Jules Baudrin

Docteur en cryptographie

UCLouvain, Louvain-la-Neuve, Belgique

jules.baudrin@uclouvain.be
baudrin-j.github.io
29 ans

Situation actuelle

Chercheur postdoctoral, *Université catholique de Louvain (UCLouvain)*, Louvain-la-Neuve, Belgique. jan 2025 –

Formation

Doctorat d'informatique, *Inria*, Paris 2021-2024

Propriétés algébriques de chiffrements symétriques et de leurs composants non-linéaires.
Thèse de Sorbonne Université réalisée sous la direction d'Anne Canteaut et de Léo Perrin à Inria, Paris. Thèse soutenue le 6 décembre 2024 devant le jury composé de :

- Anne Canteaut — Inria Paris, France, directrice de thèse
- Léo Perrin — Inria Paris, France, co-directeur de thèse
- Henri Gilbert — ANSSI, France, rapporteur
- Sondre Rønjom — Université de Bergen, Norvège, rapporteur
- Christina Boura — Université Paris Cité, France
- Gohar Kyureghyan — Université de Rostock, Allemagne
- Gregor Leander — Université de la Ruhr à Bochum, Allemagne
- François-Xavier Standaert — Université catholique de Louvain, Belgique

Ma thèse porte sur la sécurité des primitives cryptographiques symétriques, en particulier, de celles dites *légères*, qui assurent la confidentialité dans des environnements très contraints, comme les puces RFID. En effet, l'équilibre entre sécurité, performance et coût est fragile et n'est pas complètement maîtrisé. Mes travaux contribuent à mieux comprendre ce compromis grâce à la cryptanalyse de chiffrements légers. J'ai également étudié des problèmes de mathématiques discrètes directement liés à la résistance optimale contre l'une des plus importantes classes d'attaques cryptographiques. Enfin, j'ai participé à la conception de deux nouvelles primitives répondant à de nouveaux usages, autres que ceux identifiés par la cryptographie légère.

Master algèbre appliquée & cryptographie, *Université Paris-Saclay*, Versailles, mention Très Bien. 2020 – 2021
• *Cryptographie, complexité algébrique, algèbre effective, courbes algébriques.*
• *Stage de recherche (6 mois) encadré par A. Canteaut et L. Perrin : Cryptanalyse d'une primitive symétrique légère soumise à la compétition du NIST : Ascon.*

Master mathématiques et applications, *Sorbonne Université*, Paris, mention Bien. 2018 – 2020
• *M1 : Calcul algébrique, algèbre commutative, théorie de Galois, représentations de groupes.*
• *M2 : Préparation à l'agrégation, option algèbre, calcul formel.*

Licence de mathématiques, *Sorbonne Université*, Paris, mention Très Bien. 2016 – 2018

Classe préparatoire et 1ère année de cycle ingénieur, *EPITA (Ecole Pour l'Informatique et les Techniques Avancées)*, Le Kremlin-Bicêtre, arrêt avant validation, pour reconversion. 2013 – 2016

Concours et distinctions

Bourse d'excellence, financée par la Fondation Mathématique Jacques Hadamard. 2020-2021

Reçu au concours de l'agrégation externe de mathématiques, rang 100. 2020

Enseignement

Encadrement de travaux dirigés universitaires, *Université de Versailles/Saint-Quentin-en-Yvelines (UVSQ)*, Versailles (vacations) 2021 – 2024
- *192 heures équivalent TD : travaux dirigés ou pratiques, du niveau L1 à M1.*
- *Rédaction de sujets, corrections, notes complémentaires.*
- *Surveillance et correction d'examens.*

Tutorat universitaire, *Sorbonne Université*, Paris (CDD) 2018 – 2020
- *Tutorats d'algèbre linéaire, bilinéaire et appliquée, niveau L2-L3.*
- *Missions pour le service handicap : transmission de cours, surveillance.*

Assistant d'éducation, *Collège-lycée Massillon*, Paris (CDD) 2014 – 2018
Surveillance scolaire, préparation des examens nationaux.

