RESEARCH CENTRE

Inria Paris Centre

2023 ACTIVITY REPORT

Project-Team COSMIQ

Code-based Cryptology, Symmetric Cryptology and Quantum Information

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team COSMIQ

Creation of the Project-Team: 2019 December 01

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

1 Team members, visitors, external collaborators

Research Scientists

- Jean-Pierre Tillich [Team leader, INRIA, Senior Researcher, HDR]
- Ivan Bardet [INRIA, Starting Research Position, until Jan 2023]
- Anne Canteaut [INRIA, Senior Researcher, HDR]
- Andre Chailloux [INRIA, Researcher]
- Pascale Charpin [INRIA, Emeritus, HDR]
- Nicholas Connolly [INRIA, Starting Research Position, until Aug 2023]
- Gaetan Leurent [INRIA, Researcher, HDR]
- Anthony Leverrier [INRIA, HDR]
- María Naya Plasencia [INRIA, Senior Researcher, HDR]
- Leo Perrin [INRIA, Researcher]
- Nicolas Sendrier [INRIA, Senior Researcher, HDR]

PhD Students

- Augustin Bariant [INRIA, until Nov 2023]
- Jules Baudrin [INRIA]
- Agathe Blanvillain [INRIA, from Oct 2023]
- Aurelien Boeuf [INRIA]
- Clémence Bouvier [SORBONNE UNIVERSITE, until Nov 2023]
- Pierre Briaud [SORBONNE UNIVERSITE, until Sep 2023]
- Nicolas David [INRIA, until Nov 2023]
- Loïc Demange [THALES, until Nov 2023]
- Aurélie Denys [INRIA]
- Simona Etinski [INRIA, until Mar 2023, Phd Student]
- Virgile Guemard [INRIA]
- Axel Lemoine [DGA, from Oct 2023]
- Johanna Loyer [INRIA]
- Dounia M'Foukh [INRIA, from Sep 2023]
- Charles Meyer-Hilfiger [INRIA]
- Rocco Mora [INRIA, until Mar 2023]
- Clara Pernot [INRIA]
- Maxime Remaud [BULL, until Nov 2023]
- Simon Richoux [DGA, from Nov 2023]

Technical Staff

- Rocco Mora [INRIA, Engineer, from Apr 2023 until Oct 2023]

Interns and Apprentices

- Agathe Blanvillain [INRIA, Intern, from Apr 2023 until Sep 2023]
- Axel Lemoine [DGA, Intern, from Mar 2023 until Aug 2023]
- Dounia M'Foukh [INRIA, Intern, from Mar 2023 until Aug 2023]
- Roman Randrianarisoa [INRIA, Intern, from Aug 2023 until Sep 2023]
- Fanny Terrier [INRIA, Intern, from Mar 2023 until Aug 2023]

Administrative Assistants

- Christelle Guiziou [INRIA]
- Christelle Rosello [INRIA, from Apr 2023]

External Collaborators

- Christina Boura [UVSQ, HDR]
- Yann Rotella [UVSQ]
- Valentin Vasseur [THALES]
- Thomas Vidick [CALTECH]

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 20 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. NIST has anounced in 2021 that this call for postquantum primitives would be extended specifically for digital signatures based on techniques other than lattices. This new call should be released in the first quarter of 2022.

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 are also preparing to submit Wave to the new code-based signature whose deadline is June 1, 2023.

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.

At the moment, we are 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 competition[1] 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. It is expected to have a huge and long-term impact on all public-key cryptography. It has received 69 proposals in November 2017, among which five have been co-designed by the project-team. Four of them have made it to the second round in January 2019. One of them was chosen in July 2020 for the third round and another one was chosen as an alternate third round finalist. We have also broken two first round candidates EDON-K [90] and RANKSIGN [89], and have devised a partial break of the RLCE encryption scheme [88]. In 2020, we obtained a significant breakthrough in solving more efficiently the MinRank problem and the decoding problem in the rank metric [86, 87] by using algebraic techniques. This had several consequences: all second round rank metric candidates were dismissed 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.

NIST competition on lightweight symmetric encryption.

The NIST lightweight cryptography standardization process[2] 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 have been co-designed by members of the team. Furthermore, one of the 10 finalists was co-designed by a member 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 unsage. 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.

[1] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[2] Website of the NIST project.

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.

5 Highlights of the year

5.1 Awards

Irène Joliot-Curie Prize 2023

Anne Canteaut was awarded by the French Academy of Sciences the "Female Scientist of the Year" prize. This prize distinguishes one senior woman scientist per year among all disciplines. www.academie-sciences.fr/Laureats/

Online-audience award, “My thesis in 180 seconds”, Sorbonne Université

Clémence Bouvier, 2023,

EDITE PhD thesis second prize, [58]

Clémence Bouvier, Cryptanalysis and design of symmetric primitives defined over large finite fields, Sorbonne Université, 2023

6 New software, platforms, open data

6.1 New software

6.1.1 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/`

Authors: Nicolas Sendrier, Thomas Debris

Contact: Nicolas Sendrier

6.1.2 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

Participants: Grégory Landais, Nicolas Sendrier

7 New results

7.1 Quantum algorithms and cryptanalysis

Participants: Ritam Bhaumik, André Chailloux, Nicolas David, Simona Etinski, Antonio Flórez-Gutiérrez, Paul Frixons, Gaëtan Leurent, Johanna Loyer, María Naya-Plasencia, Maxime Remaud, Jean-Pierre Tillich.

We have kept on working on symmetric quantum cryptanalysis and generic quantum algorithms related to cryptanalysis, and in addition, started looking at some asymmetric cryptanalysis problems in lattice based cryptography or isogeny based cryptography.

7.2 Symmetric cryptology

Participants: Augustin Bariant, Jules Baudrin, Ritam Bhaumik, Aurélien Boeuf, Clémence Bouvier, Anne Canteaut, Pascale Charpin, Daniel Coggia, Nicolas David, Gaëtan Leurent, María Naya-Plasencia, Clara Pernot, Léo Perrin.

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.

7.3 Post-quantum asymmetric cryptology

Participants: Pierre Briaud, André Chailloux, Loïc Demange, Charles Meyer-Hilfiger, Rocco Mora, Maxime Remaud, 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).

7.4 Quantum information

Participants: Ivan Bardet, André Chailloux, Aurélie Denys, Lucien Grouès, Virgile Guémard, Anthony Leverrier, Andrea Olivo.

