 2022, https://webthesis.biblio.polito.it/24866/1/tesi.pdf.
4. E. L. Lehmann, J. P. Romano, and G. Casella, *Testing statistical hypotheses* 3, Springer, 1986.
5. G. Morgari, *Randomness Tests for Binary Sequenes*, Politecnico di Torino, 2023, https://iris.polito.it/retrieve/9539c0eb-79e8-40c7-bf2c-bc27d54b2c07/GuglielmoMorgari_PhD_Thesis.pdf.
6. K. Marton and A. Suciu, *On the interpretation of results from the NIST statistical test suite*, Journal of Science and Technology 18 (1), 2015, pp. 18–32, https://www.romjist.ro/content/pdf/02-msys.pdf.
7. Multiple authors, *Public Comments on the Decision Proposal for SP 800-22 Rev. 1a*, 2022, https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/sp800-22r1a-decision-proposal-comments-2022.pdf.
8. A. L. Rukhin, *Statistical testing of randomness: New and old procedures*, Randomness through computation: Some answers, more questions/Ed. by H. Zenil, 2011, pp. 33–51.

WORKSHOP
CPSID - Cryptography, Protocols and Security in Digital Identity 2024

Organizers: Andrea D'Intino and Denis "Jaromil" Roio

Overview of the current digital identity standards

Andrea D'Intino

Dyne Foundation, Netherlands

Abstract. In this talk we provide an overview of the ongoing digital identity efforts, focusing on the cryptography but including context about the political standpoints as well as the institutional and industry actors involved, int the EU and USA/Canada. We will provide a comparative analysis of the main cryptographic scheme used, along with communication protocols and the data formats for both digital identities and verifiable credentials.

De Cifris Koine – CIFRIS24 ACTA –

Current status of the implementation of the Italian Wallet and Trust Framework Infrastructure

Francesco Marino

Poligrafico e Zecca dello Stato, Italy

Abstract.

De Cifris Koine – CIFRIS24 ACTA –

Challenges and upcoming standards

Simone Onofri[1] and Denis Roio[2]

[1] W3.org, USA
[2] Dyne Foundation, Netherlands

Abstract. In our talks we will discuss the most actively discussed challenges of the existing digital identity standards, with extra focus on privacy. We will focus on the non-unlinkability issue of EUDI-ARF, on the revocation and on possible mitigations that are being discussed and experimented with.

WORKSHOP
SymCrypt - Symmetric Cryptography and Boolean Functions 2024

Organizers: Marco Calderini, George Petrides, and Irene Villa

Stream ciphers encoded by difference equations over finite fields and their cryptanalysis

Roberto La Scala

University of Bari, Italy

Abstract. Many stream ciphers of practical interest, such as Trivium and Bluetooth's E_0, can be modeled as systems of explicit ordinary difference equations with coefficients and solutions in a finite field. These systems govern the evolution of the internal registers of these so-called "difference ciphers" over discrete time. By leveraging the formalism of difference equations, it is possible to define critical properties of stream ciphers, such as invertibility and periodicity, which are essential for assessing their security. This modeling, coupled with the corresponding cryptanalysis, actively supports the development of new ciphers.

Many stream ciphers of real practical interest, such as Trivium and Bluetooth's E0, can be modeled as systems of difference equations with coefficients and solutions in a finite field. Alongside this system of equations, one also needs a polynomial that enables the calculation of the keystream elements from the cipher register. This register can indeed be considered the state whose evolution is governed by the system of explicit ordinary difference equations. Such a system ensures that each state is uniquely determined by the initial state, which effectively serves as the cipher's key. We will refer to this class of stream ciphers as "difference ciphers".

Using the formalism of difference equations, it is possible to define some relevant properties of stream ciphers, in particular their invertibility and periodicity. These properties are introduced in terms of fundamental functions associated with the difference system, such as the "state transition endomorphism" and its corresponding "state transition map". Additionally, it is possible to precisely define an algebraic attack on the cipher based on the knowledge of a certain number of keystream elements. The property of a cipher being invertible also allows for the optimization of such an attack, which can drastically reduce the security of the cryptosystem. Indeed, assuming invertibility, it is sufficient to calculate any internal state, such as the one from which the keystream begins, to know the initial state that contains the key. To determine if a difference cipher is invertible, one can use the calculation of a Gröbner basis of an ideal associated with the state transition endomorphism. From this computation, one also obtains the inverse difference system that allows the clock progression within the cipher to be reversed.

Another critical property for the security of such stream ciphers is the non-linearity of the difference equations and/or the keystream polynomial. Indeed, it is well known that a system of LFSRs, which corresponds to the fully linear case, can be attacked in polynomial time. In the presence of non-linear equations in the system, however, an algebraic attack corresponds to solving a system of non-linear polynomial equations over a finite field, the resolution of which is generally an NP-complete problem. Using the notion of difference cipher, we can analyze the various systems of polynomial equations corresponding to different types of algebraic attacks and understand why they are complex to solve.

Finally, to illustrate these concepts and the corresponding cryptanalytic techniques, we consider the stream ciphers Trivium and E0. These ciphers have been the subject of recent attacks in [1,2,3].

References

1. La Scala, Roberto; Pintore, Federico; Tiwari, Sharwan K.; Visconti, Andrea. A multistep strategy for polynomial system solving over finite fields and a new algebraic attack on the stream cipher Trivium, Finite Fields Appl. 98 (2024), Paper No. 102452, 1–33.
2. La Scala, Roberto; Polese, Sergio; Tiwari, Sharwan K.; Visconti, Andrea. An algebraic attack to the Bluetooth stream cipher E0, Finite Fields Appl. 84 (2022), Paper No. 102102, 1–29.
3. La Scala, Roberto; Tiwari, Sharwan K. Stream/block ciphers, difference equations and algebraic attacks, J. Symbolic Comput. 109 (2022), 177–198.