Encadrement de TP de programmation C, *EPITA*, Le Kremlin-Bicêtre (CDD) 2015

Détails des enseignements à l'UVSQ de 2021 à 2024

Applications Web et Sécurité, Master 1, (MIN17217), 5 séances de 3h réparties sur deux mois de fév. à mai 2024 (15h de TD). Responsable de l'UE : Yann Rotella. 2024
Projet libre de programmation Web en groupe, et en particulier de sécurité Web. Les séances permettent le suivi des projets, grâce à des rapports courts à l'écrit et à l'oral.

Cryptographie, Master 1, (MIN15122), 3h/semaine pendant 12 semaines de sept. à déc. 2023 (36h de TD). Responsable de l'UE : Louis Goubin. 2023
Cours de cryptographie, principalement de cryptographie symétrique : cryptanalyse et construction de chiffrements par blocs (DES, AES), cryptanalyses différentielle et intégrale, attaques génériques, compromis temps-mémoire, paradoxe des anniversaires, code d'authentification de message, cryptosystème RSA et attaques par fautes.

Mathématiques pour l'informatique, Licence 2, (LSIN310), 3h/semaine pendant 12 semaines de sept. à déc. 2022 (36h de TD). Responsable de l'UE : Christina Boura. 2022
Cours général de mathématiques : raisonnement par récurrence, fonctions, relations d'ordre et d'équivalence, arithmétique modulaire, Euclide étendu, calcul matriciel.

Cryptographie, Licence 3, (LSIN603), 3h/semaine pendant 12 semaines de fév. à mai 2022 (36h de TD). Responsable de l'UE : Christina Boura. 2022
Introduction à la cryptographie moderne : Enigma, chiffrements à flot (basé sur des LFSR) et par blocs (basé sur des schémas de Feistel, par ex. DES), modes d'opérations, cryptosystèmes RSA & ElGamal, protocole Diffie-Hellman.

Compléments de mathématiques discrètes, Master 1, (MIN17101), cours intensif : 5 séances de 3h réparties sur deux semaines en septembre 2022, idem en 2023 (2 × 15h de TD). Responsables de l'UE : Franck Quessette & Yann Rotella. 2022, 2023
Remise à niveau ou rappels en mathématiques discrètes, en particulier en algèbre (structure de groupe, anneau, corps, Euclide étendu, restes chinois) et en probabilités discrètes (dénombrements, lois de probabilités).

Compléments d'algorithmique, Master 1, (MIN17102), cours intensif : 5 séances de 3h réparties sur deux semaines en septembre 2022 (15h de TD). Responsable de l'UE : Sandrine Vial. 2022
Remise à niveau ou rappels en algorithmique : algorithmes de tri, d'insertion et de recherche, analyse de complexité, structures de données, tableaux, listes, piles, files, arbres (binaires, de recherche).

Fondements de l'informatique 1 - Initiation Python, Licence 1, (LSIN100), 3h/semaine pendant 12 semaines de sept. à déc. 2021 (36h de TP). Responsable de l'UE : Yann Rotella. 2021

Introduction à la programmation et en particulier au langage Python : structures conditionnelles et itératives, fonctions, listes, Git.

Recherche

Mes recherches portent principalement sur la *cryptographie symétrique*, mais aussi sur l'étude de *fonctions booléennes* et les *mathématiques discrètes*.

La *cryptographie* est la science assurant la sécurité de l'information lors d'une communication ou du stockage. Pour cela, la cryptographie *symétrique* présuppose la connaissance, par tous les protagonistes engagés dans une communication, d'un secret commun, appelé clé, qui permet le chiffrement et le déchiffrement des messages échangés.