Most of our work in quantum information deals with either quantum algorithms, quantum error correction or cryptography.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

LOTUS:(01/2021 -> 31/12/2023) Contract with Thales for a survey on the implementation of code-based post-quantum cryptosystems.
45 kEuros.

8.2 Bilateral grants with industry

- **Bull-ATOS** (07/2020 -> 06/2023) Funding for the supervision of Maxime Rémaud's PhD.
  60 kEuros.
- **Thalès** (11/2020 -> 10/2023) Funding for the supervision of Loïc Demange's PhD.
  45 kEuros.

9 Partnerships and cooperations

9.1 International initiatives

9.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program

COSINUS Associate team between COSMIQ and Simula UiB (Bergen, Norway).
The aim of the team is to investigate the design and analysis of symmetric primitives operating over large and/or prime fields.

9.2 International research visitors

9.2.1 Visits of international scientists

Inria International Chair

Participants: Thomas Vidick.

Other international visits to the team

Carlos Cid

Status researcher

Institution of origin: Simula UIB

Country: Norway

Dates: November 6- November 9

Context of the visit: visit in the framework of the associate COSINUS team

Haavard Raddum

Status researcher

Institution of origin: Simula UIB

Country: Norway

Dates: November 6- November 10

Context of the visit: visit in the framework of the associate COSINUS team

Manterola Ayala

Status PhD

Institution of origin: Simula UIB

Country: Norway

Dates: November 6- November 10

Context of the visit: visit in the framework of the associate COSINUS team

Atharva Phanse

Status PhD

Institution of origin: Simula UIB

Country: Norway

Dates: November 6- November 10

Context of the visit: visit in the framework of the associate COSINUS team

9.2.2 Visits to international teams

Research stays abroad

Visit to Simula

Participants: Aurélien Boeuf, Clémence Bouvier, Axel Lemoine, Leo Perrin.

Visited institution: Simula

Country: Norway

Dates: June 13- June 16

Context of the visit: in the framework of the COSINUS associate team with Simula UIB. Leo Perrin, Aurélien Boeuf, Clémence Bouvier and Axel Lemoine went for one week to work on the design and cryptanalysis of symmetric primitives operating over large and/or prime fields.

Mobility program/type of mobility: Associate team with Simula.

Visit to the University of Rostock

Participants: Clémence Bouvier, Leo Perrin.

Visited institution: University of Rostock

Country: Germany

Dates: June 5- June 9

Context of the visit: Work with Pr. Gohar Kyureghyan.

Mobility program/type of mobility: NA.

9.3 European initiatives

9.3.1 Horizon Europe

ReSCALE ReSCALE project on 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: Léo Perrin

Coordinator: Léo Perrin

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>2̂64. 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 were 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."

ERC QUASYModo

Title: QUASYModo *Symmetric Cryptography in the Post-Quantum World*

Duration: From September 1, 2017 to August 31, 2023

Partners:

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

Inria contact: María Naya Plasencia

Coordinator: María Naya Plasencia

Total amount: 1.33 MEuros

Summary: Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which had not been studied prior to our project. This is the big gap we have been filling during the last 6 years thanks to QUASYModo. We have also proposed efficient solutions secure in the post-quantum world with the help of our previously obtained quantum symmetric cryptanalysis toolbox. The main challenge of QUASYModo was to redesign symmetric cryptography for the post-quantum world.

9.3.2 Digital Europe

QuantERA QUANTAGENOMICS

Title: QUANTAGENOMICS *Quantum Enabled Secure Multiparty Computation for Genomic Medicine*

Program: QuantERA ERA-NET Cofund

Duration: May 2022 - April 2025

Partners: Instituto de Telecomunicações (Portagal), Sorbonne Université (France), Inria de Paris, Ophiomics (Portugal), UPM (Spain), ICFO (Spain),

Total amount: 1 MEuros

Summary: QuantaGenomics is a QuantERA ERA-NET Cofund in Quantum Technologies project with focus on the development of a quantum-enabled secure multiparty computation service for collaborative genomic medicine. In this project, we are going to replace the classical oblivious transfer(OT) implementation by a quantum-enabled OT in a secure multiparty computation (SMC) protocol, leading to a solution that is both fast and secure, even against quantum computer attacks. On top of the quantum-enabled SMC protocol, we are going to develop a privacy-preserving data mining service involving a particular genomic medicine use case.

9.4 National initiatives

- **ANR SWAP** (02/22→01/26)
  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(https://www.pepr-cybersecurite.fr), 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.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair

- STAP'23: Apr 2023, Lyon, France (workshop co-located with Eurocrypt'23): L. Perrin (general chair)

10.1.2 Scientific events: selection

Chair of conference program committees

- IEEE ITW 2023, Apr. 2023, St-Malo, France: A. Canteaut (co-chair)
- WCC 2024, June 2024, Perugia, Italy: M. Naya Plasencia (co-chair)
- Dagstuhl seminar on Quantum Cryptanalysis, Oct. 2023: M. Naya-Plasencia (co-organizer)
- Dagstuhl seminar on Symmetric Cryptography, Jan. 2024: M. Naya-Plasencia (co-organizer)

Steering Committees.

- *Fast Software Encryption (FSE)*, A. Canteaut (chair, 2014–2023), M. Naya-Plasencia (member 2016–2023), G. Leurent (member since 2019)
- *Post-quantum cryptography (PQCrypto)*, N. Sendrier, J.-P. Tillich
- *Workshop on Coding and Cryptography (WCC)*, P. Charpin, N. Sendrier, J.-P. Tillich

Member of the conference program committees

Anne Canteaut:

- Eurocrypt: 2024
- Crypto: 2024
- FSE: 2024
- ITW: 2023 (co-chair)

Pascale Charpin:

- WCC: 2024

Gaëtan Leurent:

- Eurocrypt: 2023
- Crypto: 2024

Anthony Leverrier:

- QIP: 2023
- AQIS: 2023

María Naya Plasencia:

- Eurocrypt: 2024 (area chair)
- Asiacrypt: 2023
- WCC: 2024 (co-chair)
- CFail: 2021

Léo Perrin:

- Crypto: 2023
- Eurocrypt: 2023
- WCC: 2024

Nicolas Sendrier:

