


2025 Activity Report

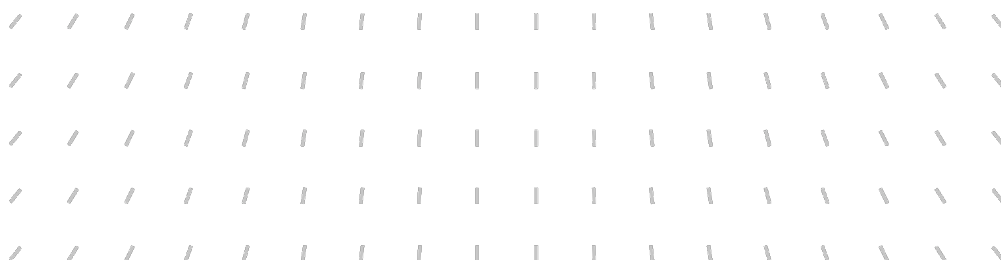
RESEARCH CENTRE: Inria Paris Centre


Project-Team

COSMIQ

Code-based Cryptology, Symmetric Cryptology and
Quantum Information





Project-Team COSMIQ

Creation of the Project-Team: 2019 December 01

Each year, Inria research teams publish an Activity Report presenting their work and results over the reporting period. These reports follow a common structure, with some optional sections depending on the specific team. They typically begin by outlining the overall objectives and research programme, including the main research themes, goals, and methodological approaches. They also describe the application domains targeted by the team, highlighting the scientific or societal contexts in which their work is situated. The reports then present the highlights of the year, covering major scientific achievements, software developments, or teaching contributions. When relevant, they include sections on software, platforms, and open data, detailing the tools developed and how they are shared. A substantial part is dedicated to new results, where scientific contributions are described in detail, often with subsections specifying participants and associated keywords. Finally, the Activity Report addresses funding, contracts, partnerships, and collaborations at various levels, from industrial agreements to international cooperations. It also covers dissemination and teaching activities, such as participation in scientific events, outreach, and supervision. The document concludes with a presentation of scientific production, including major publications and those produced during the year.

Keywords

Computer sciences and digital sciences

- A1.2.8. – Network security
- A3.1.5. – Control access, privacy
- A4. – Security and privacy
- A4.2. – Correcting codes
- A4.3. – Cryptography
- A4.3.1. – Public key cryptography
- A4.3.2. – Secret key cryptography
- A4.3.3. – Cryptographic protocols
- A4.3.4. – Quantum Cryptography
- A6.2.3. – Probabilistic methods
- A7.1. – Algorithms
- A7.1.4. – Quantum algorithms
- A8.1. – Discrete mathematics, combinatorics
- A8.6. – Information theory

Other research topics and application domains

- B6.4. – Internet of things
- B6.5. – Information systems
- B9.5.1. – Computer science
- B9.5.2. – Mathematics
- B9.10. – Privacy

Contents

Project-Team COSMIQ	1
1 Team members, visitors, external collaborators	5
2 Overall objectives	7
3 Research program	7
3.1 Quantum algorithms and cryptanalysis	7
3.2 Symmetric cryptology	7
3.3 Post-quantum asymmetric cryptology	8
3.4 Quantum information	8
4 Application domains	9
4.1 Designing, Analyzing and Choosing Cryptographic Standards	9
4.2 Large scale deployment of quantum cryptography	10
5 Social and environmental responsibility	11
5.1 Impact of research results	11
6 Highlights of the year	11
6.1 Awards	11
6.2 NIST PQC competition and standardization of HQC	11
7 Latest software developments, platforms, open data	11
7.1 Latest software developments	11
7.1.1 Wave	11
7.1.2 Collision Decoding	11
8 New results	12
8.1 Quantum algorithms and cryptanalysis	12
8.2 Symmetric cryptology	12
8.3 Post-quantum asymmetric cryptology	12
8.4 Quantum information	12
9 Bilateral contracts and grants with industry	13
9.1 Bilateral grants with industry	13
10 Partnerships and cooperations	13
10.1 International initiatives	13
10.1.1 Inria associate team not involved in an ILL or an international program	13
10.1.2 Visits to international teams	13
10.2 European initiatives	14
10.2.1 Horizon Europe	14
10.3 National initiatives	16
11 Dissemination	17
11.1 Promoting scientific activities	17
11.1.1 Scientific events: organisation	17
11.1.2 Scientific events: selection	17
11.1.3 Journal	18
11.1.4 Invited talks	19
11.1.5 Leadership within the scientific community	19
11.1.6 Research administration	19
11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach	20
11.2.1 Supervision	20

11.2.2	Juries	21
11.2.3	Educational and pedagogical outreach	22
11.3	Popularization	22
11.3.1	Productions (articles, videos, podcasts, serious games, ...)	23
11.3.2	Others science outreach relevant activities	23
12	Scientific production	23
12.1	Major publications	23
12.2	Publications of the year	24
12.3	Cited publications	28

1 Team members, visitors, external collaborators

Research Scientists

- Jean-Pierre Tillich [Team leader, INRIA, Senior Researcher, HDR]
- Anne Canteaut [INRIA, Senior Researcher, HDR]
- André Chailloux [INRIA, Researcher, HDR]
- Pascale Charpin [INRIA, Emeritus, HDR]
- Gaëtan Leurent [INRIA, Senior Researcher, HDR]
- Anthony Leverrier [INRIA, HDR]
- María Naya Plasencia [INRIA, Senior Researcher, HDR]
- Léo Perrin [INRIA, Researcher]
- Nicolas Sendrier [INRIA, Senior Researcher, HDR]
- Michael John George Vasmer [INRIA, ISFP]

Faculty Member

- Laura Luzzi [ENSEA, Associate Professor Delegation, HDR]

Post-Doctoral Fellows

- Pierre Galissant [INRIA, Post-Doctoral Fellow, from Feb 2025]
- Shibam Ghosh [INRIA, Post-Doctoral Fellow]
- Paul Hermouet [INRIA, Post-Doctoral Fellow, from Apr 2025]
- Eran Lambooi [INRIA, from Apr 2025]
- Patrick Neumann [INRIA, Post-Doctoral Fellow]
- Christophe Piveteau [SNSF, Post-Doctoral Fellow, from May 2025]
- Quan Quan Tan [INRIA, from Nov 2025]
- Thomas Van Himbeek [INRIA, Post-Doctoral Fellow]

PhD Students

- Sacha Baillarguet-Gajic [INRIA]
- Antoine Bak [DGA]
- Agathe Blanvillain [INRIA]
- Aurelien Boeuf [INRIA]
- Quentin Buzet [INRIA, from Sep 2025]
- Bruno Costa Alves Freire [PASQAL, CIFRE]
- Baptiste Daumen [INRIA, from Nov 2025]
- Merlin Fruchon [DGA]

- Virgile Guémard [INRIA]
- Valerian Hatey [ENSEA]
- Guilhem Jazeron [INRIA]
- Axel Lemoine [DGA]
- Dounia M’Foukh [INRIA]
- Florent Mazelet [INRIA, from Feb 2025]
- Antoine Mesnard [INRIA]
- Charles Meyer-Hilfiger [INRIA, until Mar 2025]
- Bastien Michel [INRIA]
- Ewan Murphy [Quandela, CIFRE, from Sep 2025]
- Samuel Novak [INRIA]
- Clement Poirson [ALICE ET BOB, CIFRE]
- Magali Salom [THALES, CIFRE]

Technical Staff

- Etienne Stock [INRIA, Engineer, from Nov 2025]

Interns and Apprentices

- Quentin Buzet [INRIA, from Feb 2025 until Jul 2025]
- Baptiste Daumen [INRIA, Intern, from Mar 2025 until Oct 2025]
- César Mathéus [INRIA, Intern, from Mar 2025 until Sep 2025]
- Florent Mazelet [INRIA, until Jan 2025]
- Jules Perrin De Brichambaut [INRIA, Intern, from May 2025 until Aug 2025]
- Maria Slim [INRIA, from Sep 2025 until Nov 2025]

Administrative Assistants

- Christelle Guiziou [INRIA]
- Abigail Palma [INRIA]

External Collaborators

- Augustin Bariant [ANSSI]
- Jules Baudrin [UVSQ, from Dec 2025]
- Christina Boura [IRIF, until Aug 2025]
- Kevin Carrier [CY CERGY PARIS UNIV, until Aug 2025]
- Yann Rotella [UVSQ, HDR]
- Valentin Vasseur [THALES]
- Thomas Vidick [CALTECH, until Aug 2025]

2 Overall objectives

The research within the project-team is related to cryptography and more generally to protection of information, be it classical or quantum. In a nutshell, the overall goal within our project-team is to cover the following classical and quantum aspects of cryptology, together with the specific area of quantum codes:

- new cryptanalysis, classical or quantum, in symmetric and asymmetric cryptography,
- new designs of classical symmetric and asymmetric primitives or quantum primitives that are resistant against a classical and quantum adversary,
- design of quantum codes allowing for efficient fault-tolerant quantum computation.

3 Research program

3.1 Quantum algorithms and cryptanalysis

Well-analyzed mathematical problems such as integer factorization or the discrete logarithm problem, that have been the foundations of asymmetric cryptographic for many years, were found to be easily solved with Shor's algorithm by a quantum computer. This has prompted the community to actively search for alternatives and the NIST to launch in 2017 a still ongoing competition aiming at standardizing the most suitable candidates. Even if the proposed solutions to this competition have good reasons to be believed resistant to a quantum computer, they often have a rich mathematical structure that makes them tantalizing targets for quantum speedups that go beyond the usual Grover/quantum-walk speedups. The recent work of Chen, Liu and Zhandry on solving LWE in superposition (Eurocrypt 2022) is a good illustration of this potential. It gives a quantum polynomial time algorithm of the Short Integer Solution (SIS) problem for some parameters seemingly unreachable for classical computers. The SIS problem appears in lattice-based cryptography and while this does not break current proposals for lattice-based cryptography, it shows that even computational assumptions believed to be secure against quantum computers are at risk with quantum algorithms going way beyond Shor's algorithm.

On the other hand, symmetric cryptography, essential for enabling secure communications, used to seem much less affected at first sight: the biggest known threat was Grover's algorithm, which allows exhaustive key searches in the square root of the normal complexity. Thus, it was believed that doubling key-lengths suffices to maintain an equivalent security in the post-quantum world, but this has changed since our project QUASYModo.