On the computation of the Walsh-Hadamard Transform using Binomial Trees

Luca Mariot

University of Twente, Netherlands

Abstract. The Walsh-Hadamard Transform is a fundamental tool to characterize several cryptographic properties of Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ known that this transform can be efficiently computed in $O(n2^n)$ steps by using the Fast Walsh Transform (FWT) algorithm, while the naive implementation requires $O(2^{2n})$ steps.

In this talk, we investigate a new approach to compute the Walsh- Hadamard transform. The main data structure underlying this method is a binomial tree, where the path back to the root of each node represents a Walsh-Hadamard coeffcient, and inductively defines the related scalar product. We show that the Walsh-Hadamard transform is obtained by visiting such a binomial tree, and consider both a depth-first and a breadth-first search strategy to perform this task. Although the resulting algorithms yield the same $O(2^{2n})$ time complexity of the naive Walsh-Hadamard transform, we experimentally observe that they are faster in practice. We then show how to adapt the BFS-based algorithm to check a Boolean function's correlation immunity order by requiring only its support as an input. Interestingly, this modified algorithm gives an effcient way to check whether a binary matrix of a large number of columns is an orthogonal array. Such a task cannot be practically accomplished with the Fast Walsh-Hadamard Transform procedure, due to the amount of memory required to hold the truth table of the associated Boolean function.

(Cryptographic) Functions for Designing Locally Recoverable Codes in Distributed Storage

Sihem Mesnager

University of Paris VIII, France

Abstract. There is a crucial need for highly scalable and reliable extensive data storage systems due to the rapid growth in data. Distributed storage systems (DSSs) store data on multiple distributed nodes and are widely used in file system storage, ample database storage, backup files, cloud storage, and more. The repair problem in DSSs is a key focus area. Lately, there has been a notable increase in interest and focus on Locally Recoverable Codes (LRCs), highlighting their growing importance in distributed storage systems. In this talk, we will explore function-based codes and present mathematical techniques for creating (optimal) LRC codes from functions and polynomials. Notably, we emphasize the significant role of specific cryptographic functions in the design of LRCs.

In coding theory, Boolean functions, fundamental primitives in symmetric cryptography ([1]), or more generally, p-ary functions have been used to construct linear codes. Historically, the Reed-Muller and Kerdock codes have long been the two famous classes of binary codes derived from Boolean functions. Next, much progress has been made in this direction, and further codes have been derived from more general and complex functions. Nevertheless, despite the advances in the past two decades, one can isolate essentially two generic constructions of linear codes from functions only (see *e.g.* [6], Chapter 18). This talk focuses on *locally repairable codes* (LRCs). In recent years, interest in and attention paid to LRCs have proliferated in the context of storage. LRC codes have recently been a fascinating subject in research in coding theory due to their theoretical appeal and applications in large-scale distributed storage systems, where a single storage node erasure is considered a frequent error event. Indeed, there is a need for highly scalable and reliable extensive data storage systems because of explosive data growth. Distributed storage systems (DSSs) store data on several distributed nodes and are widely used in file system storage, ample database storage, backup files, cloud storage, etc. The repair problem in DSSs addresses the recovery of the data encoded using erasure codes such as Reed-Solomon codes, *locally repairable codes* (LRCs).

Specifically, we recall that a code $\mathcal{C} \subseteq \mathbb{F}_{q^n}$ is called *locally recoverable (LRC)* code if every coordinate of the codeword $c = (c_1, \ldots, c_n) \in \mathcal{C}$ can be recovered from

a subset of r other coordinates of c. Such a LRC code is said to have *locality* r. Mathematically, it gives the following mathematical definition.

Definition 1. *Code $\mathcal{C}$ has locality r if for every $i \in [1, \cdots, n]$ there exists a subset $R_i \subset [1, \cdots, n] \backslash \{i\}$, $|R_i| \leqslant r$ and a function ϕ_i such that for every codeword $c \in \mathcal{C}$:*

$$c_i = \phi_i(\{c_j, j \in R_i\}).$$

An (n, k, r) LRC code $\mathcal{C}$ over $\mathbb{F}_q$ is of code length n, cardinality q^k, and locality r. The parameters of an (n, k, r) LRC code have been studied.

Theorem 1. *[8,9] Let $\mathcal{C}$ be an (n, k, r) LRC code of cardinality q^k over an alphabet of size q, then the minimum distance of $\mathcal{C}$ satisfies*

$$d \leqslant n - k - \lceil k/r \rceil + 2.$$

The rate of $\mathcal{C}$ satisfies

$$\frac{k}{n} \leqslant \frac{r}{r+1}.$$

Note that if $r = k$, the upper bound given in the above theorem coincides with the well-known Singleton bound ($d \leqslant n - k + 1$). Given the above upper bound on the minimal distance, optimal (resp. almost optimal) LRC codes have been defined as follows.

Definition 2 (Optimal-Almost optimal LRC codes). *LRC codes for which $d = n - k - \lceil k/r \rceil + 2$ are called optimal codes. We refer to almost optimal codes when the minimum distance differs by, at most, one from the optimal value.*

In the first part of this talk, we discuss the concept of r-good polynomials as the key ingredient for constructing optimal linear LRC codes.