Pour s'assurer de la sécurité des primitives symétriques, il est nécessaire de continuellement *cryptanalyser* ces dernières. La *standardisation* d'algorithmes permet à la communauté d'avoir confiance en un nombre restreint de standards. Néanmoins, les standards se doivent de suivre les contraintes dictées par les nouveaux usages. Parmi eux, la cryptographie dite *légère* assure la sécurité de dispositifs très contraints, comme les objets connectés ou les puces RFID.

Mon travail de recherche porte notamment sur l'analyse de primitives légères, avec une approche de nature *algébrique*. En effet, afin d'obtenir des performances compétitives et au plus bas coût, il est souvent nécessaire de se tourner vers des chiffrements dont la représentation comme ensemble de polynômes à coefficients dans $\mathbb{F}_2$ (c'est-à-dire comme une fonction booléenne vectorielle) peut s'avérer *creuse* et/ou de *bas degré*. Cette « légèreté algébrique » est un vecteur d'attaque fertile. Dans mes travaux, j'illustre par exemple comment ce type d'attaque compromet la confidentialité du futur standard de cryptographie légère aux États-Unis, Ascon, lorsque celui-ci est mal utilisé.

Je m'intéresse également à des classes d'attaques plus répandues, comme les attaques dites *différentielles*, qui exploitent la distribution de probabilité de la différence entre deux chiffrés correspondant à deux messages dont la différence est connue. Bien que très étudiées depuis plus de 30 ans, nombreux sont les problèmes ouverts par la cryptanalyse différentielle. Parmi eux, je m'intéresse à la généralisation de ces attaques à d'autres représentations d'un chiffrement donné, et notamment aux interactions avec des *changements de variables non-linéaires* qui peuvent permettre de mettre en évidence des faiblesses qui sont beaucoup plus difficiles à détecter en utilisant uniquement la représentation initiale du chiffrement.

J'étudie également les fonctions (dites *APN*) qui résistent de manière optimale à la cryptanalyse différentielle. Si leur définition est simple, la construction effective de tels objets est, elle, beaucoup plus compliquée, surtout lorsque l'on exige d'autres propriétés, comme la bijectivité. L'étude approfondie des fonctions APN est donc primordiale et nécessite des notions avancées de théorie des corps finis (de caractéristique 2) et plus généralement de mathématiques discrètes.

Enfin, outre la cryptanalyse, je participe également à la conception d'algorithmes de cryptographie symétrique pour des usages émergents, comme par exemple des codes d'authentification de message (MAC) qui permettent d'assurer l'authenticité et l'intégrité de communications et ce, en exploitant les jeux d'instructions mis à disposition par les concepteurs de processeurs pour obtenir des performances compétitives. Un autre exemple est celui d'un chiffrement à flot, opérant sur un corps fini $\mathbb{F}_p$ pour un p premier et impair, pour une utilisation dans des protocoles de cryptographie asymétrique qui imposent des contraintes très éloignées des contraintes usuelles en cryptographie symétrique.

Publications

Journaux internationaux avec comité de lecture

Fast AES-based Universal Hash Functions and MACs. Featuring LeMac and PetitMac, Bariant A., Baudrin J., Leurent G., Pernot C., Perrin L. & Peyrin T., *IACR Transactions on Symmetric Cryptology*, 2024(2), 35-67 `https://doi.org/10.46586/tosc.v2024.i2.35-67`. 2024

Les MAC permettent, entre autre, de s'assurer que des messages proviennent bien de l'expéditeur annoncé. Ils peuvent être construits à partir de fonctions de hachage universelles (UHF). Nous explorons une vaste classe d'UHF construites à partir du standard international AES. Notre analyse de sécurité repose sur celle d'AES, standard très étudié. Les performances obtenues sont compétitives grâce aux instructions AES présentes sur les processeurs modernes. J'ai participé à la conception, à l'analyse théorique, et à l'analyse assistée par un solveur mais moins à l'analyse de performance et à l'instantiation.