Indeed, our results have shown that both for symmetric and asymmetric cryptography, the impact of quantum computers goes well beyond Grover's and Shor's algorithms and has to be studied carefully in order to understand if a given cryptographic primitive is secure or not in a quantum world. To correctly evaluate the security of cryptographic primitives in the post-quantum world, it is really desirable to elaborate a quantum cryptanalysis toolbox. This whole thread of research, that needs to combine techniques from symmetric or asymmetric cryptanalysis together with quantum algorithmic tools, came naturally in our team which is composed of symmetric and asymmetric cryptologists as well as of experts in quantum computing. We have exploited this unique opportunity to become one of the leading research teams in the field. We have also managed to pass on the interest and the focus in this research direction to other international groups that have recently published some interesting new results on quantum cryptanalysis, like: G. Leander and A. May (U. Bochum), T. Iwata (U. Nagoya), Y. Sasaki and A. Hosoyamada (NTT), Xiaoyun Wang et al. (Tsinghua U, Beijing), Li Yang et al. (Chinese academy of science)...

3.2 Symmetric cryptology

Symmetric techniques are widely used because they are the only ones that can achieve some major features such as high-speed or low-cost encryption, fast authentication, and efficient hashing. It is a very active research area which is stimulated by a pressing industrial demand for low-cost implementations. Even if the block cipher standard AES remains unbroken 25 years after its design, it clearly appears that it cannot serve as a Swiss Army knife in all environments. In particular an important challenge raised by several new applications is the design of symmetric encryption schemes with some additional properties compared to

the AES, either in terms of implementation performance (low-cost hardware implementation, low latency, resistance against side-channel attacks...) or in terms of functionalities. The past decade has then been characterized by a multiplicity of new proposals and evaluating their security has become a primordial task which requires the attention of the community.

This proliferation of symmetric primitives has been amplified by public competitions, including the recent NIST lightweight standardization effort, which have encouraged innovative but unconventional constructions in order to answer the harsh implementation constraints. These promising but new designs need to be carefully analyzed since they may introduce unexpected weaknesses in the ciphers. Our research work captures this conflict for all families of symmetric ciphers. It includes new attacks and the search for new building blocks which ensure both a high resistance to known attacks and a low implementation cost. This work, which combines cryptanalysis and the theoretical study of discrete mathematical objects, is essential to progress in the formal analysis of the security of symmetric systems.

Our specificity, compared to most groups in the area, is that our research work tackles all aspects of the problem, from the practical ones (new attacks, concrete constructions of primitives and low-cost building-blocks) to the most theoretical ones (study of the algebraic structure of underlying mathematical objects, definition of optimal objects). We study these aspects not separately but as several sides of the same domain.

3.3 Post-quantum asymmetric cryptology

Current public-key cryptography is particularly threatened by quantum computers, since almost all cryptosystems used in practice rely on related number-theoretic security problems that can be easily solved on a quantum computer as shown by Shor in 1994. This very worrisome situation has prompted NIST to launch a standardization process in 2017 for quantum-resistant alternatives to those cryptosystems. This concerns all three major asymmetric primitives, namely public-key encryption schemes, key-exchange protocols and digital signatures. The NIST has made it clear that for each primitive there will be several selected candidates relying on different security assumptions. It publicly admits that the evaluation process for these post-quantum cryptosystems is significantly more complex than the evaluation of the SHA-3 and AES candidates for instance.

There were 69 (valid) submissions to this call in November 2017, with numerous lattice-based, code-based and multivariate-cryptography submissions and some submissions based either on hashing or on supersingular elliptic curve isogenies. In January 2019, 26 of these submissions were selected for the second round and 7 of them are code-based submissions. In July 2020, 15 schemes were selected as third round finalists/alternate candidates, 3 of them are code-based. In July 2022, the NIST announced the first candidates to be standardized: one lattice-based encryption/KEM and three digital signature schemes (two lattice-based and one hash based). Meanwhile four encryption/KEM schemes (three code-based and one isogeny based) which were still under discussion advanced to the fourth round. The isogeny based candidate was broken shortly afterwards and finally the code based candidate HQC was selected in March 2025. Note that our team is involved in all three code-based schemes that remained.

The lack of diversity among the signatures left in the process prompted the NIST to suggest to the community to propose in June 2023 additional signature schemes relying on other security assumptions than the ones that have been selected. Forty additional submissions of this kind were accepted in July.

The research of the project-team in this field is focused on the design and cryptanalysis of cryptosystems making use of coding theory and we have proposed code-based candidates to the NIST call for the first two types of primitives, namely public-key encryption and key-exchange protocols and have two candidates among the finalists/alternate candidates. We also submitted Wave to the second call of signature schemes and are involved in the submission MIRA, PERK and RYDE. The last three made it to the second round in 2024.

3.4 Quantum information

The field of quantum information and computation aims at exploiting the laws of quantum physics to manipulate information in radically novel ways. There are two main applications:

- (i) quantum computing, that offers the promise of solving some problems that seem to be intractable for classical computers such as for instance factorization or solving the discrete logarithm problem;

- (ii) quantum cryptography, which provides new ways to exchange data in a provably secure fashion. For instance it allows key distribution by using an authenticated channel and quantum communication over an unreliable channel with information-theoretic security, in the sense that its security can be proven rigorously by using only the laws of quantum physics, even with all-powerful adversaries.

Our team deals with quantum coding theoretic issues related to building a large quantum computer and with quantum cryptography. If these two questions may seem at first sight quite distinct, they are in fact closely related in the sense that they both concern the protection of (quantum) information either against an adversary in the case of quantum cryptography or against the environment in the case of quantum error-correction. This connection is actually quite deep since an adversary in quantum cryptography is typically modeled by a party having access to the entire environment. The goals of both topics are then roughly to be able to measure how much information has leaked to the environment for cryptography and to devise mechanisms that prevent information from leaking to the environment in the context of error correction.

While quantum cryptography is already getting out of the labs, this is not yet the case of quantum computing, with large quantum computers capable of breaking RSA with Shor's algorithms maybe still decades away. The situation is evolving very quickly, however, notably thanks to massive public investments in the past couple of years and all the major software or hardware companies starting to develop their own quantum computers. One of the main obstacles towards building a quantum computer is the fragility of quantum information: any unwanted interaction with the environment gives rise to the phenomenon of decoherence which prevents any quantum speedup from occurring. In practice, all the hardware of the quantum computer is intrinsically faulty: the qubits themselves, the logical gates and the measurement devices. To address this issue, one must resort to quantum fault-tolerance techniques which in turn rely on the existence of good families of quantum error-correcting codes that can be decoded efficiently. Our expertise in this area lies in the study of a particularly important class of quantum codes called quantum low-density parity-check (LDPC) codes. The LDPC property, which is well-known in the classical context where it allows for very efficient decoding algorithms, is even more crucial in the quantum case since enforcing interactions between a large number of qubits is very challenging. Quantum LDPC codes solve this issue by requiring each qubit to only interact with a constant number of other qubits.

4 Application domains

4.1 Designing, Analyzing and Choosing Cryptographic Standards

The research community is strongly involved in the development and evolution of cryptographic standards. Many standards are developed through open competitions (*e.g.* AES, SHA-3) where multiple teams propose new designs, and a joint cryptanalysis effort allows to select the most suitable proposals. The analysis of established standards is also an important work, in order to depreciate weak algorithms before they can be exploited. Several members of the team have been involved in this type of effort and we plan to continue this work to ensure that secure algorithms are widely available. We believe that good cryptographic standards have a large socio-economic impact, and we are active in proposing schemes to future competitions, and in analyzing schemes proposed to current or future competitions, as well as widely-used algorithms and standards.

We have been involved in the two standardization efforts run by NIST for post-quantum cryptography and lightweight cryptography. We have also uncovered potential backdoors in two algorithms from the Russian Federation (Streebog and Kuznyechik), and successfully presented the standardization of the latter by ISO. We have also implemented practical attacks against SHA-1 to speed-up its deprecation.

NIST post-quantum competition.

The NIST post-quantum competition¹ aims at standardizing quantum-safe public-key primitives. It is really about offering a credible quantum-safe alternative for the schemes based on number theory which are severely threatened by the advent of quantum computers. We are involved in two of the three candidates which remain in the fourth round of the competition. In 2020, we obtained a significant breakthrough in solving more efficiently the MinRank problem and the decoding problem in the rank metric [74, 75] by using algebraic techniques. This had several consequences: all second round rank metric candidates were dismissed

¹web site

from the third round (including our own candidate) and it was later found out that this algebraic algorithm could also be used to attack the third round multivariate finalist, namely RAINBOW and the alternate third round finalist GEMSS. Various algebraic techniques were also developed to attack the McEliece cryptosystem [79, 76, 78] or for related schemes based on other families of algebraic codes [77]. Even if these algebraic techniques are right now not a threat against the NIST fourth-round finalist [73] CLASSICMcELIECE, they indeed show that the square-code based distinguisher of high-rate Goppa codes or alternant codes that we devised in our project ten years ago, can indeed be transformed in most of the cases into an actual attack on a McEliece scheme based on them. This is not a threat though on the CLASSICMcELIECE proposal, because the rate of the code used there is not high enough to be in the distinguishable regime. However in [78], we have significantly enlarged the region of rates where there is a rather efficient distinguisher thanks to a novel concept, namely associating to a code a space of quadratic forms containing very low rank quadratic forms if the code is a Goppa code. This paves the way for new algebraic attacks on the McEliece cryptosystem.

NIST competition on lightweight symmetric encryption.

The NIST lightweight cryptography standardization process² is an initiative to develop and standardize new authenticated encryption algorithms suitable for constrained devices. As explained in Subsection 3.2, there is a real need for new standards in lightweight cryptography, and the selected algorithms are expected to be widely deployed within the Internet of Things, as well as on more constrained devices such as contactless smart cards, or medical implants. The NIST received 56 submissions in February 2019, three of which, including one of 10 finalists, have been co-designed by members of the team.

Monitoring Current Standards

While we are very involved in the design phase of new cryptographic standards (see above), we also monitor the algorithms that are already standardized. In practice, this work has two sides.

First, we work towards the deprecation of algorithms known to be unsafe. Unfortunately, even when this fact is known in the academic community, standardizing bodies can be slow to implement the required changes to their standards. This prompted for example G. Leurent to implement even better attacks against SHA-1 to illustrate its very practical weakness, and L. Perrin and X. Bonnetain (then a COSMIQ member) to find simple arguments proving that a subfunction used by the current Russian standards was not generated randomly, despite the claims of its authors.

Second, it also means that we participate to the relevant ISO meetings discussing the standardization of cryptographic primitives (JC27/WG2), and that we follow the discussions of the IETF and IRTF on RFCs. We have also provided technical assistance to members of other standardizing bodies such as the ETSI.