Definition 3 (Good polynomials). *Specifically, a polynomial F over $\mathbb{F}_{p^s}$ is said to be an* r-good polynomial *if and only if*

1. *the degree of F is $r + 1$,*
2. *there exist pairwise disjoint subsets $\{A_1, \ldots, A_l\}$ of $\mathbb{F}_{p^s}$ with cardinality $\#A_i = r+1$ for $i = 1, \ldots, l$, such that the restriction of F to each subset A_i is constant.*

We next present methods to generate good polynomials from function (in the line of [4]), key ingredients, leading to the design of optimal LRC codes based on the technique of Tamo and Barg ([10]). In the second part, after recalling, namely, the construction methods of binary linear codes from Boolean functions (see. e.g. [3]), we discuss (cryptographic) functions-based LRC codes in line with the recent results of Z. Heng et al. ([11]). If time permits, we will discuss binary LRCs with multiple repair alternatives in the last part of this talk. Specifically, an LRC is

said to have *locality* r if the value at any coordinate can be recovered by accessing at most r other coordinates and to have *availability* t if every coordinate can be retrieved from t disjoint repair sets of other coordinates. We investigate binay LRCs with locality 2 and multiple repair alternatives from specific wide families of Boolean cryptographic functions ([5]) specifically from (bent) Boolean functions through the Maiorana-McFarland constructions (see. e.g. [2])

References

1. C. Carlet. Boolean Functions for Cryptography and Coding Theory. Cambridge University Press 2020, ISBN 9781108606806 (2021)
2. C. Carlet and S. Mesnager.: Four decades of research on bent functions. Des. Codes Cryptogr., vol. 78, pp. 5-50, 2016.
3. C. Ding.: A construction of binary linear codes from Boolean functions. Discrete Mathematics, 339(9), pp. 2288–2303, 2016.
4. J. Liu, S. Mesnager and L. Chen.: New Constructions of optimal locally recoverable codes via good polynomials, IEEE Transactions on Information Theory, Vol. 62, No. 2, pp. 889–899 2018.
5. J. Liu, S. Mesnager and D. Tang.: Constructions of optimal locally recoverable codes via Dickson polynomials. Preprint 2019.
6. S. Mesnager.: Linear codes from functions. A Concise Encyclopedia of Coding Theory. CRC Press/Taylor and Francis Group (Publisher) London, New York, 2021 (Chapter 20, 94 pages).
7. S. Mesnager.: Bent functions: fundamentals and results. Springer, Switzerland, 2016. ISBN 978-3-319-32593-4, pp. 1-544 (2016)
8. P. Gopalan, C. Huang , H. Simitci, and S. Yekhanin.: On the locality of codeword symbols. IEEE Transactions on Information theory, 58(11), 6925–6934,2012.
9. D. S. Papailiopoulos and A. G. Dimakis.: Locally repairable codes, IEEE Transactions on Information Theory, vol. 60, no. 10, pp. 5843–5855, 2014.
10. I. Tamo and A. Barg.: A family of optimal locally recoverable codes, IEEE Transactions on Information Theory, vol. 60, no. 8, pp. 4661–4676, 2014.
11. Z. Heng, X. Li, Y. Wu, Q. Wang.: Two families of linear codes with desirable properties from some functions over finite fields.
https://doi.org/10.48550/arXiv.2401.0113 (2024).

WORKSHOP
CodeMath - Coding Theory and Discrete Mathematics 2024

Organizers: Massimo Giulietti, Giuseppe Marino, Olga Polverino, and Ferdinando Zullo

Hadamard products of codes: an Additive Combinatorics perspective

Gilles Zémor

Institut de Mathématiques de Bordeaux, France

For two linear codes C, D in $\mathbb{F}_q^n$, we are interested in their Hadamard product $C * D = CD$ (also called Schur product, or star product, hereafter simply product). The product $\mathbf{x} * \mathbf{y} = \mathbf{xy}$ of two vectors $\mathbf{x} = [x_1, \ldots, x_n]$ and $\mathbf{y} = [y_1, \ldots, y_n]$ is defined as $\mathbf{xy} = [x_1 y_1, \ldots, x_n y_n]$ and the product CD of codes C and D is defined as the linear span of the set of products $\mathbf{cd}$ of codewords $\mathbf{c} \in C$ with $\mathbf{d} \in D$.

Since the product CD is generated by the products $\mathbf{cd}$ where $\mathbf{c}$ and $\mathbf{d}$ span a basis of C and a basis of D respectively, we have $\dim CD \leqslant \dim C \dim D$, and we may expect a typical product CD to either be equal to the whole space $\mathbb{F}_q^n$ or to have dimension close to $\dim C \dim D$, which is indeed what happens [1]. However, there are codes with a dimension much smaller than the typical case. One striking example is that of Reed-Solomon codes for which we have, when CD is not equal to the whole space, $\dim CD = \dim C + \dim D - 1$. It is therefore somewhat natural to ask what can we say about pairs of codes whose products have small dimension, all the more so since a number of applications have been found for such pairs of codes. The first such application is probably due to Pellikaan [5] and concerns the decoding problem. Suppose we are given a vector $\mathbf{y}$ which is a corrupted codeword of some code C. The idea is to identify the positions in error by looking for a codeword $\boldsymbol{\ell}$ of some auxiliary code L (the *locator code*) whose coordinates are 0 in all positions for which $\mathbf{y}$ is in error. Such a vector $\boldsymbol{\ell}$ will have the property that $\mathbf{y}\boldsymbol{\ell} \in C * L$: therefore, we can try to find such a vector $\boldsymbol{\ell}$ by solving the linear system $\mathbf{y}\boldsymbol{\ell} \in C * L$. However, for this strategy to work, we need the code $C * L$ to be non-trivial, so we need a pair (C, L) of codes with a product of unusually small dimension. For a range of applications of pairs of codes with small dimension see [6].

Some sort of characterisation of pairs C, D of codes for which $\dim C \dim D = \dim C + \dim D - 1$ was found in [4] for MDS codes. It states:

Theorem 1. *Let C, D be MDS linear codes in $\mathbb{F}_q^n$ with $\dim C \geqslant 2$, $\dim D \geqslant 2$ and $\dim CD \leqslant n - 2$. Suppose $\dim CD = \dim C + \dim D - 1$. Then C and D are Reed-Solomon codes with a common evaluation-point sequence.*

It is not clear to us what becomes of this theorem when the MDS hypothesis is weakened. However, it already serves to highlight some connections with phenomena that occur in the field of additive combinatorics. Indeed, notice that from the point of

view of code products, a (generalised) Reed-Solomon code of dimension k can simply be defined as a code that has a basis in geometric progression $\beta, \beta\alpha, \beta\alpha^2, \ldots, \beta\alpha^{k-1}$. Notice the similarity between Theorem 1 and the classical theorem of Vosper from additive combinatorics (see e.g. [7]).