- Indocrypt: 2023
- PQCrypto: 2023, 2024
- SAC: 2023
- WCC: 2024

Jean-Pierre Tillich:

- AAC' 24: 2024
- Asiacrypt: 2023
- ISIT: 2023
- ITW: 2023
- PKC: 2023
- PQCrypto: 2023, 2024
- WCC: 2024

10.1.3 Journal

Editorial boards

- *Advances in Mathematics for Communications*, associate editors : N. Sendrier (since 2018), J.-P. Tillich (since 2017)
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut (since 2016)
- *Designs, Codes and Cryptography*, associate editors: P. Charpin (since 2003), M. Naya Plasencia (since 2020)
- *Finite Fields and Their Applications*, associate editors: A. Canteaut, P. Charpin (since 2013)
- *IACR Transactions on Symmetric Cryptology*, co-editor-in-chief: G. Leurent (2019–20); other members of the editorial board: A. Canteaut (2019–20, 2023), G. Leurent (2022), M. Naya-Plasencia (2019–20), L. Perrin (2019–22)
- *IACR Transactions on Cryptographic Hardware and Embedded Systems*, member of the editorial board: G. Leurent (2019)
- *IEEE Transactions on Information Theory*, A. Canteaut: area editor (since 2021), associate editor (2018–20), A. Leverrier: associate editor (since 2023)
- *Journal of Cryptology*, A. Canteaut (since 2021)
- *Quantum Journal*, associate editor: A. Leverrier (2018–22).

10.1.4 Invited talks

- J.-P. Tillich, “Recent algebraic attacks on the McEliece cryptosystem”, invited talk at Finite Fields and Their Applications 2023 (Fq15), Jun 21, 2023
- A. Canteaut, “The Unbearable Lightness of Symmetric Primitives”, Invited talk at Africacrypt 2023, July 18, 2023
- J.-P. Tillich, “Recent algebraic attacks on the McEliece cryptosystem”, invited talk at PQCrypto 2023, August
- G. Leurent, “Cryptanalysis Beyond Primitives”, FSE 2024 keynote talk, Leuven, March 25-29 2024

10.1.5 Scientific expertise

A. Canteaut, G. Leurent, M. Naya Plasencia and L. Perrin have been asked to analyze the security of some primitives to be deployed by some blockchain providers. Back in 2019 A. Canteaut brought together and led a group of several international researchers to compare the security levels offered by some STARK-friendly hash functions, as a consulting activity group for Starkware. A similar study focusing on RESCUE was then commissioned by the German compagny *cryptosolutions*. In 2023, the Ethereum Fondation organized an event with a group of international experts to analyze the candidate sequential function MINROOT; they asked G. Leurent and M. Naya Plasencia to lead one the groups, and also invited A. Canteaut, and L. Perrin to participate [75]. In each case, our expertise was needed to choose the appropriate solutions for their products.

10.1.6 Research administration

Committees for the selection of professors, assistant professors and researchers.

- Inria, Senior Research Scientists (DR): A, Canteaut (2019, chair 2020–23), M. Naya Plasencia (2020–23)
- Inria Nancy, Junior Research Scientists (CR/ISFP): M. Naya-Plasencia (2023)
- Inria, Admission Committee, DR and CR: A. Canteaut (2020–23)
- Université de Limoges, Assistant Professor, N. Sendrier (2023)

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

- Master: A. Canteaut, Error-correcting codes and applications to cryptology, 12 hours, M2, University Paris-Diderot (MPRI), France;
- Master: A. Chailloux, Quantum Circuits and Logic Gates, 12 hours, M1, Sorbonne Université
- Master: A. Chailloux, Quantum information, 12 hours, M2, University Paris-Diderot (MPRI), France;
- Master: A. Chailloux, Quantum algorithms, 4 hours, M2, Ecole Normale Supérieure de Lyon, France;
- Master: A. Leverrier, Quantum information theory, 12 hours, M2, Ecole Normale Supérieure (ICFP), France;
- Master: L. Perrin, Application Web et Sécurité, 24 hours, M1, UVSQ, France;
- Bachelor: L. Perrin, Cryptographie, 29 hours, L3, UVSQ, France;
- Master: J.-P. Tillich, Introduction to Information Theory, 36 hours, M2, Ecole Polytechnique, France;
- Master: J.-P. Tillich, Quantum Information and Applications, 36 hours, M2, Ecole Polytechnique, France.

10.2.2 Supervision

- PhD: S. Etinski, Generalized Syndrome Decoding Problem and its Application to Post-Quantum Cryptography, Université Paris Cité, June 28, 2023, supervior: A. Chailloux.

- PhD: Rocco Mora, Algebraic Techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece cryptosystems, Sorbonne Université, April 7, 2023, supervisor: J.-P. Tillich.

- PhD : Nicolas David, Techniques améliorées en cryptanalyse différentielle, Sorbonne Université, November 8, 2023, supervisor: M. Naya-Plasencia.

- PhD: Maxime Remaud, Applications of Quantum Fourier Sampling and the Dihedral Hidden Subgroup Problem, Sorbonne Université, November 17, 2023, supervisor: J.-P. Tillich.

- PhD: Clémence Bouvier, Cryptanalysis and design of symmetric primitives defined over large finite fields, Sorbonne Université, November 27, 2023, supervisors: A. Canteaut, L. Perrin.

- PhD: Pierre Briaud, Algebraic Cryptanalysis of Post-Quantum Schemes and Related Assumptions, Sorbonne Université, December 11, 2023, supervisour: J.-P. Tillich.

- PhD: Johanna Loyer, Quantum Cryptanalysis on Lattices and Codes, Sorbonne Université, December 18, 2023, supervisors: A. Chailloux, N. Sendrier.

- PhD in progress: Clara Pernot, Cryptanalyse des algorithmes de cryptographie symétrique, since September 2020, supervisors: L. Perrin, M. Naya Plasencia.

- PhD in progress: Aurélie Denys, Security proofs for continuous variable quantum cryptography protocols, since October 2020, supervisor: A. Leverrier.

- PhD in progress: Loïc Demange, Implementation of BIKE, since November 2020, supervisor: N. Sendrier.

- PhD in progress: Augustin Bariant, Sécurité des algorithmes cryptographiques à bas coût, since March 2021, supervisors: A. Canteaut, G. Leurent.

- PhD in progress: Jules Baudrin, Analyse de la sécurité de primitives symétriques légères, since September 2021, supervisors: A. Canteaut, L. Perrin.