Commutative Cryptanalysis Made Practical, Baudrin J., Felke P., Leander G., Neumann P., Perrin L. & Stennes L., *IACR Transactions on Symmetric Cryptology*, 2023(4), 299–329 `https://doi.org/10.46586/tosc.v2023.i4.299-329`. 2023

Les chiffrements par blocs sont les briques principales des constructions qui assurent la confidentialité. Un chiffrement par blocs doit pour cela avoir des propriétés proches de celles d'une famille de bijections aléatoires. Pourtant, nous montrons qu'une version faiblement modifiée du chiffrement par blocs Midori commute avec une application affine et ce, pour de nombreuses clés. Son comportement est donc très loin de celui attendu aléatoirement. J'ai participé activement à l'ensemble du projet (analyse théorique et expérimentations sur ordinateur).

Practical Cube Attack against Nonce-Misused Ascon, Baudrin J., Canteaut A., & Perrin L., *IACR Transactions on Symmetric Cryptology*, 2022(4), 120–144. `https://doi.org/10.46586/tosc.v2022.i4.120-144`. 2022

Ascon est le nouveau standard international de chiffrement à bas coût. Il assure la sécurité des messages transmis à partir d'une clé secrète et d'une valeur publique éphémère appelée nonce. Nous montrons dans cet article que la confidentialité des messages est mise à défaut lorsque le nonce est utilisé pour chiffrer de l'ordre de 2^{40} messages. Pour cela, nous étudions précisément sa forme polynomiale dans $\mathbb{F}_2$, ce qui est rendu possible par le faible degré des composants internes d'Ascon. J'ai participé activement à l'ensemble du projet (analyse théorique et expérimentations sur ordinateur).

Workshops internationaux avec comité de lecture

On Functions of $\mathbb{F}_{2^{2t}}$ mapping Cosets of $\mathbb{F}_{2^t}^*$ to Cosets of $\mathbb{F}_{2^t}^*$, Baudrin J., Canteaut A., & Perrin L., *Workshop on Coding and Cryptography* (WCC), 2024, 45-57. `https://wcc2024.sites.dmi.unipg.it/WCC_proceedings.pdf`. 2024

Nous étudions des structures géométriques découvertes dans deux types d'objets cryptographiques : d'une part dans un composant non-linéaire utilisé dans deux standards russes de cryptographie, et d'autre part dans une fonction, dite APN, qui est optimale du point de vue de sa résistance à une technique de cryptanalyse. Dans les deux cas, les fonctions définies sur $\mathbb{F}_{2^{2t}}$ reflétent un certain alignement avec le sous-corps $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^{2t}}$.

Practical Cube Attack against Nonce-Misused Ascon, Baudrin J., Canteaut A., & Perrin L., *NIST fifth Lightweight Cryptography Workshop*, 2022, 19 pages. 2022

Présentation d'une version préliminaire de l'article du même nom (publié dans IACR Transactions on Symmetric Cryptology en 2022) au cours d'un workshop organisé par le NIST dans le cadre du processus de standardisation d'un chiffrement à bas coût.

Prépublications

Linear self-equivalence of the known families of APN functions : a unified point of view, Baudrin J., Canteaut A., & Perrin L., Article long soumis à un journal international. 43 pages. 2024
Les fonctions APN sont optimales du point de vue de l'analyse différentielle mais difficiles à construire. Depuis 35 ans, de multiples familles de fonctions APN ont été construites en utilisant des représentations polynomiales diverses (univariées ou multivariées), ce qui complexifie la comparaison entre ces constructions. Dans ce papier, nous exhibons pour de nombreuses d'entre elles une relation d'auto-équivalence linéaire, c'est-à-dire une symétrie dans la définition de la-dite fonction. Nous sommes donc en mesure de classifier la plupart des fonctions APN connues en fonction de la nature de leurs auto-équivalences, et ce, quelque soit la représentation initiale de la fonction. J'ai participé activement à l'ensemble du projet.