4.2 Large scale deployment of quantum cryptography

Major academic and industrial efforts are currently underway to implement quantum key distribution at large scale by integrating this technology within existing telecommunication networks. Colossal investments have already taken place in China to develop a large network of several thousand kilometers secured by quantum cryptography, and there is little doubt that Europe will follow the same strategy, as testified by the current European projects CiViQ (in which we are involved), OpenQKD and the future initiative Euro-QCI (Quantum Communication Infrastructure). While the main objectives of these actions are to develop better systems at lower cost and are mainly engineering problems, it is crucial to note that the security of the quantum key distribution protocols to be deployed remains far from being completely understood. For instance, while the asymptotic regime of these protocols (where one assumes a perfect knowledge of the quantum channel for instance) has been thoroughly studied in the literature, it is not the case of the much more relevant finite-size regime accounting for various sources of statistical uncertainties for instance. Another issue is that compliance with the standards of the telecommunication industry requires much improved performances compared to the current state-of-the-art, and this can only be achieved by significantly tweaking the original protocols. It is therefore rather urgent to better understand whether these more efficient protocols remain as secure as the previous ones. Our work in this area is to build upon our own expertise in continuous-variable quantum key distribution, for which we have developed the most advanced security proofs, to give security proofs for the protocols used in this kind of quantum networks.

²Website of the NIST project.

5 Social and environmental responsibility

5.1 Impact of research results

Our project is still involved in the NIST competition for standardizing quantum-safe cryptosystems where we were involved in two fourth-round finalists and are now part of the HQC team which is the code based candidate selected for standardization. This is expected to have a strong impact since the standardized solution will likely replace large parts of the world's infrastructure underpinning secure global communication.

6 Highlights of the year

6.1 Awards

Anne Canteaut and Anthony Leverrier are among the hundred winners in Le Point's 2025 Inventors' Awards ranking. Their distinction continues a tradition within the team, as Maria Naya-Plasencia had already been honored in a previous edition of this ranking.

6.2 NIST PQC competition and standardization of HQC

Nicolas Sendrier, Jean-Pierre Tillich and Valentin Vasseur are coauthors of the HQC proposal which was selected by NIST in 2025 as standard for post-quantum Key-Encapsulation Mechanism (KEM). This provides outstanding visibility to the researchers involved and to the COSMIQ team. The mathematical background of HQC relates to codes defined as subspaces of binary cyclic polynomial ring and to the hardness of their decoding, topics in which the team members had numerous, sometimes pioneering, contributions.

7 Latest software developments, platforms, open data

7.1 Latest software developments

7.1.1 Wave

Name: Wave

Keywords: Cryptography, Error Correction Code

Functional Description: Implementation of the code based signature scheme Wave whose security relies solely on decoding large Hamming weight errors and distinguishing a generalized $U, U+V$ code from a random code.

URL: <http://wave.inria.fr/en/implementation/>

Contact: Nicolas Sendrier

7.1.2 Collision Decoding

Keywords: Algorithm, Binary linear code

Functional Description: Collision Decoding implements two variants of information set decoding : Stern-Dumer, and MMT. To our knowledge it is the best full-fledged open-source implementation of generic decoding of binary linear codes. It is the best generic attack against code-based cryptography.

URL: <https://gforge.inria.fr/projects/collision-dec/>

Contact: Nicolas Sendrier

Participant: 2 anonymous participants

8 New results

8.1 Quantum algorithms and cryptanalysis

Participants: Agathe Blanvillain, Quentin Buzet, André Chailloux, Paul Hermouet, Christophe Piveteau, María Naya-Plasencia, Jean-Pierre Tillich.

We have kept on working on generic quantum algorithms related to cryptanalysis, and in addition, have devised some new algorithms showing a quantum advantage for solving approximate interpolation problems.

8.2 Symmetric cryptology

Participants: Sacha Baillarguet-Gajic, Antoine Bak, Augustin Bariant, Jules Baudrin, Aurélien Boeuf, Anne Canteaut, Pascale Charpin, Baptiste Daumen, Merlin Fruchon, Pierre Galissant, Shibam Ghosh, Guilhem Jazeron, Eran Lambooj, Gaëtan Leurent, César Mathéus, Dounia M’Foukh, Bastien Michel, María Naya-Plasencia, Patrick Neumann, Léo Perrin, Jules Perrin De Brichambaut, Maria Slim, Quan Quan Tan.

Our recent results in symmetric cryptography concern either the security analysis of existing primitives, or the design of new primitives. This second topic includes some work on the construction and properties of suitable building-blocks for these primitives, e.g. on the search of highly nonlinear functions.

8.3 Post-quantum asymmetric cryptology

Participants: André Chailloux, Loïc Demange, Valerian Hatey, Axel Lemoine, Laura Luzzi, Antoine Mesnard, Charles Meyer-Hilfiger, Magali Salom, Nicolas Sendrier, Jean-Pierre Tillich.

Our work in this area is mainly focused on code-based cryptography, but some of our contributions, namely algebraic attacks, have applications in multivariate cryptography or in algebraic coding theory. Many contributions relate to the NIST call for postquantum primitives, either cryptanalysis or design.

We have also been organizing since 2015 a working group held every month or every two months on code-based cryptography that structures the French efforts on this topic: every meeting is attended by most of the groups working in France on this topic (project-team GRACE, University of Bordeaux, University of Limoges, University of Rennes and University of Rouen).

8.4 Quantum information

Participants: André Chailloux, Bruno Costa Alves Freire, Virgile Guémard, Thomas Van Himbeeck, Anthony Leverrier, Ewan Murphy, Samuel Novak, Clement Poirson, Etienne Stock, Jean-Pierre Tillich, Michael John George Vasmer.

Most of our work in quantum information deals with either quantum algorithms, quantum error correction or cryptography. Our work on quantum error correction and fault tolerant quantum computation has significantly expanded with the arrival of Michael Vasmer.

9 Bilateral contracts and grants with industry

Participants: Anthony Leverrier, Nicolas Sendrier, Michael John George Vasmer.

9.1 Bilateral grants with industry

- **Thalès** (10/2024 -> 9/2027) Funding for the supervision of Magali Salom's PhD. 45 kEuros.
- **Alice & Bob** (11/2024 -> 10/2027) Funding for the supervision of Clement Poirson's PhD. 45 kEuros.
- **Pasqal** (11/2024 -> 10/2027) Funding for the supervision of Bruno Costa Alves Freire's PhD. 45 kEuros.
- **Quandela** (9/2025 -> 8/2028) Funding for the supervision of Ewan Murphy's PhD. 45 kEuros.
- **Apple Inc.** (12/2024 -> 02/2026)

10 Partnerships and cooperations

10.1 International initiatives

10.1.1 Inria associate team not involved in an IIL or an international program

COSINUS

Title: Collaboration On Secrecy to Investigate New USE

Duration: January 2023 -> December 2025

Coordinator: Carlos Cid (carlos@simula.no)

Partners:

- Simula (Norvège)

Inria contact: Leo Perrin

Summary: The aim of the COSINUS associated team is for the COSMIQ team and the cryptography group at Simula to join forces to work on an emerging trend in symmetric cryptography, namely "arithmetization-orientation". A primitive such as a hash function is said to be arithmetization-oriented if, in a nut-shell, it lends itself well to an implementation as an arithmetic circuit. This requirement implies significant changes for the symmetric primitives, one of the main ones being that of the underlying alphabet: rather than CPU instructions operating over bitstrings, arithmetization-oriented primitives rely on finite field operations (addition, multiplication), where the finite field has a large (often prime) size.

The final outcome of this collaboration is expected to be a new family of arithmetization-oriented symmetric primitives that significantly outperforms the state-of-art, as well as a deeper understanding of the security of the primitives of this type.

10.1.2 Visits to international teams

Research stays abroad

Michael John George Vasmer

Visited institution: Perimeter Institute for Theoretical Physics

Country: Canada

Dates: March 3-April 4 and August 4-8

Context of the visit: part of Visiting fellow position

Mobility program/type of mobility: research stay

Michael John George Vasmer

Visited institution: Yale Quantum Institute

Country: USA

Dates: April 7-18

Context of the visit: invited by Aleksander Kubica

Mobility program/type of mobility: research stay

Michael John George Vasmer

Visited institution: Kavli Institute for Theoretical Physics

Country: USA

Dates: August 18-September 5

Context of the visit: invitation to the *Noise-robust Phases of Quantum Matter* program

Mobility program/type of mobility: research stay

10.2 European initiatives

10.2.1 Horizon Europe

ReSCALE [ReSCALE project on cordis.europa.eu](https://cordis.europa.eu)

Title: Reinventing Symmetric Cryptography for Arithmetization over Large fields

Duration: From September 1, 2022 to August 31, 2027

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France

Inria contact: Leo Perrin

Coordinator:

Summary: "Symmetric cryptography is finding new uses because of the emergence of novel and more complex (e.g. distributed) computing environments.

These are based on sophisticated zero-knowledge and Multi-Party Computation (MPC) protocols, and they aim to provide strong security guarantees of types that were unthinkable before. In particular, they make it theoretically possible to prove that a computation was done as claimed by those performing it without revealing its inputs or outputs. This would make it possible e.g. for e-governance algorithms to prove that they are run honestly; and overall would increase the trust we can have in various automated processes.

The security techniques providing these guarantees are sequences of operations in a large finite field $GF(q)$, where typically $q > 2^{64}$. However, these procedures also rely on hash functions and other "symmetric" cryptographic algorithms that are defined over $GF(2) = \{0,1\}$. But encoding $GF(2)$ operations using $GF(q)$ operations is very costly: relying on standard hash functions leads to significant performance overhead, to the point where the protocols mentioned before are unusable in practice.

In order to alleviate this bottleneck, it is necessary to devise symmetric algorithms that are natively described in $GF(q)$. This change requires great care: some hash functions described in $GF(q)$ have already been presented, and subsequently exhibited significant flaws. The inherent structural differences between $GF(2)$ and $GF(q)$ are the cause behind these problems: our understanding of the construction of symmetric primitives in $GF(2)$ does not carry over to $GF(q)$.

With this project, I will bring symmetric cryptography into $GF(q)$ in a safe and efficient way. To this end, I will rebuild the analysis tools and methods that are used both by designers and attackers. This project will naturally lead to the design of new algorithms whose adoption will be simplified by the efficient and easy-to-use software libraries we will provide."

SoBaSyC [SoBaSyC project on cordis.europa.eu](https://cordis.europa.eu/so-ba-sy-c)

Title: Solid Basis for Symmetric Cryptography

Duration: From April 1, 2024 to March 31, 2029

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France

Inria contact: Maria NAYA PLASENCIA

Coordinator:

Summary: Symmetric cryptography, essential for enabling secure communications, has benefited from an explosion of new results in the last two decades, in big part due to several standardization efforts: many public competitions have been launched since 1997, where the community proposes cryptographic constructions and simultaneously evaluates their security and performance. The security of symmetric cryptography is based on cryptanalysis: we only gain confidence in a symmetric cryptographic function through extensive and continuous scrutiny.