Theorem 2. *Let A, B be subsets of a cyclic group of prime order $(\mathbb{Z}/p\mathbb{Z}, +)$ such that $|A| \geqslant 2$, $|B| \geqslant 2$, $|A+B| = \#\{a+b, a \in A, b \in B\} \leqslant p-2$. If $|A+B| = |A| + |B| - 1$, then A and B are arithmetic progressions with the same difference.*

Can one do better than Reed-Solomon codes, i.e. can we have pairs of codes C, D for which the product CD is a non-trivial code such that $\dim CD < \dim C + \dim D - 1$? The answer is 'not really': if $\dim CD < \dim C + \dim D - 1$ then the code CD must be degenerate in the sense that it must be a direct sum of two codes that have disjoint supports. Equivalently it must have a block-diagonal generator matrix. Indeed, the following theorem is proved in [4]:

Theorem 3. *Let C, D be linear codes in $\mathbb{F}_q^n$. Then*

$$\dim CD \geqslant \dim C + \dim D - \dim \mathrm{St}(CD).$$

Here $\mathrm{St}(CD)$ is the *stabiliser* of CD which is defined as the set of vectors $\mathbf{x}$ such that $\mathbf{x}(CD) \subset CD$. The stabiliser is always generated by a set of vectors whose coordinates are in $\{0, 1\}$ and that have disjoints supports. This implies that CD is indeed a disjoint direct sum. There is a striking parallel between this result and Kneser's Theorem [3] in Abelian groups.

Theorem 4. *Let A, B be subsets of an Abelian group G. We have:*

$$|A+B| \geqslant |A| + |B| - |\mathrm{St}(A+B)|$$

where $\mathrm{St}(A+B) = \{g \in G,\ g + (A+B) = A+B\}$.

We have also a connection to the theory of products of spaces in function fields. Indeed, a large class of algebraic codes are evaluation codes, i.e. they are constructed by evaluating in $\mathbb{F}_q$ a subspace of functions in some function field at a fixed number of places. If the product of two such spaces sits inside a subspace of small dimension in the function field, then the corresponding evaluation codes will have products of small dimension. We are therefore interested in characterising subspaces of function fields whose products have small dimension. A recent result in this direction is given in [2].

References

1. Ignacio Cascudo, Ronald Cramer, Diego Mirandola and Gilles Zémor. Squares of Random Linear Codes. *IEEE Trans. Inform. Theory*, 61(3):1159–1173, 2015.

2. Alain Couvreur and Gilles Zémor. Freiman's $3k-4$ Theorem for function fields. Preprint available at `https://arxiv.org/abs/2408.00183`
3. Martin Kneser. Summenmengen in lokalkompakten abelesche Gruppen. *Math. Z.*, 66:88–110, 1956.
4. Diego Mirandola and Gilles Zémor. Critical pairs for the product Singleton bound. *IEEE Trans. Inform. Theory*, 61(9):4928–4937, 2015.
5. Ruud Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.,* 106-–107:369–381, 1992.
6. Hugues Randriambololona. On products and powers of linear codes under componentwise multiplication. In *Algorithmic Arithmetic, Geometry and Coding Theory*, volume 637 of *Contemp. Math.* Amer. Math. Soc., 2015.
7. Terence Tao and Van H. Vu. *Additive combinatorics*, volume 105 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 2006.

Recent results on scattered spaces and MRD codes

Daniele Bartoli

University of Perugia, Italy

Linear sets have numerous applications in various areas of mathematics, including finite geometry and coding theory. In particular, scattered linear sets are of special interest due to their unique properties and the role they play in these fields. One of the most effective methods to describe and analyze these scattered linear sets is through the use of linearized polynomials that are particularly useful because they allow us to leverage techniques from both algebraic geometry and group theory. By employing these techniques, one can gain deeper insights into the properties of scattered linear sets and their applications. In this talk, I will present recent advances in the study of exceptional scattered polynomials and their generalizations (scattered sequences). Furthermore, I will explore the connection between these concepts and maximum rank distance (MRD) codes.

References

1. D. Bartoli, A. Cossidente, G. Marino, F. Pavese, *On cutting blocking sets and their codes*, Forum Mathematicum **34**(2), 347–368 (2022).
2. D. Bartoli, G. Zini, F. Zullo, *Linear maximum rank distance codes of exceptional type*, IEEE Transactions on Information Theory **69**(6), 3627–3636 (2023).
3. D. Bartoli, G. Marino, A. Neri, *New MRD codes from linear cutting blocking sets*, Annali di Matematica Pura e Applicata **202**, 115–142 (2023).
4. D. Bartoli, M. Giulietti, G. Zini, *The classification of exceptional scattered polynomials of odd degree*, submitted.
5. D. Bartoli, G. Marino, A. Neri, L. Vicino, *Exceptional scattered sequences*, submitted.
6. D. Bartoli, M. Borello, G. Marino, *Saturating linear sets of minimal rank*, submitted.
7. D. Bartoli, G. Longobardi, G. Marino, M. Timpanella, *Scattered trinomials of* $\mathbb{F}_{q^6}[X]$ *in even characteristic*, submitted.

Cryptographic uses of (polar) Grassmannians

Luca Giuzzi[1]
Joint work with Ilaria Cardinali

University of Brescia, Italy

Abstract. Embeddings of (polar) Grassmannians determine error correcting codes with high length and nice minimum distance. In this talk we shall propose the use of punctured Grassmann codes in a McEliece-like cryptosystem. The security of the scheme is based on hiding from potential attackers the point-line structure of the geometry of the Grassmannian, as this structure is essential in order to provide efficient decoding algorithms.