- PhD in progress: Charles Meyer-Hilfiger, Cryptographie post-quantique : Conception, analyse et mise œuvre d'algorithmes de décodage générique, since November 2021, supervisor: N. Sendrier.

- PhD in progress: Aurelien Boeuf, Analyse de la se‘curite‘ de primitives syme‘triques "Oriente‘es Arithme‘tisation", since October 2022, supervisors: A. Canteaut, L. Perrin.

- PhD in progress: Virgile, Quantum LDPC codes, since November 2022, supervisor: A. Leverrier.

- PhD in progress: Dounia M'Foukh, Symmetric cryptography, since September 2023, supervisor: M. Naya Plasencia.

- PhD in progress: A. Blanvillain, The quantum decoding problem, since October 2023, supervisor: J.-P. Tillich.

- PhD in progress: A. Lemoine, Algebraic attacks on the McEliece cryptosystem, since October 2023, supervisor: J.P. Tillich.

- PhD in progress: Simon Richoux, quantum LDPC codes, since November 2023, supervisor: A. Leverrier.

10.2.3 Juries

R. Mora, *Algebraic Techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece cryptosystems*, Sorbonne Université, April 7, 2023, committee: N. Sendrier, J.-P. Tillich (supervisor).

T. Beyne, *A geometric approach to symmetric-key cryptanalysis*, KU Leuven, Belgium, April 18, 2023, committee: A. Canteaut

S. Neves, *Security and Simulation in Modern Computer Hardware*, Universidade de Coimbra, Portugal, Mai 22, 2023, committee: M. Naya-Plasencia.

S. Etinski, *Generalized Syndrome Decoding Problem and its Application to Post-Quantum Cryptography*, Université Paris Cité, June 28, 2023, committee: A. Chailloux (supervisor), N. Sendrier.

F. Martinez, *Mathematical studies of arithmetical pseudo-random numbers generators*, Sorbonne Université, July 4, 2023, committee: M. Naya-Plasencia (chair).

L. Luzzi [HDR], *Lattices and Codes for Wireless Communications and Security*, CY Cergy Paris Université, October 12, 2023, committee: J.-P. Tillich (reviewer).

R. Lüftenegger, *Algebraic Analysis of Arithmetization-Friendly Cryptographic Primitives*, TU Graz, Austria, October 31, 2023, committee: A. Canteaut (reviewer).

T. Quan Quan, *Cryptanalysis of lightweight symmetric-key cryptographic algorithms*, NTU Singapore, Singapore, November 1, 2023, committee: M. Naya-Plasencia (reviewer).

N. David, *Techniques améliorées en cryptanalyse différentielle*, Sorbonne Université, November 8, 2023, committee: M. Naya-Plasencia (supervisor).

T. Feneuil, *Post-Quantum Signatures from Secure Multiparty Computation*, Sorbonne Université, October 23, 2023, committee: N. Sendrier (chair).

F. Göloglu [HDR], *Projective polynomials over finite fields and their applications in cryptography and combinatorics*, Charles University in Prague, Czech Republic, November 15, 2023, committee: A. Canteaut (opponent).

M. Remaud, *Applications of Quantum Fourier Sampling and the Dihedral Hidden Subgroup Problem*, Sorbonne Université, November 17, 2023, committee: M. Naya-Plasencia (chair), J.-P. Tillich (supervisor).

C. Bouvier, *Cryptanalysis and design of symmetric primitives defined over large finite fields*, Sorbonne Université, November 27, 2023, committee: A. Canteaut (supervisor), L. Perrin (supervisor).

P. Briaud, *Algebraic Cryptanalysis of Post-Quantum Schemes and Related Assumptions*, Sorbonne Université, December 11, 2023, commitee: J.-P. Tillich (supervisor).

J. Loyer, *Quantum Cryptanalysis on Lattices and Codes*, Sorbonne Université, December 18, 2023, committee: A. Chailloux (supervisor), N. Sendrier (supervisor).

A. Cheriere, *Side-Channel Resistance of Cryptographic Primitives Based on Error-Correcting Codes*, Université de Rennes, December 19, 2023, committee: N. Sendrier (reviewer).

S. Tap, *Construction de nouveaux outils de chiffrement homomorphe efficace*, Université de Rennes, December 19, 2023, committee: A. Canteaut.

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

- **Anne Canteaut.**
  - Head of *Inria Evaluation Committee*, Sep. 2019-Aug. 2023
  - International Scientific Advisory Board of the Flemish Strategic Research Program on Cybersecurity (since 2019)
- **André Chailloux.**
  - Member of *Inria Paris Scientific Hiring Committee*, since 2022
- **Gaëtan Leurent.**
  - Member of the *PhD Follow-up Committee* at Inria Paris (Comité de suivi doctoral), 2019–23.
  - (Elected) member of *Inria Evaluation Committee*, since Sep. 2023
  - Member of FSE test-of-time award Committee, 2023
- **Anthony Leverrier.**
  - Member of the Scientific Committee of the French Quantum Strategy, since Oct 2023
  - Coordinator of the Inria challenge EQIP on Quantum Technologies, 2020–24
- **María Naya Plasencia.**
  - (Elected) member of *Inria Evaluation Committee*, Sep. 2019-Aug. 2023
  - Co-chair of *Inria Paris Scientific Hiring Committee* (Assignment of PhD, postdoctoral and delegation Inria fundings), since 2022.
  - Member of the Jury of the Inria – Academie des sciences prizes, 2023.
  - Member of FSE test-of-time award Committee, 2023
  - Elected director of the IACR board, (2024–2027).
- **Léo Perrin.**
  - Member of the French delegation at ISO/IEC JTC1/SC27, in particular in the WG 2 (2019–2022)
- **Jean-Pierre Tillich.**
  - in charge of “Formation par la recherche” for the Inria Paris research center.

10.3.2 Articles and contents

General-audience papers. Anne Canteaut has written (in French): *Peut-on rêver d’une écriture impénétrable ?*, in : “Déchiffrement(s) : des hiéroglyphes à l’ADN”, Colloque annuel du Collège de France, Odile Jacob, Sep. 2023 [85][3] The members of the project-team have published several general-audience papers (in French):

Our research activities have received significant media attention, and raised several general-audience papers. A selection is given below:

- A. Canteaut: *Femmes et sciences: Anne Canteaut, lauréate de l’année, se désole de la situation*, Agence France Press, Nov. 2023[4]
- M. Naya-Plasencia : *Anticiper les attaques pour mieux sécuriser les données*, Nov. 2023[5]

[3] The talk at Collège de France is available on https://www.youtube.com/playlist?list=PL1NaqiieWs8ns6ymJxapaF3xcgoKCIdrb.