However, the current context has not allowed the community to digest all the new findings, as can be seen from several recurrent issues. The two main ones are:

- 1) primitives proposed at top-tier venues often get broken by slight modifications of already known techniques;
- 2) published cryptanalysis at top conferences sometimes include mistakes or are suboptimal. They are also often re-invented and re-named.

The main challenge of SoBaSyC is to establish solid bases for symmetric cryptography. Using cryptanalysis as the starting point, my aim is to unify the knowledge obtained through the years on the different families of attacks, to transform it with an algorithmic approach and to endow it with optimizations. The final result will be a toolbox congregating all our newly proposed optimized algorithms, that will provide the best known attacks on a given construction, through an easy application. Next, I plan to derive from this algorithmic approach some theoretical bounds, as well as some properties that I will include in the security proofs of symmetric constructions, providing more meaningful and realistic security arguments.

This would allow, for the first time, to ensure that any newly proposed primitive or construction is already resistant to all known attacks, and will considerably increase the confidence on these functions. It will also save a considerable amount of time and allow the field to advance, at last, on solid ground.

10.3 National initiatives

- **ANR SWAP** (02/22→09/26)
 Sboxes for Symmetric-Key Primitives
 ANR Program: AAP Générique 2021
 Partners: UVSQ (coordinateur), Inria COSMIQ, ANSSI, CryptoExperts, Univ. of Rouen, Univ. of Toulon.
 172 kEuros
 Sboxes are small nonlinear functions that are crucial components of most symmetric-key designs and their properties are highly related to the security of the overall construction. The development of new attacks has given rise to many Sbox design criteria. However, the emerge of new contexts, applications and environments requires the development of new design criteria and strategies. The SWAP project aims first at investigating such criteria for emerging use cases like whitebox cryptography, fully homomorphic encryption and side-channel resistance. Then, we wish for analyzing the impact of these particular designs on cryptanalysis and see how the use of Sboxes with some special mathematical structures can accelerate some known attacks or introduce new ones. Finally, we aim at studying Sboxes from a mathematical point of view and provide new directions to the Big APN problem, an old conjecture on the existence of a particular type of optimal permutations.
- **CRYPTANALYSE** (10/23→09/28)
 Cryptanalysis of classical cryptographic primitives
 ANR Program: AAP PEPR Cybersécurité
 Partners: COSMIQ (coordinator), CARAMBA (coordinator), LFANT, LIRMM, IRISA, LMV, MIS, LIP6, LJK
 605 kEuros (Total amount: 5 MEuros)
 This is one of the ten projects within the Program on Cybersecurity([url](#)), funded by the French investment plan, France 2030. This project brings together the main French research groups working on cryptanalysis. It will study simultaneously the most widely used cryptographic primitives, the more recent primitives which have been around for a shorter time or which are within the long process of academic approval or standardisation, and finally the project also studies specialized primitives which are designed for some specific application contexts. In all cases, the main goal is to provide accurate hardness estimations for the underlying problems and, ultimately, a good understanding of the security level, both for symmetric and for asymmetric primitives. Software tools, which will be made openly available when appropriate, are bound to play a key role in this work. This project will advance the state of the art in cryptanalysis, and eventually increase the security of primitives used today and in the future.
- **ANR EPIQ** (01/22→12/27)
 Quantum Software - Study of the quantum stack: Algorithm, models, and simulation for quantum computing
 ANR Program: PEPR on Quantum Technologies
 Partners: MOCQA(coordinator), COSMIQ, CEA (LIST, IPHT, MEM), Inria (Paris, Bordeaux, Nancy, Lyon, Rennes, Saclay), University of Aix-Marseille (LIS), University of Bordeaux (LABRI), University of Bourgogne and Franche Comté (ICB), University of Grenoble (LPMMC, NEEL), University of Paris (IRIF), Sorbonne University (LIP6),
 230 kEuros
 The purpose of this project is (i) to understand the advantages and limits of quantum computing via both quantum complexity research and the discovery and enhancement of algorithms, (ii) to define the framework for quantum computation using high-level languages, comparison of computational models as well as using their relations for program optimization, (iii) develop simulation tools to anticipate the performances of algorithms on noisy quantum machines. We are involved in studying the limits of quantum algorithms in cryptanalysis.
- **ANR NISQ2LSQ** (01/22→12/27)
 From NISQ to LSQ: Bosonic and LDPC codes
 ANR Program: PEPR on Quantum Technologies

Partners: COSMIQ (coordinator), Inria (Paris, Nancy, Lyon, Saclay), SPEC/CEA Saclay, PHELIQS/CEA Grenoble, LPMMC, ENS Lyon, LPTHE, Alice&Bob, C2N, Majulab, LCF, LIP6, LKB, MPQ, Quandela, Institut de Mathématiques de Bordeaux, CEA-LETI, GR2IF, XLIM

420 kEuros

This project aims at accelerating the R&D efforts in the theory and conception of hardware-efficient fault-tolerant quantum codes. As far as codes are concerned, the project focuses on two of the most promising solutions, namely bosonic codes and Low-Density Parity-Check (LDPC) codes. On the hardware side, the targeted platforms are superconducting qubits and photonic ones.

- **ANR TLS-PQ** (01/22→12/26)

Post-quantum padlock for web browser

ANR Program: PEPR on Quantum Technologies

Partners: CAPSULE(coordinator), COSMIQ, Inria (Paris, Bordeaux, Nancy, Lyon, Rennes, Saclay), CEA-LETI, University of Bordeaux (TDN), University of Caen (AMACC), University of Limoges (Cryptis), University of Rouen (CA), University of Saint-Etienne (SESAM), University of Versailles (Cryptis), ARCAD

430 kEuros

This integrated project aims to develop in 5 years post-quantum primitives in a prototype of « post-quantum lock » that will be implemented in an open-source browser. We are involved in developing code-based solutions and analyzing the security of the proposed algorithms.

- **Q-LOOP** (01/24 → 12/29)

Préparer le contrôle commande de l'ordinateur quantique ANR program on Quantum Technologies

Partners: CEA, IRT, CNRS, Inria, Siemens, A&B, C12, Quandela, Qubly 120 kEuros

This project aims at building a portfolio of HW and SW technologies enabling the control at large scale of emerging solid state qubits technologies e.g. Superconducting cat qubits, semiconductor qubits (carbon nanotubes, spin qubits) and photonic qubits in development by emerging industrial actors. The project will cover a large span of technologies ranging from cryo-electronics to real time error correction under a system approach encompassing the development of models for control chains enabling the exploration of various architectures and leading to demonstration of solutions representative of future scaling requirements.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Dagstuhl seminar: Quantum error correction meets ZX-calculus, September 15-19 2025, Dagstuhl (Germany), Michael John George Vasmer
- Dagstuhl seminar: Symmetric Cryptology, Feb. 2026, Dagstuhl (Germany), María Naya Plasencia

Member of the organizing committees

- WCC 2026, June 12- June 16, Paris, Leo Perrin
- [SKCAM 2025](#) María Naya Plasencia

11.1.2 Scientific events: selection

Chair of conference program committees

- SAC 2026, August 24–28, 2026, Ottawa, Canada, Gaëtan Leurent

Steering Committees

- Fast Software Encryption (FSE) Gaëtan Leurent(member since 2019)
- Post-quantum cryptography (PQCrypto), Nicolas Sendrier, Jean-Pierre Tillich
- Workshop on Coding and Cryptography (WCC), Pascale Charpin, Nicolas Sendrier, Jean-Pierre Tillich.

Member of the conference program committees

Anne Canteaut: • Crypto 2025

- FSE 2025, 2026
- Test-of-Time Award Committee of Eurocrypt, Crypto and Asiacrypt 2025.

Andre Chailloux • QIP 2026

Gaëtan Leurent: • Eurocrypt 2025, 2026

- Crypto 2025 (area chair)

Anthony Leverrier: • ISIT 2025

- QEC 2025
- QIP 2025

María Naya Plasencia: • FSE 2025

- Eurocrypt 2026

Leo Perrin: • Boolean Functions and their Applications, 2025

- Eurocrypt 2026

Nicolas Sendrier: • PQCrypto 2025, 2026

Jean-Pierre Tillich: • Asiacrypt 2025, Asiacrypt 2026 (area chair)

- Eurocrypt 2025
- PQCrypto 2025, 2026
- PKC 2026 (area chair)
- WCC 2026

Michael John George Vasmer: • QIP 2026

11.1.3 Journal

Member of the editorial boards

- Advances in Mathematics for Communications, associate editors : Nicolas Sendrier (since 2018), Jean-Pierre Tillich(since 2017)
- Applicable Algebra in Engineering, Communication and Computing, associate editor: Anne Canteaut (since 2016)
- Designs, Codes and Cryptography, associate editor: Pascale Charpin (since 2003)
- Finite Fields and Their Applications, associate editors: Anne Canteaut, Pascale Charpin (since 2013)
- IACR Transactions on Symmetric Cryptology, Anne Canteaut(2025, 2026), Leo Perrin (2025)
- IEEE Transactions on Information Theory, Anne Canteaut: area editor (since 2021), Anthony Leverrier: associate editor (since 2023)
- Journal of Cryptology, Anne Canteaut (since 2021)
- Quantum – the open journal for quantum science, Michael John George Vasmer

11.1.4 Invited talks

- Anne Canteaut, *Stream Ciphers Strike Back*, *FSE (Fast Software Encryption)*, Rome, Italy, March 2025.
- Anne Canteaut, *On the structure of the known infinite families of APN functions*, *AGCCT (Arithmetic, Geometry, Cryptography and Coding Theory)*, Luminy, June 9-13, 2025.
- Anne Canteaut, *On the structure of the known infinite families of APN functions*, BFA (Boolean Functions and their Applications), September 1-5, 2025.
- Anne Canteaut, *Understanding Unexpected Fixed-Key Differential Behaviours*, *Gelcrypt*, Nijmegen, November 2025.
- Anne Canteaut, *À la recherche de fonctions optimales sur les corps finis pour la cryptographie symétrique*, *Congrès de la Société Mathématique de France* (Dijon, June 2025)
- Anne Canteaut, *Plaidoyer pour une recherche ouverte, publique et indépendante en cryptographie (et en informatique)*, 10 years of Cristal Lab, Lille, Oct. 3, 2025.
- Anne Canteaut, *Un problème mathématique issu de la cryptographie symétrique : la recherche de fonctions APN*, *Forum des jeunes mathématiciennes et mathématiciens* (Bordeaux, Nov. 26-28, 2025).
- Leo Perrin, *What happens when you *don't* have tools? The case of algebraic cryptanalysis*. Workshop on Symmetric-key Cryptanalysis Automation and Modelling (SKCAM), Rome, Italy, March 15, 2025.
- María Naya-Plasencia, *Symmetric Cryptanalysis State-of-the-Art and Future: Towards a Generalization of Cryptanalysis techniques*. Workshop on Symmetric-key Cryptanalysis Automation and Modelling (SKCAM), Rome, Italy, March 15, 2025.
- María Naya-Plasencia, *On Cryptanalysis of Low-Latency Primitives*. 2nd Workshop on Low-Latency Encryption (LLE 2025), Madrid, Spain, May 3, 2025.
- Michael John George Vasmer, *Fault-tolerant photonic quantum computing by stitching together resource states*, International Conference on Quantum Photonics, Wenzhou, China, October 25-26, 2025.