De Cifris Koine – CIFRIS24 ACTA –

CROSS: a signature scheme with restricted errors

Violetta Weger

Technical University of Munich, Germany

Last year, the National Institute of Standards and Technology (NIST) has reopened the standardization call for post-quantum cryptography, targeting solely signature schemes[1]. This additional call has greatly shifted the focus of the cryptographic community to finding new and efficient post-quantum signature schemes. One of the main strategies to construct code-based signatures is via the Fiat-Shamir transform [5] on a Zero-Knowledge (ZK) protocol. Although this strategy has been deemed impractical for many years due to the large signature sizes, with the significant attention over the last years, many solutions have evolved to decrease the sizes. In fact, this approach is now perceived as one of the most promising solutions. This is visible within the round 1 submissions to the additional call, where 15 of the 40 candidates are based on such a paradigm. One of the most prominent solutions to reduce the sizes is by changing the ZK protocol and employing Multi-Party Computations [6]. However, this comes at the cost of a slower scheme.

CROSS [1] is using a different solution: instead of changing the ZK protocol, we change the underlying problem. In this talk I introduce restricted errors and the Restricted Syndrome Decoding Problem (RSDP) [3] used in CROSS. Instead of imposing a target weight on the error vector, the RSDP searches for a vector with entries in a restricted set. The new problem is highly related to the classical Syndrome Decoding Problem. In fact, it is still an NP-hard problem and many decoders can be translated to the new setting [4]. We will explore the mathematical properties of restricted errors and their linear transitive maps, which play a crucial role in code-based ZK protocols. In fact, we can show that they achieve the theoretical minimum in communication costs [2]. Finally, we compare the performance of CROSS with the other code-based schemes in the first round.

References

1. M. Baldi, A. Barenghi, S. Bitzer, P. Karl, F. Manganiello, A. Pavoni, G. Pelosi, P. Santini, J. Schupp, F. Slaughter, A. Wachter-Zeh, and V. Weger, *CROSS*, First Round Submission to the additional NIST Postquantum Cryptography Call, 2023.

De Cifris Koine – CIFRIS24 ACTA –

[1] See, e.g., the official NIST call `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf`

2. M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, and V. Weger, *Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem*, PKC 2024.
3. M. Baldi, M. Battaglioni, F. Chiaraluce, A. L. Horlemann-Trautmann, E. Persichetti, P. Santini, and V. Weger, *A new path to code-based signatures via identification schemes with restricted errors*, arXiv preprint, 2020, arXiv: 2008.06403.
4. S. Bitzer, A. Pavoni, V. Weger, P. Santini, M. Baldi, and A. Wachter-Zeh, *Generic Decoding of Restricted Errors*, 2023 IEEE International Symposium on Information Theory (ISIT), 2023, pp. 246–251.
5. A. Fiat and A. Shamir, *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, Crypto 86, Springer, 1986, pp. 186–194.
6. Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, *Zero-knowledge from secure multiparty computation*, Proceedings of the thirty-ninth annual ACM symposium on Theory of computing, 2007, pp. 21–30.

WORKSHOP
QCifris - Quantum Cifris 2024

Organizers: Paolo Villoresi, Marco Genovese, Fabio Sciarrino, Cristian Antonelli, Giuseppe Vallone

Introduction to Quantum Technologies for secure information from an Italian perspectives Abstract

Paolo Villoresi

University of Padova, Italy

Abstract. Italy has been active in the development of quantum communications protocols for more than two decades, with groups of researchers perfecting different techniques and fields of application. Quantum communication protocols are also complemented by research and development at a very advanced level in the areas of quantum meteorology, experimental components development and the establishment of a nationwide infrastructure to enable communication on a large scale. In addition, our Country is also active in the research and development of quantum computing. This includes both a part of theoretical study of algorithms and is an experimental part for its implementation, in different platforms. Given the crucial significance of quantum computing in cyberattacks, this area is also of strategic importance in the field of cryptography.

De Cifris Koine – CIFRIS24 ACTA –

Entanglement for quantum key distribution

Fabio Sciarrino

University of Roma La Sapienza, Italy

Abstract. Italy has been active in the development of quantum communications protocols for more than two decades, with groups of researchers perfecting different techniques and fields of application. Quantum communication protocols are also complemented by research and development at a very advanced level in the areas of quantum meteorology, experimental components development and the establishment of a nationwide infrastructure to enable communication on a large scale. In addition, our Country is also active in the research and development of quantum computing. This includes both a part of theoretical study of algorithms and is an experimental part for its implementation, in different platforms. Given the crucial significance of quantum computing in cyberattacks, this area is also of strategic importance in the field of cryptography.

Quantum Computing in Cybersecurity

Simone Montangero

University of Padova, Italy

Abstract.

De Cifris Koine – CIFRIS24 ACTA –

Genuine random numbers from quantum processes for cybersecurity

Giuseppe Vallone

University of Padova, Italy

Within the last two decades, Quantum Technologies have made tremendous progress, from proof of principle demonstrations to real life applications. In particular, two paradigmatic examples of Quantum Technologies that are extremely relevant for security application are Quantum Random Number Generators (QRNGs) and Quantum Key Distribution (QKD). The generation of random numbers is of fundamental importance for applications related to security. Indeed, all cryptographic protocols are based on the availability of private random numbers and any predictability on their generation can weaken the protocol. Unlike algorithm-based generators (the so called Pseudo-Random Generators), QRNGs are based on the intrinsic randomness of quantum measurements.

Here, we first briefly review the basic principles of QRNGs. We then discuss the results that we have recently obtained in our group at the University of Padova and the perspectives of quantum technologies for cybersecurity.

In particular, we recently developed new theoretical and experimental methods for the realization of ultra-fast and secure QRNGs based on the "Semi-Device-Independent" approach [12,5,6,1,7,2,10,11,9,3,8,4]. The latter allows to certify the randomness of the generated numbers without the complete calibration of the used devices but exploiting some reasonable physical assumptions on them that require simple and reliable device characterization.