[4] https://www.france24.com/fr/info-en-continu/20231125-femmes-et-sciences-anne-canteaut-laur%C3%A9ate-de-l-ann%C3%A9e-se-d%C3%A9sole-de-la-situation

[5] https://www.inria.fr/fr/maria-naya-plasencia-anticiper-les-attaques-pour-mieux-securiser-les-donnees

11 Scientific production

11.1 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. 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. 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. 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. 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. 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. URL: https://hal.inria.fr/hal-02424057.

[7] O. Fawzi, A. Grospellier 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. URL: https://hal.archives-ouvertes.fr/hal-01895430.

[8] A. Flórez Gutiérrez, 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*. Daejeon / Virtual, South Korea, Dec. 2020. URL: https://hal.inria.fr/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. 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. 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. URL: https://hal.inria.fr/hal-02396814.

11.2 Publications of the year

International journals

[14] I. Bardet, Á. Capel, L. Gao, A. Lucia, D. Pérez-García and C. Rouzé. 'Rapid thermalization of spin chain commuting Hamiltonians'. In: *Physical Review Letters* 130.6 (9th Feb. 2023), p. 8. DOI: 10.1103/PhysRevLett.130.060401. URL: https://hal.science/hal-03538313.

[15] M. Bardet, P. Briaud, M. Bros, P. Gaborit and J.-P. Tillich. 'Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem'. In: *Designs, Codes and Cryptography* (19th July 2023). DOI: 10.1007/s10623-023-01265-x. URL: https://hal.science/hal-04193709.

[16] 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* (2023). URL: https://inria.hal.science/hal-04276519.

[17] J. Baudrin, P. Felke, G. Leander, P. Neumann, L. Perrin and L. Stennes. 'Commutative Cryptanalysis Made Practical'. In: *IACR Transactions on Symmetric Cryptology* 2023.4 (2023), pp. 299–329. DOI: 10.46586/tosc.v2023.i4.299-329. URL: https://inria.hal.science/hal-04277884.

[18] L. Bidoux, P. Briaud, M. Bros and P. Gaborit. 'RQC revisited and more cryptanalysis for Rank-based Cryptography'. In: *IEEE Transactions on Information Theory* (2023). URL: https://hal.science/hal-04276655.

[19] A. Boeuf, A. Canteaut and L. Perrin. 'Propagation of Subspaces in Primitives with Monomial Sboxes: Applications to Rescue and Variants of the AES'. In: *IACR Transactions on Symmetric Cryptology* (2023). URL: https://inria.hal.science/hal-04277002.

[20] A. Boeuf, A. Canteaut and L. Perrin. 'Propagation of Subspaces in Primitives with Monomial Sboxes: Applications to Rescue and Variants of the AES'. In: *IACR Transactions on Symmetric Cryptology* 2023.4 (8th Dec. 2023), pp. 270–298. DOI: 10.46586/tosc.v2023.i4.270-298. URL: https://hal.science/hal-04361453.

[21] C. Boura, P. Derbez and M. Funk. 'Related-Key Differential Analysis of the AES'. In: *IACR Transactions on Symmetric Cryptology* 2023.4 (8th Dec. 2023), pp. 215–243. DOI: 10.46586/tosc.v2023.i4.215-243. URL: https://hal.science/hal-04346377.

[22] C. Bouvier, A. Canteaut and L. Perrin. 'On the algebraic degree of iterated power functions'. In: *Designs, Codes and Cryptography* 91.3 (1st Mar. 2023), pp. 997–1033. DOI: 10.1007/s10623-022-01136-x. URL: https://inria.hal.science/hal-03901713.

[23] A. Chailloux and S. Etinski. 'On the (In)security of optimized Stern-like signature schemes'. In: *Designs, Codes and Cryptography* (2023). URL: https://inria.hal.science/hal-04320650.

[24] N. David, M. Naya-Plasencia and A. Schrottenloher. 'Quantum Impossible Differential Attacks: Applications to AES and SKINNY'. In: *Designs, Codes and Cryptography* (2023), pp. 1–33. DOI: 10.1007/s10623-023-01280-y. URL: https://inria.hal.science/hal-04321756.

[25] T. Debris-Alazard, L. Ducas, N. Resch and J.-P. Tillich. 'Smoothing Codes and Lattices: Systematic Study and New Bounds'. In: *IEEE Transactions on Information Theory* 69.9 (Sept. 2023), pp. 6006–6027. DOI: 10.1109/TIT.2023.3276921. URL: https://inria.hal.science/hal-04276505.

[26] T. Debris-Alazard, M. Remaud and J.-P. Tillich. 'Quantum Reduction of Finding Short Code Vectors to the Decoding Problem'. In: *IEEE Transactions on Information Theory* (2023), pp. 1–1. DOI: 10.1109/TIT.2023.3327759. URL: https://inria.hal.science/hal-04276190.

[27] A. Denys and A. Leverrier. 'The 2T -qutrit, a two-mode bosonic qutrit'. In: *Quantum* 7 (31st May 2023), p. 1032. DOI: 10.22331/q-2023-06-05-1032. URL: https://inria.hal.science/hal-04277372.

Invited conferences

[28] A. Canteaut. 'The Unbearable Lightness of Symmetric Primitives'. In: Africacrypt 2023 - 14th International Conference on Cryptology. Sousse, Tunisia, 18th July 2023. URL: https://inria.hal.science/hal-04277017.

[29] J.-P. Tillich. 'Recent algebraic attacks on the McEliece cryptosystem'. In: *Numéro spécial de Finite Fields*. International Conference on Finite Fields and Their Applications 2023 (Fq15). Aubervilliers (espace Condorcet), France, 21st June 2023. URL: https://inria.hal.science/hal-04276638.

[30] J.-P. Tillich. 'Recent algebraic attacks on the McEliece cryptosystem'. In: PQCrypto 2023. College Park, United States, 21st June 2023. URL: https://inria.hal.science/hal-04276650.