11.1.5 Leadership within the scientific community

- Elected director of the IACR board (2024-2026) María Naya Plasencia

11.1.6 Research administration

- Committees for the selection of professors, assistant professors and researchers**
- Selection Committee, Professorship in Cryptology, Graz University of Technology (Austria): Anne Canteaut.
 - Selection Committee, Academic in Cybersecurity and Software security, UC Louvain-la-Neuve (Belgium), Nov 2025-Feb. 2026: Anne Canteaut.
 - Selection Committee, Anne Beffort Excellence Programme - Associate / Assistant Professor in Theoretical Computer Science, University of Luxembourg: Anne Canteaut.
 - Selection Committee, Chaire « Gouvernance et ingénierie de l'information », CNAM: Anne Canteaut.
 - Hiring Commission (Commission recrutement), École Polytechnique: Anne Canteaut.
- Other responsibilities**
- International Scientific Advisory Board of the Flemish Strategic Research Program on Cybersecurity: Anne Canteaut (since 2019)
 - Member of the Scientific Board of GDR IFM: Anne Canteaut.
 - Member of the Scientific Board of Direction de la Recherche Technologique at CEA: Anne Canteaut.
 - Member of the Scientific Board of Le Studium Loire Valley Institute for Advanced Studies: Anne Canteaut.

- Member of the Scientific Board of the French Police (Conseil Scientifique de la Police Nationale): Anne Canteaut.
- Member of the Hcéres evaluation panel of Laboratoire de l'Informatique du Parallélisme (LIP), Lyon: Anne Canteaut (Oct. 2025-Jan. 2026).
- Members of the Jury of Prix Inria-Académie des Sciences: Anne Canteaut, María Naya Plasencia.
- Member of the jury of Prix Irène Joliot-Curie: Anne Canteaut.
- Member of the jury of the prize "Jeunes Talents France 2025 L'Oréal-UNESCO Pour les Femmes et la Science": Anne Canteaut.
- Member of the steering committee of PCQT (Paris Center for Quantum Technologies): André Chailloux (since 2024)
- Elected member in the Inria Evaluation Committee: Gaëtan Leurent (since September 2023)
- Member of the board of the GdR TEQ: Anthony Leverrier (since 2023)
- Member of the Hcéres evaluation panel of Lirmm, Grenoble: María Naya Plasencia (2025)
- Member of the *Comité Égalité-Parité* of the GT-C2: Léo Perrin (since 2023)

Local committees

- Gaëtan Leurent is a member of the IT Users Commission (CUMI-R)
- Anne Canteaut, Léo Perrin and Dounia M'Foukh are members of the *Comité de Centre*
- María Naya Plasencia is the president of the *Commission pour l'Emploi Scientifique* (since 2022)
- Léo Perrin is a member of the *Commission pour l'Emploi Scientifique* (since 2024)
- Jean-Pierre Tillich is in charge of the *Mission Jeunes Chercheurs*

11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

- Master: Anne Canteaut, *Canteaut, Error-correcting codes and applications to cryptology*, 12 hours, M2, University Paris-Cité (MPRI), France;
- Master: André Chailloux, *Quantum Circuits and Logic Gates*, 12 hours, M1, Sorbonne Université;
- Master: André Chailloux, Quantum information, 12 hours, M2, University Paris-Cité (MPRI), France;
- Master: André Chailloux Quantum algorithms, 4 hours, M2, Ecole Normale Supérieure de Lyon, France;
- Master: Léo Perrin, Application Web et Sécurité, 24 hours, M1, UVSQ, France;
- Master: Anne Canteaut, María Naya Plasencia, Léo Perrin, *Symmetric Cryptography*, M2, 6+6+6 hours, Université Paris-Cité (MIC), France.
- Master: Michael John George Vasmer, *Introduction to quantum information theory*, 32 hours, M2, Université PSL, France
- Spring school: Anne Canteaut and Léo Perrin gave 6-hour lectures at the Spring School on Symmetric Cryptography, Rome, Italy, Feb. 9-14.

11.2.1 Supervision

- PhD: Charles Meyer-Hilfiger, Design and analysis of dual attacks in code- and lattice-based cryptography, September 30, supervisors: Nicolas Sendrier, Jean-Pierre Tillich;
- Phd: Louis Paletta, Autonomous quantum error correction with cat qubits, October 17, supervisors: Anthony Leverrier, M. Mirrahimi, A. Sarlette, C. Vuillot;
- PhD: Virgile Guemard, Lifts de codes quantiques CSS, November 28, supervisors: B. Audoux, A. Leverrier;

- PhD in progress: Aurelien Boeuf, Analyse de la sécurité de primitives symétriques “Orientées Arithmétisation”, since October 2022, supervisors: Anne Canteaut, Léo Perrin;
- PhD in progress: Dounia M’Foukh, Symmetric cryptography, since September 2023, supervisor: María Naya Plasencia;
- PhD in progress: Agathe Blanvillain, The quantum decoding problem, since October 2023, supervisor: Jean-Pierre Tillich;
- PhD in progress: Valerian Hatey, The decoding problem and attacks on FHE protocols, since October 2023, supervisors: Laura Luzzi, Kevin Carrier;
- PhD in progress: Axel Lemoine, Algebraic attacks on the McEliece cryptosystem, since October 2023, supervisor: Jean-Pierre Tillich;
- PhD in progress: Sacha Baillarguet-Gajic, Improving key-recovery attacks, since October 2024, supervisor: María Naya Plasencia;
- PhD in progress: Antoine Bak, since October 2024, supervisors: Léo Perrin and Anne Canteaut.
- PhD in progress: Bruno Costa Alves Freire, Quantum LDPC codes, since October 2024, supervisors: F.M. Le Régent, Anthony Leverrier
- PhD in progress: Merlin Fruchon, Towards a better understanding of the security of symmetric primitives, since October 2024, supervisor: Anne Canteaut.
- PhD in progress: Guilhem Jazon, Cryptanalyse algébrique de primitives symétriques destinées au protocoles avancés, since October 2024, supervisors: Léo Perrin and Gaëtan Leurent;
- PhD in progress: Florent Mazelet, Cryptanalyse des modes opératoires en cryptographie symétrique, since February 2025, supervisors: Gaëtan Leurent and María Naya Plasencia;
- PhD in progress: Bastien Michel, Automatization of attacks, since October 2024, supervisor: María Naya Plasencia.
- PhD in progress: Samuel Novak, Fault-tolerant homological codes, since October 2024 supervisors: Anthony Leverrier, C. Vuillot.
- PhD in progress: Clement Poirson, Bosonic codes, since October 2024, supervisor: Anthony Leverrier, C. Vuillot.
- PhD in progress: Magali Salom, Side-channel attacks and implementation of code-based cryptographic schemes, since October 2024, supervisor: Nicolas Sendrier.
- PhD in progress: Antoine Mesnard, Code based cryptographic schemes, since November 2024, supervisor: Nicolas Sendrier;
- PhD in progress: Ewan Murphy, Improving quantum error correction with dynamical codes and teleportation, since October 2025, supervisors: P. Hilaire, Anthony Leverrier, Michael John George Vasmer.

11.2.2 Juries

- Yann Rotella, Éléments de Cryptanalyse (HDR), February 6, UVSQ, comité: María Naya Plasencia(reviewer);
- Nouédyn Baspin, On the locality of quantum codes, University of Sydney, May 29, 2025, committee: Michael John George Vasmer (reviewer);
- Daniël Kuijsters, Structured randomness, Radboud University, NL, July 3, 2025, committee: Anne Canteaut(reviewer);

- Dina Khaled Sayed Abdelhadi, Noisy Quantum Communication and Computation, July 7, EPFL, committee: Jean-Pierre Tillich (reviewer);
- Corentin Lanore, Toward photonic device-independent quantum key distribution, September 25, Université Paris-Saclay, committee: Anthony Leverrier (reviewer);
- Charles Meyer-Hilfiger, Design and analysis of dual attacks in code- and lattice-based cryptography, September 30, Sorbonne Université, committee: Nicolas Sendrier, Sendrier, Jean-Pierre Tillich (supervisors);
- Enrico Piccione, Construction of Cryptographic Functions and Threshold Implementations, Univ. Bergen, Norway, Oct. 16 2025, , committee: Anne Canteaut (first opponent);
- Louis Paletta, Autonomous quantum error correction with cat qubits, October 17, Université Paris sciences et lettres, committee: Anthony Leverrier (supervisor);
- Daphné Trama, Conception d'un jeu d'instructions homomorphe universel et applications au transchiffrement avec TFHE, CEA List, Nov. 13 2025, committee: Anne Canteaut (chair);
- Adrien Vinçotte, Protocoles cryptographiques basés sur les codes correcteurs d'erreur en métrique rang, November 21, Université de Limoges, committee: Jean-Pierre Tillich.
- Virgile Guémard, Lifts de codes quantiques CSS, November 28, Aix Marseille Université, committee: Anthony Leverrier (supervisor);
- Wouter Rozendaal, Étude de codes LDPC quantiques et de leur décodage, December 2, University of Bordeaux, committee: Jean-Pierre Tillich (reviewer).

11.2.3 Educational and pedagogical outreach

- Talk at Collège Anne Franck, Sauzé-Vaussais, classe de troisième, Jan. 31, 2025. Anne Canteaut.
- Talk at "Cycle de conférences - vers une nouvelle équation académique", classes de lycée et enseignants, Maison des mathématiques, Pantin, Feb. 12, 2025, Anne Canteaut.
- Talk at Collège Gaspard Malo, Dunkerque, classes de cinquième, Feb. 26, 2025, Anne Canteaut.
- Talk for high-school students, Académie des Sciences, October 2025 (250 attendees), Anne Canteaut.
- Three talks Lycée Stendahl, Milano, Italy, classes de CM2, de seconde et de terminale, Nov. 2025, Anne Canteaut.
- Talks at Collège Eugène Delacrois, Roissy-en-Brie, classes de quatrième et troisième, December 2025, Anne Canteaut.
- Cours découverte métier Cryptographie, classe de CM2, École Fagon. December 2, 2025, María Naya Plasencia.
- Talk on Spanish highschool Piles, Gijón, Spain. "Encuentros con científicos" December 4, 2025 María Naya Plasencia.