By exploiting the uncertainty principle and the source-device-independent framework, it is possible to bound the content of quantum randomness in a given setup. This technique, proposed in [12] for discrete variables, was extended to continuous variables in [5,1,7] and recently implemented in integrated photonics [4]. The method has been extended to Positive Operator Valued Measurement (POVM), which can arbitrarily increase the number of certified bits for any fixed dimension [3].

On the other hands, we will present several QRNG that exploits a semi-device-independent scenario in which the measurement and source are uncharacterized,

but a bound on the energy of the prepared states is assumed [2,10,11].

Finally, we recently proposed a new protocols in the full Device-Independent scenario that exploits sequential quantum correlations for efficient device-independent QRNG [8].
We believe that the above results represent an important step towards mature and efficient QRNG systems for cybersecurity.

Acknowledgements

The results here presented were obtained thanks to the work of all members of the QuantumFuture research group: `https://quantumfuture.dei.unipd.it/people`.

References

1. M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, *Source-device-independent heterodynebased quantum random number generator at 17 Gbps*, Nature Communications Sta, 5365, 2018.
2. M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, *Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator*, Physical Review Applied 15, 034034, 2021.
3. M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, *Unbounded randomness from uncharacterized sources*, Communications Physics 5, 2022.
4. T. Bertapelle, M. Avesani, A. Santamato, A. Montanaro, M. Chiesa, D. Rotta, M. Artiglia, V. Sorianello, F. Testa, G. D. Angelis, G. Contestabile, G. Vallone, M. Romagnoli, and P. Villoresi, *High-speed source-device-independent quantum random number generator on a chip*, 2024, arXiv: 2305.12472.
5. D. G. Marangon, G. Vallone, and P. Villoresi, *Source-Device-Independent Ultrafast Quantum Random Number Generation*, Physical Review Letters 118, 060503, 2017.
6. D. G. Marangon, G. Vallone, U. Zanforlin, and P. Villoresi, *Enhanced security for multi-detector quantum random number generators*, Quantum Science and Technology 1, 015005, 2016.
7. T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, *Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States*, Physical Review Applied 12, 034017, 2019.
8. M. Padovan, G. Foletto, L. Coccia, M. Avesani, P. Villoresi, and G. Vallone, *Geometry of sequential quantum correlations and robust randomness certification*, 2023, arXiv: 2309.12286.
9. A. Stanco, D. G. Marangon, G. Vallone, S. Burri, E. Charbon, and P. Villoresi, *Certification of the efficient random number generation technique based on single-photon detector arrays and time-to-digital converters*, IET Quantum Communication 2, 2021, pp. 74–79.

10. H. Tebyanian, M. Avesani, G. Vallone, and P. Villoresi, *Semi-device-independent randomness from d-outcome continuous-variable detection*, Physical Review A 104, 2021.
11. H. Tebyanian, M. Zahidy, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, *Semi-device independent randomness generation based on quantum state's indistinguishability*, Quantum Science and Technology 6, 045026, 2021.
12. G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, *Quantum randomness certified by the uncertainty principle*, Physical Review A 90, 052327, 2014.

National and European Quantum Communications for Enhanced Security: Technology and Applications

Alessandro Zavatta[1] and Simone Capeleto[2]

[1] CNR-INO, Italy
[2] ThinkQuantum SRL, Italy

Quantum key distribution (QKD) is a mature technology that establishes symmetric encryption keys between two remote parties in an unconditionally secure way. It has been successfully implemented in various real-world scenarios, including cross-border networks, underwater links, and Metropolitan Area Networks. Here, we present the latest results from our real-world implementations of QKD, demonstrating its adaptability and effectiveness in different environments.

WORKSHOP
CifrisCloud - Cryptography for the Cloud
2024

Organizers: Michela Iezzi, Matteo Nardelli, and Marco Pedicini.

ANTI-fraud: ABE Solutions

Martina Palmucci

NTT Data, Italy

1 Background

In today's financial environment, online transactions usually require users to provide a username and password. However, behind the scenes, additional factors are analysed to assess the security of the transaction. A simple username and password combination is no longer enough to guarantee a user's identity and authorize certain operations. Financial institutions must consider a wider range of factors when determining whether to approve specific transactions.
For dispositive operations, Risk-Based Authentication (RBA) [4,7,8] is employed to evaluate the user profile and assess the risk level of the transaction based on several criteria. This evaluation is critical in deciding whether to grant or deny authorization.
RBA analyses various factors, including:

- time of day
- location
- device and browser information
- IP address
- user behaviour patterns
- context of the transaction

Each transaction is assigned a risk level based on these factors, contributing to an overall risk score. Depending on the perceived risk, users may be asked to perform Multi-Factor Authentication (MFA) or other security measures [6]. For instance, RBA may identify a high-risk level when an online banking customer requests a large financial transfer to an external account. Even if factors such as the IP address and user behaviour align with expectations, such a sensitive transaction would trigger additional MFA methods.
A medium or high-risk level may be assigned when a transaction is initiated from a non-certified device, such as a personal computer. Since the financial institution cannot trust this device, the user will need to verify the transaction using a certified smartphone, typically through a One-Time Password (OTP) [5] sent via SMS, a virtual OTP or biometric authentication such as fingerprint or facial recognition.

De Cifris Koine – CIFRIS24 ACTA –

Additional authentication may be required depending on the specific risk level.
Traditionally, banks have managed these risks by implementing hard-coded RBA policies within their web services, limiting flexibility and scalability. Additionally, these policies often categorize a broad and diverse user base into only a few predefined profiles. This approach can lead to inaccuracies, increasing the likelihood of false positives or false negatives when assessing risk levels.
In the search for innovative solutions within this context, it's essential to consider that the banking sector, particularly under the EU's Payment Services Directive 2 (PSD2), includes a security requirement known as Strong Customer Authentication (SCA) [2]. A key component of SCA is Dynamic Linking, which mandates the use of an authentication code unique to each transaction. This code must accompany the payment amount and recipient details throughout the payment and authentication process. Moreover, the payer must clearly view both the amount and recipient information during the authentication step. If the authentication code or any payment details are altered at any stage, the transaction must be invalidated.