International peer-reviewed conferences

[31] A. Bariant and G. Leurent. 'Truncated Boomerang Attacks and Application to AES-Based Ciphers'. In: *LNCS - Lecture Notes in Computer Science*. EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Technique. Vol. 14007. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland, 15th Apr. 2023, pp. 3–35. DOI: 10.1007/978-3-031-30634-1_1. URL: https://inria.hal.science/hal-04277583.

[32] X. Bonnetain, A. Chailloux, A. Schrottenloher and Y. Shen. 'Finding many Collisions via Reusable Quantum Walks: Application to Lattice Sieving'. In: *Lecture Notes in Computer Science*. EUROCRYPT 2023 - International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland, 16th Apr. 2023, pp. 221–251. DOI: 10.1007/978-3-031-30589-4_8. URL: https://inria.hal.science/hal-04261002.

[33] C. Boura, N. David, P. Derbez, G. Leander and M. Naya-Plasencia. 'Differential Meet-In-The-Middle Cryptanalysis'. In: *LNCS - Lecture Notes in Computer Science*. CRYPTO 2023 - 43rd International Cryptology Conference. Vol. 14083. Lecture Notes in Computer Science. Santa Barabara, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 240–272. DOI: 10.1007/978-3-031-38548-3_9. URL: https://inria.hal.science/hal-04276899.

[34] C. Boura, N. David, R. Heim Boissier and M. Naya-Plasencia. 'Better Steady than Speedy: Full Break of SPEEDY-7-192'. In: EUROCRYPT 2023 - 42nd Annual International Conference on Theory and Applications of Cryptographic Techniques. Vol. 14007. Lecture Notes in Computer Science. Lyon, France: Springer, 15th Apr. 2023, pp. 36–66. DOI: 10.1007/978-3-031-30634-1_2. URL: https://hal.science/hal-04268885.

[35] C. Bouvier, P. Briaud, P. Chaidos, L. Perrin, R. Salen, V. Velichkov and D. Willems. 'New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations and Jive Compression Mode'. In: Crypto 2023 - 43rd International Cryptology Conference. Vol. 14083. Lecture Notes in Computer Science. Santa Barbara (CA), United States: Springer, 19th Aug. 2023. DOI: 10.1007/978-3-031-38548-3_17. URL: https://hal.science/hal-04276646.

[36] P. Briaud and P. Loidreau. 'Cryptanalysis of rank-metric schemes based on distorted Gabidulin codes'. In: PQCrypto 2023 : The 14th International Conference on Post-Quantum Cryptography. Vol. 14154. Lecture Notes in Computer Science. College Park, MD, United States: Springer, 16th Aug. 2023, pp. 38–56. DOI: 10.1007/978-3-031-40003-2_2. URL: https://hal.science/hal-04145226.

[37] P. Briaud and M. Øygarden. 'A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions'. In: Eurocrypt 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, 12th Feb. 2023, pp. 391–422. DOI: 10.1007/978-3-031-30589-4_14. URL: https://hal.science/hal-03984470.

[38] A. Chailloux and J. Loyer. 'Classical and Quantum 3 and 4-Sieves to Solve SVP with Low Memory'. In: *LNCS - Lecture Notes in Computer Science*. PQCrypto 2023 - 14th International Conference on Post-Quantum Cryptography. Vol. 14154. Lecture Notes in Computer Science. College Park, MD, United States: Springer, 10th Aug. 2023, pp. 225–255. DOI: 10.1007/978-3-031-40003-2_9. URL: https://inria.hal.science/hal-04276492.

[39] A. Couvreur, R. Mora and J.-P. Tillich. 'A new approach based on quadratic forms to attack the McEliece cryptosystem'. In: ASIACRYPT 2023. Guangzhou, China: Springer, 4th Dec. 2023. URL: https://inria.hal.science/hal-04215135.

[40] A. Leverrier and G. Zémor. 'Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes'. In: SODA 2023 - ACM-SIAM Symposium on Discrete Algorithms. Florence, Italy: Society for Industrial and Applied Mathematics, 16th Jan. 2023, pp. 1216–1244. DOI: 10.1137/1.9781611977554.ch45. URL: https://inria.hal.science/hal-04022061.

[41] F. Liu, L. Grassi, C. Bouvier, W. Meier and T. Isobe. 'Coefficient Grouping for Complex Affine Layers'. In: *LNCS - Lecture Notes in Computer Science*. CRYPTO 2023 - 43rd Annual International Cryptology Conference. Vol. 14083. Lecture Notes in Computer Science. Santa Barbara, CA, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 540–572. DOI: 10.1007/978-3-031-38548-3_18. URL: https://inria.hal.science/hal-04278165.

[42] C. Meyer-Hilfiger and J.-P. Tillich. 'Rigorous Foundations for Dual Attacks in Coding Theory'. In: Theory of Cryptography Conference (TCC). Vol. 14372. Lecture Notes in Computer Science. Taipei, Taiwan: Springer, 29th Nov. 2023, pp. 3–32. DOI: 10.1007/978-3-031-48624-1_1. URL: https://inria.hal.science/hal-04276901.

[43] M. Remaud, A. Schrottenloher and J.-P. Tillich. 'Time and Query Complexity Tradeoffs for the Dihedral Coset Problem'. In: *LNCS - Lecture Notes in Computer Science*. PQCrypto 2023 - 14th International Conference on Post-Quantum Cryptography. Vol. 14154. Lecture Notes in Computer Science. College Park, United States: Springer Nature Switzerland, 10th Aug. 2023, pp. 505–532. DOI: 10.1007/978-3-031-40003-2_19. URL: https://inria.hal.science/hal-04276584.

Conferences without proceedings

[44] C. Bouvier, A. Canteaut and L. Perrin. 'Iterated Power Functions: from Univariate Polynomial Representation to Multivariate Degree'. In: Fq15 - International Conference on Finite Fields and Their Applications 2023. Aubervilliers, France, 19th June 2023. URL: https://inria.hal.science/hal-04277028.

[45] K. Carrier, J.-P. Tillich and V. Hatey. 'Security Analysis of SDiTH'. In: Workshop on Code-Based Cryptography. Lyon, France, 20th Nov. 2023. URL: https://inria.hal.science/hal-04311262.