11.3 Popularization

- *Rencontre avec la chercheuse qui casse les codes secrets*, Paris Saclay Summit, Feb. 13, 2025. Anne Canteaut.
- *La recherche sur le numérique : périmètre et enjeux scientifiques et sociétaux*, INSP, January 24, 2025. Anne Canteaut.
- *Quel(s) type(s) d'engagement, de l'individu aux institutions ?*, **Congrès du Collège des Sociétés savantes**, Montpellier, Feb. 4, 2025. Anne Canteaut.

- *Pilotage de la recherche et liberté académique*, AFDESRI (Association des femmes dirigeantes de l'ESRI), Nogent-sur-Marne, May 14, 2025. Anne Canteaut.
- Demi-journée "Carrières après le doctorat", GDR Sécurité, May 5, 2025. Anne Canteaut.
- Journées Parité, Scientific Boards of CNRS Sciences Informatiques et CNRS Mathématiques, Oct 2025. Anne Canteaut.
- *Cybersécurité - Un temps d'avance*, CNRS, December 2025. Anne Canteaut.

11.3.1 Productions (articles, videos, podcasts, serious games, ...)

- Article: Anne Canteaut, *La cryptographie post-quantique : où en sommes-nous ?*, *Revue des ingénieurs des Mines*, 2025.
- Documentary series: *TV5 Monde Femmes de Sciences : Anne Canteaut - La science du secret*, Nov. 2025.

11.3.2 Others science outreach relevant activities

Michael John George Vasmer participated to the panel of experts of Q2B 2025 which is Europe's leading quantum conference, bringing together global experts, industry leaders, and policymakers to explore breakthroughs, assess technologies, and unlock business value in the evolving quantum ecosystem.

12 Scientific production

12.1 Major publications

- [1] C. Beierle, A. Canteaut, G. Leander and Y. Rotella. 'Proving Resistance Against Invariant Attacks: How to Choose the Round Constants.' In: *Crypto 2017 - Advances in Cryptology*. Ed. by J. Katz and H. Shacham. Vol. 10402. LNCS - Lecture Notes in Computer Science. Steven Myers. Santa Barbara, United States: Springer, Aug. 2017, pp. 647–678. DOI: [10.1007/978-3-319-63715-0_22](https://doi.org/10.1007/978-3-319-63715-0_22). URL: <https://hal.inria.fr/hal-01631130>.
- [2] A. Canteaut and L. Perrin. 'On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting'. In: *Finite Fields and Their Applications* 56 (Mar. 2019), pp. 209–246. DOI: [10.1016/j.ffa.2018.11.008](https://doi.org/10.1016/j.ffa.2018.11.008). URL: <https://hal.inria.fr/hal-01953353>.
- [3] A. Chailloux, M. Naya-Plasencia and A. Schrottenloher. 'An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography'. In: *Asiacrypt 2017 - Advances in Cryptology*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. LNCS - Lecture Notes in Computer Science. Hong Kong, China: Springer, Dec. 2017, pp. 211–240. DOI: [10.1007/978-3-319-70697-9_8](https://doi.org/10.1007/978-3-319-70697-9_8). URL: <https://hal.inria.fr/hal-01651007>.
- [4] K. Chakraborty, A. Chailloux and A. Leverrier. 'Arbitrarily Long Relativistic Bit Commitment'. In: *Physical Review Letters* 115 (Dec. 2015). DOI: [10.1103/PhysRevLett.115.250501](https://doi.org/10.1103/PhysRevLett.115.250501). URL: <https://hal.inria.fr/hal-01237241>.
- [5] P. Charpin, G. M. Kyureghyan and V. Suder. 'Sparse Permutations with Low Differential Uniformity'. In: *Finite Fields and Their Applications* 28 (Mar. 2014), pp. 214–243. DOI: [10.1016/j.ffa.2014.02.003](https://doi.org/10.1016/j.ffa.2014.02.003). URL: <https://hal.archives-ouvertes.fr/hal-01068860>.
- [6] T. Debris-Alazard, N. Sendrier and J.-P. Tillich. 'Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes'. In: *ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 11921. LNCS. Kobe, Japan: Springer, Dec. 2019, pp. 21–51. DOI: [10.1007/978-3-030-34578-5_2](https://doi.org/10.1007/978-3-030-34578-5_2). URL: <https://hal.inria.fr/hal-02424057>.

- [7] O. Fawzi, A. Gropellier and A. Leverrier. ‘Constant overhead quantum fault-tolerance with quantum expander codes’. In: *FOCS 2018 - 59th Annual IEEE Symposium on Foundations of Computer Science*. Paris, France, Oct. 2018, pp. 743–754. DOI: [10.1109/FOCS.2018.00076](https://doi.org/10.1109/FOCS.2018.00076). URL: <https://hal.archives-ouvertes.fr/hal-01895430>.
- [8] A. Florez-Gutierrez, G. Leurent, M. Naya-Plasencia, L. Perrin, A. Schrottenloher and F. Sibleyras. ‘New results on Gimli: full-permutation distinguishers and improved collisions’. In: *Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 12491. Lecture Notes in Computer Science. Daejeon / Virtual, South Korea, 7th Dec. 2020, pp. 33–63. DOI: [10.1007/978-3-030-64837-4_2](https://doi.org/10.1007/978-3-030-64837-4_2). URL: <https://inria.hal.science/hal-03045986>.
- [9] M. Kaplan, G. Leurent, A. Leverrier and M. Naya-Plasencia. ‘Breaking Symmetric Cryptosystems Using Quantum Period Finding’. In: *Crypto 2016 - 36th Annual International Cryptology Conference*. Ed. by M. Robshaw and J. Katz. Vol. 9815. LNCS - Lecture Notes in Computer Science. Santa Barbara, United States: Springer, Aug. 2016, pp. 207–237. DOI: [10.1007/978-3-662-53008-5_8](https://doi.org/10.1007/978-3-662-53008-5_8). URL: <https://hal.inria.fr/hal-01404196>.
- [10] G. Leurent and T. Peyrin. ‘SHA-1 is a Shambles’. In: *USENIX 2020 - 29th USENIX Security Symposium*. Boston / Virtual, United States, Aug. 2020. URL: <https://hal.inria.fr/hal-03136301>.
- [11] A. Leverrier. ‘Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction’. In: *Physical Review Letters* 118.20 (May 2017), pp. 1–24. DOI: [10.1103/PhysRevLett.118.200501](https://doi.org/10.1103/PhysRevLett.118.200501). URL: <https://hal.inria.fr/hal-01652082>.
- [12] R. Misoczki, J.-P. Tillich, N. Sendrier and P. S. L. M. Barreto. ‘MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes’. In: *IEEE International Symposium on Information Theory - ISIT 2013*. Istanbul, Turkey, July 2013, pp. 2069–2073. URL: <https://hal.inria.fr/hal-00870929>.
- [13] L. Perrin. ‘Partitions in the S-Box of Streebog and Kuznyechik’. In: *IACR Transactions on Symmetric Cryptology* 2019.1 (Mar. 2019), pp. 302–329. DOI: [10.13154/tosc.v2019.i1.302-329](https://doi.org/10.13154/tosc.v2019.i1.302-329). URL: <https://hal.inria.fr/hal-02396814>.

12.2 Publications of the year

International journals

- [14] H. Aghaee Rad, T. Ainsworth, R. Alexander, B. Altieri, M. Askarani, R. Baby, L. Banchi, B. Baragiola, J. Bourassa, R. Chadwick et al. ‘Scaling and networking a modular photonic quantum computer’. In: *Nature* 638.8052 (22nd Jan. 2025), pp. 912–919. DOI: [10.1038/s41586-024-08406-9](https://doi.org/10.1038/s41586-024-08406-9). URL: <https://hal.science/hal-05467868>.
- [15] J. Alich, A. Askeland, S. Banik, T. Beyne, A. Canteaut, P. Felke, G. Leander, W. Meier and L. Stennes. ‘Observations on TETRA Encryption Algorithm TEA-3’. In: *IACR Transactions on Symmetric Cryptology* 2025.1 (7th Mar. 2025), pp. 276–308. DOI: [10.46586/tosc.v2025.i1.276-308](https://doi.org/10.46586/tosc.v2025.i1.276-308). URL: <https://inria.hal.science/hal-05466815>.
- [16] R. Avanzi, O. Dunkelman and S. Ghosh. ‘Differential Cryptanalysis of the Reduced Pointer Authentication Code Function Used in Arm’s FEAT_PACQARMA3 Feature’. In: *IACR Transactions on Symmetric Cryptology* 2025.1 (7th Mar. 2025), pp. 380–419. DOI: [10.46586/tosc.v2025.i1.380-419](https://doi.org/10.46586/tosc.v2025.i1.380-419). URL: <https://inria.hal.science/hal-05519460>.
- [17] A. Bak, G. Jazeron, P. Galissant and L. Perrin. ‘Attacking Split-and-Lookup-Based Primitives Using Probabilistic Polynomial System Solving: Applications to Round-Reduced Monolith and Full-Round Skyscraper’. In: *IACR Transactions on Symmetric Cryptology* 2025.3 (25th Sept. 2025), pp. 337–367. DOI: [10.46586/tosc.v2025.i3.337-367](https://doi.org/10.46586/tosc.v2025.i3.337-367). URL: <https://inria.hal.science/hal-05519443>.
- [18] A. Bak and L. Perrin. ‘On the Security of Split-and-Lookup-Based ZK-Friendly Primitives’. In: *IACR Transactions on Symmetric Cryptology* 2025.2 (11th June 2025), pp. 87–123. DOI: [10.46586/tosc.v2025.i2.87-123](https://doi.org/10.46586/tosc.v2025.i2.87-123). URL: <https://hal.science/hal-05485299>.