2 Research question

Given the current landscape of online banking, where hard-coded policies in bank web services limit flexibility, scalability, and the ability to accommodate diverse user behaviours, we investigated whether a RBA system could be made more adaptable and customizable. Additionally, compliance requirements, such as SCA and Dynamic Linking under the EU's PSD2 directive, highlight the need for dynamic, transaction-specific security measures.
Our aim is to enhance fraud prevention by developing a security system that can not only respond to evolving user behaviour and risk factors but also comply with regulatory demands. This system should offer greater flexibility and scalability, while ensuring that security remains robust and seamlessly integrated into the authorization process.

3 Our contribution

In response to the limitations of traditional hard-coded RBA policies and the regulatory requirements, particularly under PSD2, we propose an innovative solution that integrates Key-Policy Attribute-Based Encryption (KP-ABE) [3] into RBA systems.
KP-ABE is an encryption paradigm that enables data protection by embedding access control policies directly into cryptographic keys. This method allows data access to be controlled at the cryptographic level, reducing reliance on application-level logic.
Our Proof of Concept (PoC) explores an approach that integrates KP-ABE with

a challenge-response mechanism to cryptographically enforce action authorization [1]. By merging this dual approach into RBA systems, it is possible to shift policy enforcement from hard-coded rules within bank-side web services to a cryptographic key securely stored on the user's certified device. This key can be issued, updated, and revoked independently of the application itself, enhancing both flexibility and scalability.
Since KP-ABE supports expressive policy structures, these policies can encapsulate complex conditions. The policies embedded in the cryptographic key represent a formal characterization of the results of behavioural analysis. Operations that align with the user's normal behaviour are authorized, while anomalous transactions would trigger further controls, such as MFA or, in extreme cases, a phone call from an operator. This results in more precise control over transaction authorization, reducing the likelihood of false positives and false negatives.
Moreover, user behaviour evolves over time but typically exhibits a certain level of inertia. Therefore, periodic updates of the cryptographic key, along with corresponding updates to the policy based on the user's behavioural patterns, can ensure that the system remains accurate and secure without requiring constant real-time updates of the policy embedded in the user's key.
An essential aspect of integrating KP-ABE with the challenge-response mechanism is its ability to meet PSD2's Dynamic Linking requirements. Our solution ensures that each challenge-response interaction is unique to the transaction by including transaction details and a randomly generated code. This approach satisfies the PSD2 requirement for a unique authentication code tied to each transaction's specific details, such as the payment amount and recipient, ensuring both security and compliance.

4 Conclusion

In this work, we explored the integration of KP-ABE into RBA systems to enhance flexibility, scalability, and accuracy while maintaining security and regulatory compliance in banking operations. By shifting policy enforcement from hard-coded application-server logic to user cryptographic keys, KP-ABE allows for more flexible and scalable control over transaction authorization. The KP-ABE cryptographic approach strengthens fraud prevention by supporting expressive policies that reduce the likelihood of false positives and false negatives.

Our PoC demonstrates the feasibility of combining KP-ABE with challenge-response mechanisms, ensuring compliance with regulations like PSD2, particularly in meeting the Dynamic Linking requirement for unique authentication codes tied to each transaction.
As a potential future evolution, a behavioural analysis system could be developed to automatically generate policies in the Attribute-Based Encryption formalism.

This would allow the system to dynamically adapt policies based on ongoing user behaviour, further enhancing flexibility and precision in transaction authorization. Such an approach would allow for a more responsive and adaptive fraud prevention mechanism, keeping pace with evolving user behaviours and threat landscapes.

References

1. G. Bartolomeo, *Attribute-based encryption for access control in cloud ecosystems*, TechRxiv Preprints, 2021), https://www.techrxiv.org/users/678993/articles/676279-attribute-based-encryption-for-access-control-in-cloud-ecosystems, accessed: 2023-09-06.
2. European Banking Authority: Regulatory activities: Payment services and electronic money (nd), https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/payment-services-and-electronic-money-0, accessed: 2024-09-06.
3. V. Goyal, O. Pandey, A. Sahai, and B. Waters, *Attribute-based encryption for fine-grained access control of encrypted data*, IACR Cryptology ePrint Archive 2006, 309, 2006, https://eprint.iacr.org/2006/309.pdf, accessed: 2024-09-06.
4. T. Kato, *Risk-based authentication patent*, 2015, https://patents.google.com/patent/US9021555B2/en, issued March 29, 2006.
5. K. G. Paterson and D. Stebila, *One-time-password-authenticated key exchange*, Information Security and Privacy, Lecture Notes in Computer Science 6168, pp. 264–281. Springer, 2010, https://doi.org/10.1007/978-3-642-14081-5_17.
6. P. A. Grassi, M. E. Garcia, J. L. Fenton, *Digital identity guidelines*, Tech. Rep. SP 800-63, National Institute of Standards and Technology (NIST), 2017, https://doi.org/10.6028/NIST.SP.800-63-3, accessed: 2023-09-06.
7. S. Wiefling, L. L. Iacono, and M. Dürmuth, *Information website on risk-based authentication*, https://www.riskbasedauthentication.org, 2019, accessed: 2019-04-29.
8. S. Wiefling, L. L. Iacono, and M. Dürmuth, *Is this really you? An empirical study on risk-based authentication applied in the wild*, ICT Systems Security and Privacy Protection, IFIP Advances in Information and Communication Technology 562, pp. 134–148, Springer, 2019, https://doi.org/10.1007/978-3-030-22312-0_10, arXiv:2003.07622.

An introduction to Functional Encryption with multivariate algebra

Roberto La Scala

University of Bari, Italy

Abstract. In this talk, we introduce fundamental concepts behind the paradigm of Functional Encryption. Alongside Homomorphic Encryption, this protocol represents a primary tool for preserving data confidentiality during cloud-based processing. When the decrypted functions of the data are linear, this is referred to as Inner Product Functional Encryption. Finally, we present an IPFE protocol based on multivariate cryptography, specifically employing the Unbalanced Oil and Vinegar (UOV) digital signature scheme.