[46] L. Paletta, A. Leverrier, A. Sarlette, M. Mirrahimi and C. Vuillot. 'Robust sparse IQP sampling in constant depth'. In: QIP2024. Taipei, Taiwan, 20th July 2023. URL: https://inria.hal.science/hal-04312163.

Scientific books

[47] C. Boura and M. Naya-Plasencia. *Symmetric Cryptography 1: Design and Security Proofs*. John Wiley & Sons, Ltd, 20th Dec. 2023, p. 272. DOI: 10.1002/9781394256358. URL: https://inria.hal.science/hal-04332733.

[48] C. Boura and M. Naya-Plasencia. *Symmetric Cryptography 2: Cryptanalysis and Future Directions*. John Wiley & Sons, Ltd, Dec. 2023, p. 272. DOI: 10.1002/9781394256327. URL: https://inria.hal.science/hal-04332735.

Scientific book chapters

[49] C. Boura and M. Naya-Plasencia. 'Impossible Differential Cryptanalysis'. In: *Symmetric Cryptography 2: Cryptanalysis and Future Directions*. John Wiley & Sons, Ltd, 1st Dec. 2023, pp. 47–55. DOI: 10.1002/9781394256327.ch3. URL: https://inria.hal.science/hal-04332993.

[50] A. Canteaut. 'Higher Order Differentials, Integral Attacks and Variants'. In: *Symmetric Cryptography 2: Cryptanalysis and Future Directions*. John Wiley & Sons, Ltd, 1st Dec. 2023, pp. 123–132. DOI: 10.1002/9781394256327.ch10. URL: https://inria.hal.science/hal-04333167.

[51] G. Leurent. 'MDS Matrices'. In: *Symmetric Cryptography 1: Design and Security Proofs*. John Wiley & Sons, Ltd, 8th Dec. 2023, pp. 99–109. DOI: 10.1002/9781394256358.ch7. URL: https://inria.hal.science/hal-04333233.

[52] G. Leurent. 'Modes of Operation'. In: *Symmetric Cryptography 1: Design and Security Proofs*. John Wiley & Sons, Ltd, 8th Dec. 2023, pp. 73–85. DOI: 10.1002/9781394256358.ch5. URL: https://inria.hal.science/hal-04333230.

[53] M. Naya-Plasencia. 'Post-Quantum Symmetric Cryptography'. In: *Symmetric Cryptography 2: Cryptanalysis and Future Directions*. John Wiley & Sons, Ltd, 1st Dec. 2023, pp. 203–213. DOI: 10.1002/9781394256327.ch17. URL: https://inria.hal.science/hal-04332991.

[54] K. Nyberg and A. Florez Gutierrez. 'Linear Cryptanalysis'. In: *Symmetric Cryptography 2: Cryptanalysis and Future Directions*. John Wiley & Sons, Ltd, 1st Dec. 2023, pp. 29–46. DOI: 10.1002/9781394256327.ch2. URL: https://inria.hal.science/hal-04333163.

[55] L. Perrin. 'Addition, Rotation, XOR'. In: *Symmetric Cryptography 2: Cryptanalysis and Future Directions*. John Wiley & Sons, Ltd, 1st Dec. 2023, pp. 155–165. DOI: 10.1002/9781394256327.ch13. URL: https://inria.hal.science/hal-04333185.

[56] L. Perrin. 'New Fields in Symmetric Cryptography'. In: *Symmetric Cryptography 2: Cryptanalysis and Future Directions*. John Wiley & Sons, Ltd, 1st Dec. 2023, pp. 215–225. DOI: 10.1002/9781394256327.ch18. URL: https://inria.hal.science/hal-04333189.

[57] L. Perrin. 'Rationale, Backdoors and Trust'. In: *Symmetric Cryptography 1: Design and Security Proofs*. John Wiley & Sons, Ltd, 8th Dec. 2023, pp. 123–134. DOI: 10.1002/9781394256358.ch9. URL: https://inria.hal.science/hal-04333236.

Doctoral dissertations and habilitation theses

[58] C. Bouvier. 'Cryptanalysis and design of symmetric primitives defined over large finite fields'. Sorbonne Université, 27th Nov. 2023. URL: https://inria.hal.science/tel-04327955.

[59] P. Briaud. 'Algebraic Cryptanalysis of Post-Quantum Schemes and Related Assumptions'. Sorbone Université, 11th Dec. 2023. URL: https://hal.science/tel-04358018.

[60] N. David. 'Improved Techniques in Differential Cryptanalysis'. Sorbonne Université, 8th Nov. 2023. URL: https://inria.hal.science/tel-04277996.

[61] J. Loyer. 'Quantum Cryptanalysis on Lattices and Codes'. Sorbonne Université, 18th Dec. 2023. URL: https://theses.hal.science/tel-04390173.

[62] R. Mora. 'Algebraic techniques for decoding Reed-Solomon codes and cryptanalyzing McEliece-like cryptosystems'. Sorbonne Université, 7th Apr. 2023. URL: https://theses.hal.science/tel-04153803.

[63] M. Remaud. 'Applications of Quantum Fourier Sampling and the Dihedral Hidden Subgroup Problem'. Sorbonne Université, 17th Nov. 2023. URL: https://theses.hal.science/tel-04318027.

Reports & preprints

[64] I. Bardet, Á. Capel, L. Gao, A. Lucia, D. Pérez-García and C. Rouzé. *Entropy decay for Davies semigroups of a one dimensional quantum lattice*. 2021. DOI: 10.48550/arXiv.2112.00601. URL: https://hal.science/hal-04406053.

[65] A. Bariant. *Algebraic Cryptanalysis of Full Ciminion*. 25th Aug. 2023. URL: https://inria.hal.science/hal-04277605.

[66] Y. Barsamian and A. Chailloux. *Compressing integer lists with Contextual Arithmetic Trits*. 5th Sept. 2022. URL: https://inria.hal.science/hal-04320912.

[67] F. Blanqui, A. Canteaut, H. de Jong, S. Imperiale, N. Mitton, G. Pallez, X. Pennec, X. Rival and B. Thirion. *Recommandations sur les « éditeurs de la zone grise »*. Inria, 25th Jan. 2023, pp. 1–3. URL: https://inria.hal.science/hal-04001505.

[68] F. Blanqui, A. Canteaut, H. D. Jong, S. Imperiale, N. Mitton, G. Pallez, X. Pennec, X. Rival and B. Thirion. *Recommendations on "Grey-Zone Publishers": Recommendations from the Inria Evaluation Committee, translated from https://hal.inria.fr/hal-04001505*. Inria, 25th Jan. 2023, pp. 1–3. URL: https://inria.hal.science/hal-04201298.