- [19] A. Bariant, J. Baudrin, G. Leurent, C. Pernot, L. Perrin and T. Peyrin. ‘Corrigendum to Fast AES-Based Universal Hash Functions and MACs’. In: *IACR Transactions on Symmetric Cryptology* 2025.1 (7th Mar. 2025), pp. 623–628. DOI: [10.46586/tosc.v2025.i1.623-628](https://doi.org/10.46586/tosc.v2025.i1.623-628). URL: <https://inria.hal.science/hal-05468291>.
- [20] J. Baudrin, C. Beierle, P. Felke, G. Leander, P. Neumann, L. Perrin and L. Stennes. ‘Commutative Cryptanalysis as a Generalization of Differential Cryptanalysis’. In: *Designs, Codes and Cryptography* 93.8 (10th May 2025), pp. 3243–3281. DOI: [10.1007/s10623-025-01625-9](https://doi.org/10.1007/s10623-025-01625-9). URL: <https://inria.hal.science/hal-05519430>.
- [21] C. Boura, G. Couteau, L. Perrin and Y. Rotella. ‘SoK: On Shallow Weak PRFs’. In: *IACR Transactions on Symmetric Cryptology* 2025.3 (25th Sept. 2025), pp. 289–336. DOI: [10.46586/tosc.v2025.i3.289-336](https://doi.org/10.46586/tosc.v2025.i3.289-336). URL: <https://hal.science/hal-05379116>.
- [22] A. Chailloux and T. Debris-Alazard. ‘New Solutions to Delsarte’s Dual Linear Programs’. In: *IEEE Transactions on Information Theory* 71.1 (Jan. 2025), pp. 297–316. DOI: [10.1109/TIT.2024.3476974](https://doi.org/10.1109/TIT.2024.3476974). URL: <https://inria.hal.science/hal-04884027>.
- [23] A. Chakraborti, S. Ghosh, T. Isobe and S. Kundu. ‘EWEMrl: A White-Box Secure Cipher with Longevity’. In: *IACR Communications in Cryptology* 2.4 (8th Jan. 2026). DOI: [10.62056/ak2i5wol7](https://doi.org/10.62056/ak2i5wol7). URL: <https://inria.hal.science/hal-05472568>.
- [24] N. Datta, A. Dutta, S. Ghosh, E. List and H. Nandi. ‘HCTR+: An Optimally Secure TBC-Based Accordion Mode’. In: *IACR Transactions on Symmetric Cryptology* 2025.3 (25th Sept. 2025), pp. 183–229. DOI: [10.46586/tosc.v2025.i3.183-229](https://doi.org/10.46586/tosc.v2025.i3.183-229). URL: <https://inria.hal.science/hal-05466306>.
- [25] P. Derbez, B. Germon, B. Michel and M. Naya Plasencia. ‘Improved Cryptanalysis of GIFT-64’. In: *IACR Transactions on Symmetric Cryptology* 2025.4 (2025), pp. 284–307. DOI: [10.46586/tosc.v2025.i4.284-307](https://doi.org/10.46586/tosc.v2025.i4.284-307). URL: <https://hal.science/hal-05432869>.
- [26] T. Hillmann, G. Dauphinais, I. Tzitrin and M. Vasmer. ‘Single-shot and measurement-based quantum error correction via fault complexes’. In: *Physical Review A* 112.4 (9th Oct. 2025), p. L040401. DOI: [10.1103/cjb4-157n](https://doi.org/10.1103/cjb4-157n). URL: <https://hal.science/hal-05368432>.
- [27] A. K. Kundu, S. Ghosh, A. Aikata and D. Saha. ‘ToFA: Towards Fault Analysis of GIFT and GIFT-like Ciphers Leveraging Truncated Impossible Differentials’. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025.3 (5th June 2025), pp. 614–643. DOI: [10.46586/tches.v2025.i3.614-643](https://doi.org/10.46586/tches.v2025.i3.614-643). URL: <https://inria.hal.science/hal-05466295>.
- [28] A. Lemoine, R. Mora and J.-P. Tillich. ‘Understanding the new distinguisher of alternating codes at degree 2’. In: *Designs, Codes and Cryptography* 93.8 (19th Apr. 2025), pp. 3083–3105. DOI: [10.1007/S10623-025-01626-8](https://doi.org/10.1007/S10623-025-01626-8). URL: <https://inria.hal.science/hal-05461754>.
- [29] G. Leurent and C. Mathéus. ‘Generic Attacks on Double Block Length Sponge Hashing’. In: *IACR Transactions on Symmetric Cryptology* 2025.4 (17th Dec. 2025), pp. 262–283. DOI: [10.46586/tosc.v2025.i4.262-283](https://doi.org/10.46586/tosc.v2025.i4.262-283). URL: <https://inria.hal.science/hal-05517858>.
- [30] A. Leverrier. ‘Bosonic quantum Fourier codes’. In: *Quantum* 10 (9th Feb. 2026), p. 2000. DOI: [10.22331/q-2026-02-09-2000](https://doi.org/10.22331/q-2026-02-09-2000). URL: <https://inria.hal.science/hal-05503264>.
- [31] A. Leverrier and G. Zémor. ‘Efficient Decoding up to a Constant Fraction of the Code Length for Asymptotically Good Quantum Codes’. In: *ACM Transactions on Algorithms* 21.4 (8th Sept. 2025), pp. 1–34. DOI: [10.1145/3663763](https://doi.org/10.1145/3663763). URL: <https://inria.hal.science/hal-05462487>.
- [32] M. Nageler, S. Ghosh, M. Jüttler and M. Eichlseder. ‘AutoDiVer: Automatically Verifying Differential Characteristics and Learning Key Conditions’. In: *IACR Transactions on Symmetric Cryptology* 2025.1 (7th Mar. 2025), pp. 471–514. DOI: [10.46586/tosc.v2025.i1.471-514](https://doi.org/10.46586/tosc.v2025.i1.471-514). URL: <https://inria.hal.science/hal-05519472>.
- [33] D. Ruiz, J. Guillaud, A. Leverrier, M. Mirrahimi and C. Vuillot. ‘LDPC-cat codes for low-overhead quantum computing in 2D’. In: *Nature Communications* 16.1 (26th Jan. 2025), p. 1040. DOI: [10.1038/s41467-025-56298-8](https://doi.org/10.1038/s41467-025-56298-8). URL: <https://inria.hal.science/hal-04887011>.

Invited conferences

- [34] J. Baudrin, A. Canteaut and L. Perrin. ‘On the structure of the known infinite families of APN functions’. In: *Boolean Functions and their Applications (BFA 2025)*. Larnaca, Cyprus, 1st Sept. 2025. URL: <https://inria.hal.science/hal-05488152>.
- [35] A. Canteaut. ‘Stream Ciphers Strike Back’. In: *FSE 2025 - Fast Software Encryption*. Rome, Italy, 17th Mar. 2025. URL: <https://inria.hal.science/hal-05488149>.
- [36] A. Canteaut and M. Fruchon. ‘Understanding Unexpected Fixed-Key Differential Behaviours’. In: *GelreCrypt 2025 workshop*. Nijmegen, Netherlands, 4th Nov. 2025. URL: <https://inria.hal.science/hal-05488154>.
- [37] L. Perrin. ‘On the Design Criteria for Symmetric Primitives’. In: *(C2) 2025 - Journées Codage et Cryptographie*. Pornichet, France, 30th Mar. 2025. URL: <https://inria.hal.science/hal-05470248>.
- [38] L. Perrin. ‘What happens when you *don’t* have tools? The case of algebraic cryptanalysis’. In: *SKCAM 2025 - Workshop on Symmetric-key Cryptanalysis Automation and Modelling*. Rome, Italy, 15th Mar. 2025. URL: <https://inria.hal.science/hal-05467908>.

International peer-reviewed conferences

- [39] S. Arpin, J. B. Lau, A. Mesnard, R. Perlmeyer, A. Robinson, J.-P. Tillich and V. Vasseur. ‘Error floor prediction with Markov models for QC-MDPC codes’. In: *Lecture Notes in Computer Science. CRYPTO 2025 - 45th Annual International Cryptology Conference*. Vol. LNCS-16000. Part I. Santa Barbara, United States: Springer Verlag, 17th Aug. 2025, pp. 221–252. DOI: [10.1007/978-3-032-01855-7_8](https://doi.org/10.1007/978-3-032-01855-7_8). URL: <https://inria.hal.science/hal-05461501>.
- [40] A. Bariant, A. Boeuf, P. Briaud, M. Hostettler, M. Øyegarden and H. Raddum. ‘Improved resultant attack against arithmetization-oriented primitives’. In: *CRYPTO 2025: 45th Annual International Cryptology Conference*. CRYPTO 2025 - 45th Annual International Cryptology Conference. Vol. 16004. Lecture Notes in Computer Science. Santa Barbara, CA, United States: Springer Nature Switzerland, 17th Aug. 2025, pp. 335–367. DOI: [10.1007/978-3-032-01901-1_11](https://doi.org/10.1007/978-3-032-01901-1_11). URL: <https://inria.hal.science/hal-05233805>.
- [41] J. Baudrin, S. Belaid, N. Bon, C. Boura, A. Canteaut, G. Leurent, P. Paillier, L. Perrin, M. Rivain, Y. Rotella and S. Tap. ‘Transistor: a TFHE-Friendly Stream Cipher’. In: *Lecture Notes in Computer Science. CRYPTO 2025 - 45th Annual International Cryptology Conference*. Vol. LNCS-16004. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 17th Aug. 2025, pp. 530–565. DOI: [10.1007/978-3-032-01901-1_17](https://doi.org/10.1007/978-3-032-01901-1_17). URL: <https://hal.science/hal-05258560>.
- [42] Y. Belkheyar, P. Derbez, S. Ghosh, G. Leander, S. Mella, L. Perrin, S. Rasoolzadeh, L. Stennes, S. Sun, G. van Assche and D. Vizár. ‘ChiLow and ChiChi: New Constructions for Code Encryption’. In: *EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS-15601. Lecture Notes in Computer Science. Madrid, Spain: Springer Nature Switzerland, 27th Apr. 2025, pp. 212–243. DOI: [10.1007/978-3-031-91107-1_8](https://doi.org/10.1007/978-3-031-91107-1_8). URL: <https://hal.science/hal-05435256>.
- [43] C. Bouette, L. Luzzi and M. Bloch. ‘Covert Capacity of AWGN Channels under Average Error Probability’. In: *ISIT 2025 - IEEE International Symposium on Information Theory*. Ann Arbor, MI, USA, United States, 23rd June 2025. DOI: [10.1109/ISIT63088.2025.11195632](https://doi.org/10.1109/ISIT63088.2025.11195632). URL: <https://hal.science/hal-05118024>.
- [44] C. Boura, P. Derbez, B. Germon, R. H. Boissier and M. Naya Plasencia. ‘SPEEDY: Caught at Last’. In: *LNCS. ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security*. Vol. LNCS-16245. Lecture Notes in Computer Science. Melbourne, Australia: Springer Nature Singapore, 8th Dec. 2025, pp. 189–220. DOI: [10.1007/978-981-95-5018-0_7](https://doi.org/10.1007/978-981-95-5018-0_7). URL: <https://hal.science/hal-05461455>.