In recent years, with the progressive improvement in the speed and reliability of data networks, we have witnessed a growing diffusion of "cloud computing". This practice involves entrusting storage functions, software applications, and computation to powerful remote servers capable of meeting the needs of millions or even billions of users. In this context, ensuring the confidentiality of individual user data is of fundamental importance, making the use of specific cryptographic tools indispensable. Compliance with the regulations of many nations even compels the adoption of such tools.

To allow providers to deliver services through data processing while preserving confidentiality, the paradigms that are emerging as particularly promising are Functional Encryption [2,7] and Homomorphic Encryption [4], briefly FE and HE. These approaches pursue distinct objectives: in HE, the value of functions applied to plaintext data is calculated as a function of the encrypted data and returned to the owner in encrypted form. Only the data owner has the capability to use it, unless he decide to share it with the provider through an additional encryption system. Conversely, in FE, by using specific "functional keys" the provider can directly compute the value of the required functions on plaintext data starting from encrypted data, which are never fully decrypted. These features allow the provider to deliver services to users without requiring further actions from them, except for distributing the necessary functional keys.

To illustrate the paradigm of Functional Encryption, we provide a couple of examples of its applications. Consider a bank that wants to enable a credit verification

De Cifris Koine – CIFRIS24 ACTA –

agency to search encrypted financial data of its customers without revealing the entire database. To achieve this, the bank aims to implement suitable cryptographic tools that permit only the computation of specific credit evaluation functions, returning a result (e.g., whether a customer meets a certain credit threshold) without exposing any other sensitive information.

Imagine now a hospital that records the medical data of its patients. For research purposes, it could be useful to perform data analysis on these records. Using FE, the hospital can delegate the storage of the records to a cloud service without compromising their confidentiality because the data are encrypted before being sent to the server. At the same time, the hospital can distribute functional keys to researchers, enabling them to conduct medical statistical analyses on the records stored in the cloud for purposes such as evaluating a therapy, without accessing the actual content of the records.

Another common application of FE is performing machine learning on encrypted data while ensuring confidentiality. Specifically, after training a classifier on standard data, the data owner can generate specific functional keys for the functions required by the classifier. In other words, the classifier can perform classification on encrypted data without knowing its plaintext content.

If such computations require knowledge of linear functions of the plaintext data, we refer to the FE scheme as an Inner Product Functional Encryption, briefly IPFE, protocol. Some examples of inner products widely used in data analysis are the expected value and the convolution product. Recently, in [3], the authors introduced an IPFE protocol based on Multivariate Cryptography. We recall that this type of post-quantum cryptographic primitives achieves security through the challenge of computing preimages of generic quadratic polynomial maps $F : \mathbb{F}^n \to \mathbb{F}^m$ where $\mathbb{F}$ is a finite field. These primitives are typically digital signatures where signing a vector $v \in \mathbb{F}^m$ corresponds to compute a preimage $u \in \mathbb{F}^{-1}(v) \subset \mathbb{F}^n$. The signer holds a secret that allows for efficient computation of such a preimage.

In this talk, we introduce an enhanced version of the IPFE protocol described in [3], leveraging the latest advancements in UOV digital signature [1]. In this version of the protocol, the property that the quadratic map $F : \mathbb{F}^n \to \mathbb{F}^m$ is an "oil-vinegar map" corresponds to the existence of a secret vector subspace $O \subset F^{-1}(0)$. Using this subspace one can efficiently obtain elements in the preimages of F, without the need for any linear change of coordinates. If otherwise the subspace O is unknown, an opponent faces the NP-hard problem of solving a quadratic polynomial system over a finite field. For a recent paper on solving polynomial systems over finite fields, see for instance [6].

References

1. Beullens, W.; Chen, M.-S.; Ding, J.; Gong, B.; Kannwischer, M.J.; Patarin, J.; Peng, B.-Y.; Schmidt, D.; Shih, C.-J.; Tao, C.; Yang, B.-Y., UOV: Unbalanced Oil and

Vinegar Algorithm Specifications and Supporting Documentation, Version 1.0, 2023.
2. Boneh, D.; Sahai, A.; Waters, B., Functional encryption: definitions and challenges. Theory of cryptography, 253 – 273. Lecture Notes in Comput. Sci., 6597, Springer, Heidelberg, 2011.
3. Debnath, S.K.; Mesnager, S.; Dey, K.; Kundu, N., Post-quantum secure inner product functional encryption using multivariate public key cryptography. Mediterr. J. Math. 18 (2021), no. 5, Paper No. 204, 15 pp.
4. Gentry, C., Homomorphic encryption: a mathematical survey. ICM-International Congress of Mathematicians. Vol. 2. Plenary lectures, 956–1006.
5. La Scala, R., A protocol for inner product functional encryption based on the UOV scheme, preprint, 2024.
6. La Scala, Roberto; Pintore, Federico; Tiwari, Sharwan K.; Visconti, Andrea. A multistep strategy for polynomial system solving over finite fields and a new algebraic attack on the stream cipher Trivium, Finite Fields Appl. 98 (2024), Paper No. 102452, 1–33.
7. Mascia, C.; Sala, M.; Villa, I., A survey on functional encryption. Adv. Math. Commun. 17 (2023), no. 5, 1251–1289.

Registered Functional Encryption

Daniele Friolo

University of Roma, La Sapienza,Italy

Abstract. Registered encryption tackles the key-escrow problem associated with identity-based encryption by replacing the private-key generator with a (much weaker) entity known as the key curator. The key curator holds no secret information, and is responsible to: (i) update the master public key whenever a new user registers; (ii) provide (helper decryption) keys to the users already registered, so they can decrypt after new users have joined.

De Cifris Koine – CIFRIS24 ACTA –

Ringraziamenti

[...]