[69] A. Canteaut, M. Serrano, C. Grandmont, G. Pallez, V. Perrier, X. Rival and E. Thomé. *Bilan de la mandature 2019-2023 de la Commission d'Évaluation Inria*. Inria, 31st Aug. 2023. URL: https://inria.hal.science/hal-04193082.

[70] K. Carrier, T. Debris-Alazard, C. Meyer-Hilfiger and J.-P. Tillich. *Reduction from Sparse LPN to LPN, Dual Attack 3.0*. 7th Dec. 2023. URL: https://inria.hal.science/hal-04328262.

[71] A. Chailloux and Y. Barsamian. *Relativistic zero-knowledge protocol for NP over the internet unconditionally secure against quantum adversaries*. 4th Dec. 2023. URL: https://inria.hal.science/hal-04320923.

[72] A. Chailloux and J.-P. Tillich. *The Quantum Decoding Problem*. 9th Nov. 2023. URL: https://inria.hal.science/hal-04277154.

[73] P. Frixons, S. Canard and L. Ferreira. *Quantum Security of the UMTS-AKA Protocol and its Primitives, Milenage and TUAK*. 11th Dec. 2023. URL: https://hal.science/hal-04334580.

[74] T. Kapourniotis, E. Kashefi, D. Leichtle, L. Music and H. Ollivier. *Asymmetric Quantum Secure Multi-Party Computation With Weak Clients Against Dishonest Majority*. 15th Mar. 2023. URL: https://hal.science/hal-04079704.

[75] G. Leurent, B. Mennink, K. Pietrzak, V. Rijmen, A. Biryukov, B. Bunz, A. Canteaut, I. Dinur, Y. Dodis, O. Dunkelman, B. Fisch, I. Komargodski, N. Heninger, M. Naya Plasencia, L. Perrin, C. Rechberger, G. Segev, M. Stam, S. Tessaro, B. Wesolowski, M. Schaffstein, D. Feist, G. Herold, A. Sanso, M. Simkin and D. Khovratovich. *Analysis of MinRoot: Public report*. Ethereum Foundation, 18th Sept. 2023. URL: https://inria.hal.science/hal-04320126.

[76] J. Loyer. *Quantum security analysis of Wave*. 30th Aug. 2023. URL: https://inria.hal.science/hal-04320905.

[77] M. Naya Plasencia, R. Bhaumik, A. Chailloux, P. Frixons and B. Mennink. *Block Cipher Doubling for a Post-Quantum World*. 7th Dec. 2023. URL: https://inria.hal.science/hal-04328717.

Other scientific publications

[78] N. Aaraj, S. Bettaieb, L. Bidoux, A. Budroni, V. Dyseryn, A. Esser, P. Gaborit, M. Kulkarni, V. Mateu, M. Palumbi, L. Perin and J.-P. Tillich. *PERK*. 31st May 2023. URL: https://inria.hal.science/hal-04315863.

[79] N. Aragon, M. Bardet, L. Bidoux, J.-J. Chi-Domínguez, V. Dyseryn, T. Feneuil, P. Gaborit, A. Joux, M. Rivain, J.-P. Tillich and A. Vinçotte. *RYDE specifications*. 21st June 2023. URL: https://inria.hal.science/hal-04315895.

[80] N. Aragon, M. Bardet, L. Bidoux, J.-J. Chi-Domínguez, V. Dyseryn, T. Feneuil, P. Gaborit, R. Neveu, M. Rivain and J.-P. Tillich. *MIRA Specifications*. 21st June 2023. URL: https://inria.hal.science/hal-04315820.

[81] G. Banegas, K. Carrier, A. Chailloux, A. Couvreur, T. Debris-Alazard, P. Gaborit, P. Karpman, J. Loyer, R. Niederhagen, N. Sendrier, B. Smith and J.-P. Tillich. *WAVE: Round 1 Submission*. 21st June 2023. URL: https://inria.hal.science/hal-04278563.

[82] D. M'Foukh. 'Improvements of the differential meet-in-the-middle attack'. Université de versailles Saint-Quentin-en-Yvelines, 29th Sept. 2023. URL: https://inria.hal.science/hal-04277179.

[83] L. Perrin. *How can we ensure that (symmetric) cryptographic primitives are trustworthy?* Rostock, Germany, 7th June 2023. URL: https://inria.hal.science/hal-04327478.

[84] F. Terrier. 'Good quantum low-density parity-check codes'. Sorbonne Universite, 11th Sept. 2023. URL: https://inria.hal.science/hal-04206478.

11.3 Other

Scientific popularization

[85] A. Canteaut. 'Peut-on rêver d'une écriture impénétrable ?' In: *Déchiffrement(s) : des hiéroglyphes à l'ADN*. Colloque annuel du Collège de France. Odile Jacob, 1st Sept. 2023. URL: https://inria.hal.science/hal-04276984.

11.4 Cited publications

[86] 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. URL: https://hal-unilim.archives-ouvertes.fr/hal-02303015.

[87] 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. URL: https://hal.inria.fr/hal-03133479.

[88] A. Couvreur, M. Lequesne and J.-P. Tillich. 'Recovering short secret keys of RLCE encryption scheme in polynomial time'. In: *PQCrypto 2019 - International Conference on Post-Quantum Cryptography*. Chongqing, China, May 2019. DOI: 10.1007/978-3-030-25510-7_8. URL: https://hal.inria.fr/hal-01959617.

[89] T. Debris-Alazard and J.-P. Tillich. 'Two attacks on rank metric code-based schemes: RankSign and an IBE scheme'. In: *ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 11272. LNCS - Lecture Notes in Computer Science. Brisbane, Australia: Springer, Dec. 2018, pp. 62–92. DOI: 10.1007/978-3-030-03326-2_3. URL: https://hal.inria.fr/hal-01957207.

[90] M. Lequesne and J.-P. Tillich. 'Attack on the Edon-K Key Encapsulation Mechanism'. In: *ISIT 2018 - IEEE International Symposium on Information Theory*. Vail, United States, June 2018, pp. 981–985. DOI: 10.1109/ISIT.2018.8437498. URL: https://hal.inria.fr/hal-01949569.