- [45] A. Canteaut and M. Fruchon. ‘Understanding Unexpected Fixed-Key Differential Behaviours: How to Avoid Major Weaknesses in Lightweight Designs’. In: *LNCS. ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security*. Vol. LNCS-16245. LNCS. Melbourne, Australia: Springer, 8th Dec. 2025. DOI: [10.1007/978-981-95-5018-0_4](https://doi.org/10.1007/978-981-95-5018-0_4). URL: <https://inria.hal.science/hal-05466832>.
- [46] K. Carrier, C. Meyer-Hilfiger, Y. Shen and J.-P. Tillich. ‘Assessing the Impact of a Variant of MATZOV’s Dual Attack on Kyber’. In: *Lecture Notes in Computer Science. CRYPTO 2025 - 45th Annual International Cryptology Conference*. Vol. 16000. Santa Barbara, United States: Springer, 2025, pp. 1–36. DOI: [10.1007/978-3-032-01855-7_15](https://doi.org/10.1007/978-3-032-01855-7_15). URL: <https://hal.science/hal-05406481>.
- [47] A. Chailloux and J.-P. Tillich. ‘Quantum Advantage from Soft Decoders’. In: *STOC 2025 - 57th Annual ACM Symposium on Theory of Computing*. Prague, Czech Republic: ACM, 23rd June 2025, pp. 738–749. DOI: [10.1145/3717823.3718319](https://doi.org/10.1145/3717823.3718319). URL: <https://inria.hal.science/hal-05462301>.
- [48] A. Flórez-Gutiérrez, E. Lambooj, G. Leurent, H. Raddum, T. Tiessen and M. Verbauwhede. ‘Cryptanalysis of Full SCARF’. In: *Lecture Notes in Computer Science. EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Vol. 15601. Madrid, Spain: Springer Nature Switzerland, 27th Apr. 2025, pp. 397–426. DOI: [10.1007/978-3-031-91107-1_14](https://doi.org/10.1007/978-3-031-91107-1_14). URL: <https://inria.hal.science/hal-05468322>.
- [49] B. C. A. Freire, N. Delfosse and A. Leverrier. ‘Optimizing Hypergraph Product Codes with Random Walks, Simulated Annealing and Reinforcement Learning’. In: *ISIT 2025 - IEEE International Symposium on Information Theory*. Ann Arbor, United States: IEEE, 22nd June 2025, pp. 1–6. DOI: [10.1109/ISIT63088.2025.11195424](https://doi.org/10.1109/ISIT63088.2025.11195424). URL: <https://inria.hal.science/hal-05462468>.
- [50] D. M’foukh, M. Naya-Plasencia and P. Neumann. ‘The State-Test Technique on Differential Attacks: a 26-Round Attack on Craft and Other Applications’. In: *Lecture Notes in Computer Science. ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 16245. Melbourne, Australia: Springer Nature Singapore, 8th Dec. 2025, pp. 253–284. DOI: [10.1007/978-981-95-5018-0_9](https://doi.org/10.1007/978-981-95-5018-0_9). URL: <https://hal.science/hal-05465366>.

Conferences without proceedings

- [51] J. Baudrin, A. Canteaut and L. Perrin. ‘On the structure of the known infinite families of APN functions’. In: *Arithmetic, Geometry, Cryptography and Coding Theory - AGCCT 2025*. Luminy, France, 9th June 2025. URL: <https://inria.hal.science/hal-05488153>.
- [52] J. Baudrin, P. Galissant and L. Perrin. ‘Exploring the Set of APN Functions’. In: *BFA 2025 - 10th International Workshop on Boolean Functions and their Applications*. Larnaca, Cyprus, 1st Sept. 2025. URL: <https://hal.science/hal-05376704>.
- [53] O. Fawzi, J. Kochanowski, C. Rouzé and T. van Himbeek. ‘Additivity and chain rules for quantum entropies via multi-index Schatten norms’. In: *TQC 2025 - Theory of Quantum Computation, Communication and Cryptography*. Bangalore, India, 2025. URL: <https://hal.science/hal-05459272>.

Doctoral dissertations and habilitation theses

- [54] V. Guémard. ‘Lifts of Quantum CSS Codes - New Constructions Beyond Product Codes’. Aix-Marseille Université, 28th Nov. 2025. URL: <https://hal.science/tel-05463525>.
- [55] C. Meyer-Hilfiger. ‘Design and analysis of dual attacks in code- and lattice-based cryptography’. Sorbonne Université, 30th Sept. 2025. URL: <https://theses.hal.science/tel-05464358>.

Reports & preprints

- [56] Q. Buzet and A. Chailloux. *Fine-Grained Unambiguous Measurements*. 4th Nov. 2025. URL: <https://inria.hal.science/hal-05466830>.
- [57] A. Chailloux. *OPI × Soft Decoders*. 1st Dec. 2025. URL: <https://inria.hal.science/hal-05468050>.

- [58] A. Chailloux and P. Hermouet. *On the Quantum Equivalence between $S(LWE)$ and ISIS*. 7th Oct. 2025. URL: <https://inria.hal.science/hal-05468056>.
- [59] O. Dunkelmann, E. Lambooi and G. Leurent. *Note: Full-round distinguisher for Synergy*. 20th Jan. 2026. URL: <https://inria.hal.science/hal-05468328>.
- [60] E. Dyrenkova, R. Laflamme and M. Vasmer. *Scalable Simulation of Fermionic Encoding Performance on Noisy Quantum Computers*. 2025. URL: <https://hal.science/hal-05467890>.
- [61] O. Fawzi, J. Kochanowski, C. Rouzé and T. van Himbeek. *Additivity and chain rules for quantum entropies via multi-index Schatten norms*. 2025. URL: <https://hal.science/hal-05335881>.
- [62] V. Guemard. *Lifting a CSS code via its handlebody realization*. 2025. DOI: [10.48550/arXiv.2505.14327](https://doi.org/10.48550/arXiv.2505.14327). URL: <https://hal.science/hal-05463476>.
- [63] V. Guémard. *Good quantum codes with addressable and parallelizable non-Clifford gates*. 10th Dec. 2025. URL: <https://hal.science/hal-05463484>.
- [64] V. Guémard and G. Zémor. *Moderate-length lifted quantum Tanner codes*. 17th Nov. 2025. URL: <https://hal.science/hal-05463467>.
- [65] A. Lemoine. *The tangent space attack*. 29th Apr. 2025. URL: <https://hal.science/hal-05069034>.
- [66] L. Paletta, A. Leverrier, M. Mirrahimi and C. Vuillot. *High-performance local decoders for defect matching in 1D*. 14th Nov. 2025. URL: <https://inria.hal.science/hal-05364617>.
- [67] A. Pesah, A. K. Daniel, I. Tzitrin and M. Vasmer. *Fault-tolerant transformations of spacetime codes*. 19th Dec. 2025. URL: <https://hal.science/hal-05425964>.
- [68] C. Piveteau and J. M. Renes. *Efficient and optimal quantum state discrimination via quantum belief propagation*. 2025. DOI: [10.48550/arXiv.2509.19441](https://doi.org/10.48550/arXiv.2509.19441). URL: <https://hal.science/hal-05467914>.
- [69] A. Ray, E. Swaroop, N. Cao, M. Vasmer and A. Chowdhury. *Quasiprobabilistic imaginary-time evolution on quantum computers*. 2025. URL: <https://hal.science/hal-05467880>.
- [70] M. Salom, N. Sendrier and V. Vasseur. *Sparse Vector Reconstruction from Distance Spectrum using Soft Information*. 20th Jan. 2026. URL: <https://inria.hal.science/hal-05466728>.

Other scientific publications

- [71] B. Daumen. ‘Practical Study on Solving Polynomial Systems corresponding to Algebraic Attacks on Symmetric Primitives’. Master Parisien de Recherche en Informatique (MPRI), École Polytechnique, 8th Sept. 2025. URL: <https://inria.hal.science/hal-05468019>.
- [72] C. Mathéus. ‘Internship Report -MPRI M2 Generic Attacks on Sponge Based Hash Combiners’. Télécom Paris, 8th Sept. 2025. URL: <https://inria.hal.science/hal-05518009>.

12.3 Cited publications

- [73] M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. V. Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson and W. Wang. *Classic McEliece: conservative code-based cryptography*. Round 4 submission to the NIST call for postquantum cryptographic primitives. Oct. 2022. URL: <https://inria.hal.science/hal-04288769> (cit. on p. 10).
- [74] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta and J.-P. Tillich. ‘An Algebraic Attack on Rank Metric Code-Based Cryptosystems’. In: *EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Vol. 12107. Lecture Notes in Computer Science. Zagreb / Virtual, Croatia: Springer, May 2020, pp. 64–93. DOI: [10.1007/978-3-030-45727-3_3](https://doi.org/10.1007/978-3-030-45727-3_3). URL: <https://hal-unilim.archives-ouvertes.fr/hal-02303015> (cit. on p. 9).

- [75] 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’. In: *ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 12491. Lecture Notes in Computer Science. Daejeon / Virtual, South Korea: Springer, Dec. 2020, pp. 507–536. DOI: [10.1007/978-3-030-64837-4_17](https://doi.org/10.1007/978-3-030-64837-4_17). URL: <https://hal.inria.fr/hal-03133479> (cit. on p. 9).
- [76] M. Bardet, R. Mora and J.-P. Tillich. ‘Polynomial time key-recovery attack on high rate random alternant codes’. In: *IEEE Transactions on Information Theory* 70.6 (June 2024), pp. 4492–4511. DOI: [10.1109/TIT.2023.3334592](https://doi.org/10.1109/TIT.2023.3334592). URL: <https://inria.hal.science/hal-04276519> (cit. on p. 10).
- [77] A. Couvreur and M. Lequesne. ‘On the security of subspace subcodes of Reed-Solomon codes for public key encryption’. In: *IEEE Transactions on Information Theory* 68.1 (Oct. 2021), pp. 632–648. DOI: [10.1109/TIT.2021.3120440](https://doi.org/10.1109/TIT.2021.3120440). URL: <https://hal.science/hal-02938812> (cit. on p. 10).
- [78] A. Couvreur, R. Mora and J.-P. Tillich. ‘A new approach based on quadratic forms to attack the McEliece cryptosystem’. In: *Advances in Cryptology - ASIACRYPT 2023*. Vol. 14441. Lecture Notes in Computer Science. 68 pages (Long version). Guo, J. and Steinfeld, R. Guangzhou, China: Springer Nature Singapore, Dec. 2023, pp. 3–38. DOI: [10.1007/978-981-99-8730-6_1](https://doi.org/10.1007/978-981-99-8730-6_1). URL: <https://inria.hal.science/hal-04215135> (cit. on p. 10).
- [79] R. Mora and J.-P. Tillich. ‘On the dimension and structure of the square of the dual of a Goppa code’. In: *Designs, Codes and Cryptography* 91.4 (Nov. 2022), pp. 1351–1372. DOI: [10.1007/s10623-022-01153-w](https://doi.org/10.1007/s10623-022-01153-w). URL: <https://inria.hal.science/hal-03919898> (cit. on p. 10).