Commutative Cryptanalysis as a Generalization of Differential Cryptanalysis, Baudrin J., Beierle C., Felke P., Leander G., Neumann P., Perrin L. & Stennes L., Article long soumis à un journal international. 40 pages. Disponible en ligne : `https://eprint.iacr.org/2024/1678`. 2024
Ce travail est la continuité de l'article de 2023. Nous y étudions l'uniformité affine, qui généralise l'indicateur principal de l'analyse différentielle, l'uniformité différentielle. Nous précisons également les liens entre l'analyse commutative et les analyses différentielles de chiffrements conjugués, ou qui utilisent des lois de groupes autre que l'addition modulo 2 : il s'agit de trois points de vue différents sur une même classe d'attaques. J'ai participé à l'ensemble du projet, et plus particulièrement à l'étude des relations entre les différents points de vue.

Transitor : a TFHE-friendly Stream Cipher, Baudrin J., Belaïd S., Bon N., Boura C., Canteaut A., Leurent G., Paillier P., Perrin L., Rivain M., Rotella Y. & Tap S., Article long soumis à une conférence internationale. 30 pages. Disponible en ligne : `https://eprint.iacr.org/2025/282`. 2024
Le transchiffrement propose un compromis diminuant la bande passante d'un chiffrement homomorphe (FHE) en augmentant le nombre de calculs effectués. Pour limiter les calculs supplémentaires, un chiffrement symétrique adapté aux contraintes de FHE doit être utilisé. Nous proposons pour cela un chiffrement à flot basé sur $\mathbb{F}_{17}$, inspiré entre autre de l'AES, dont la sécurité contre les attaques classiques est analysée rigoureusement. J'ai participé à la conception, à l'analyse théorique, et à l'analyse assistée par un solveur mais pas à l'implémentation et l'analyse de performance.

Développement logiciel

Participation au développement de *SboxU*, *une bibliothèque SAGE/Python (5000 lignes et 3500 en C++) d'outils pour l'étude de boîtes-S et de fonctions booléennes. Disponible en ligne : `https://github.com/lpp-crypto/sboxU`.* 2024

Implémentation de distingueurs commutatifs probabilistes, *Programmation en C++ (1100 lignes) et en SAGE/Python (1700 lignes). Disponible en ligne : `https://github.com/baudrin-j/commutative_cryptanalysis_made_practical`.* 2023

Attaque par cubes contre Ascon en complexité pratique, *Programmation en C++ (2500 lignes) et en Python (770 lignes). Disponible en ligne : `https://github.com/baudrin-j/practical_cube_attack_against_nonce_misused_ascon`.* 2022

Communications orales

Conférences internationales avec comité de lecture

Commutative Cryptanalysis Made Practical, *FSE 2024*, Leuven, Belgique. mars 2024

Practical Cube Attack against Nonce-Misused Ascon, *FSE 2023*, Kobe, Japon. mars 2023

Workshops internationaux avec comité de lecture

On Functions of $\mathbb{F}_{2^{2t}}$ mapping Cosets of $\mathbb{F}_{2^t}^*$ to Cosets of $\mathbb{F}_{2^t}^*$, *Workshop on Coding and Cryptography (WCC)*, 2024, Pérouse, Italie. juin 2024

Practical Cube Attack against Nonce-Misused Ascon, *NIST fifth Lightweight Cryptography Workshop*, 2022, en ligne. mai 2022

Conférences nationales avec comité de lecture

L'auto-équivalence linéaire, un point de vue unifié sur les familles connues de fonctions APN, *Journées Codage & Cryptographie* (JC2), organisées par le GT C2 des GDR *Informatique Fondamentale et ses Mathématiques* et *Sécurité Informatique*, 2025, Pornichet, France. mars 2025

Commutative Cryptanalysis Made Practical, *Journées Codage & Cryptographie* (JC2), 2023, Najac, France. oct 2023

Cube-like attack against Ascon, *Journées Codage & Cryptographie* (JC2), 2022, Hendaye, France. avr 2022

Séminaires nationaux

Geometrical structures among known APN functions, Séminaire national du GT C2, Sorbonne Université, France. juil 2024

Séminaires locaux

L'auto-équivalence linéaire, un point de vue unifié sur les familles connues de fonctions APN, Séminaire CRYPTO (UVSQ), Versailles, France. fév 2025

Differential cryptanalysis of conjugate ciphers, Séminaire de cryptographie de Rennes, Rennes, France. fév 2025

Cryptanalyse différentielle de chiffrements conjugués, Séminaire de l'équipe ALMASTY (LIP6), Paris, France. jan 2025

Practical cube-attack against nonce-misused Ascon, Séminaire au sein du Crypto Group de l'UCLouvain, Louvain-la-Neuve, Belgique. mai 2024

La cryptanalyse commutative, une classe (pas trop) générale d'attaques, Séminaire de l'équipe CRYPTO du laboratoire de mathématiques de Versailles (LMV), UVSQ, Versailles, France. nov 2023

Autres activités académiques

Encadrement

Co-encadrement du stage de recherche de Cyprien Gauthier, (Master 1, ENSTA Paris). Avec Anne Canteaut & Léo Perrin, du 21 mai au 26 juillet 2024. 2024
Recherche de boîte-S optimales dans $\mathbb{F}_p$. Le stage de Cyprien portait sur la recherche de bijections de $\mathbb{F}_p$ résistantes aux attaques différentielles et linéaires, pour un usage dans un chiffrement « orienté arithmétisation ». L'approche était à la fois mathématique (étude des fonctions monomiales), mais aussi algorithmique (algorithmes de recherche).

Activités éditoriales

Rapport pour le journal *Designs, Codes and Cryptography.* 2025

Rapport pour la conférence *ISC 2024* (*Information Security Conference*). 2024

Rapport pour la conférence *CRYPTO 2024.* 2024

Rapports pour le journal *Finite Fields and Their Applications.* 2022, 2023

Conceptions d'algorithmes cryptographiques

Participation à la conception de deux MAC (codes d'authentification de messages) opérant sur la fonction de tour de l'AES : *LeMac* and *PetitMac.* 2022–2024

Participation à la conception d'un chiffrement à flot basé sur $\mathbb{F}_{17}$ pour le chiffrement complétement homomorphe (FHE) : *Transistor.* 2021–2024

Invitations

Séjour scientifique, Toulon, France déc 2024
Rencontre dans le cadre de l'ANR SWAP autour de l'analyse de fonctions boolénnes avec Y. Aubry, P. Langevin (Université de Toulon), G. Chopin, Y. Rotella (UVSQ), A. Canteaut et L. Perrin (Inria).

Séjours scientifiques, Louvain-la-Neuve, Belgique mai/nov 2024
Rencontres avec le CryptoGroup de l'UCLouvain autour de sujets de cryptanalyse et d'attaques par canaux auxiliaires.

Participation au workshop sur invitation Beating Real-Time Crypto, Lorentz Center, Leiden, Pays-Bas avril 2024
Groupe de travail sur invitation organisé par S. Rasoolzadeh, C. Boura, M. Eichlseder, B. Mennink & Y. Todo et portant sur la cryptographie à bas coût, en particulier à basse latence.

Séjour scientifique, Berlin, Allemagne juin 2023
Rencontre autour de la cryptanalyse commutative et de la conception de chiffrements avec "backdoor" avec G. Leander , L. Stennes (Université de la Ruhr à Bochum, Allemagne), P. Felke (Université de Emden/Leer, Allemagne), O. Dunkelman, S. Ghosh (Université de Haifa, Israël) et L. Perrin (Inria, France)

Diffusion grand public

Animation d'un atelier dans le cadre d'un Rendez-vous des Jeunes Mathématiciennes et Informaticiennes (RJMI), organisé par les associations *Animath* et *femmes & mathématiques*, au centre Inria de Paris en novembre 2021. 2021