RESEARCH CENTRE

Inria Paris Center

2022

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

Inria

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]
- Ritam BHAUMIK [INRIA, Starting Research Position, until Sep 2022]
- Ivan Bardet [INRIA, Starting Research Position]
- Anne Canteaut [INRIA, Senior Researcher, HDR]
- Andre Chailloux [INRIA, Researcher]
- Pascale Charpin [INRIA, Emeritus, HDR]
- Nicholas Connolly [INRIA, Starting Research Position]
- Gaetan Leurent [INRIA, Researcher]
- Anthony Leverrier [INRIA, Researcher, HDR]
- María Naya Plasencia [INRIA, Senior Researcher, HDR]
- Harold Ollivier [INRIA, Senior Researcher]
- Leo Perrin [INRIA, Researcher]
- Mathys Rennela [INRIA, Starting Research Position]
- Nicolas Sendrier [INRIA, Senior Researcher, HDR]

PhD Students

- Augustin Bariant [INRIA]
- Jules Baudrin [INRIA]
- Aurelien Boeuf [INRIA, from Oct 2022]
- Aurelien Boeuf [INRIA, from Mar 2022 until Aug 2022]
- Clémence Bouvier [SORBONNE UNIVERSITE]
- Pierre Briaud [SORBONNE UNIVERSITE]
- Nicolas David [INRIA]
- Loïc Demange [THALES]
- Aurélie Denys [INRIA]
- Simona Etinski [UNIV PARIS]
- Antonio FLOREZ GUTIERREZ [INRIA, until Sep 2022]
- Paul Frixons [ORANGE LABS]
- Lucien Groues [SORBONNE UNIVERSITE]
- Virgile Guemard [INRIA, from Jul 2022]
- Johanna Loyer [INRIA]
- Charles Meyer-Hilfiger [INRIA]
- Rocco Mora [SORBONNE UNIVERSITE]
- Clara Pernot [INRIA]
- Maxime Remaud [BULL]

Technical Staff

- Valentin Vasseur [THALES, Engineer, from Oct 2022]

Interns and Apprentices

- Aurelien Boeuf [Télécom Paris, from Sep 2022 until Sep 2022]
- Julien Du Crest [UGA, from Mar 2022]

Administrative Assistants

- Christelle Guiziou [INRIA]
- Scheherazade Rouag [INRIA, until Nov 2022]

Visiting Scientists

- Zahra Ahmadian [UNIV SHAHID BEHESHTI, from Nov 2022]
- Patrick Felke [UNIV APPLIED SCIENCES-EMDEN-LEER, from Sep 2022]
- Gregor Leander [UNIV RUHR, from Aug 2022]
- Bart Mennink [UNIV RADBOUD, from May 2022]
- Kaisa Nyberg [UNIV AALTO, from Aug 2022]
- Gilles Van Assche [STMICROELECTRONICS, from Oct 2022]
- Thomas Vidick [CALTECH]

External Collaborators

- Christina Boura [UVSQ]
- Yann Rotella [UVSQ]

2 Overall objectives

The research work within the project-team is mostly devoted to the design and analysis of cryptographic algorithms, in the classical or in the quantum setting. It is especially motivated by the fact that the current situation of cryptography is rather fragile: many of the available symmetric and asymmetric primitives have been either threatened by recent progress in cryptanalysis or by the possible invention of a large quantum computer. Most of our work mixes fundamental aspects and practical aspects of information protection (cryptanalysis, design of algorithms, implementations). In particular we devise

- 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,

work on practical aspects in cryptography, e.g. lightweight constructions and implementation, but also on more fundamental issues, either on discrete mathematics or on quantum information.

3 Research program

3.1 Quantum algorithms and cryptanalysis

The current state-of-the-art asymmetric cryptography would become insecure in a post-quantum world, and the community is actively searching for alternatives. 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 search space. Thus, it was believed that doubling key-lengths suffices to maintain an equivalent security in the post-quantum world. This conventional wisdom was contradicted by Kuwakado and Morii in 2012 when they proposed for the first time to use Simon's algorithm in symmetric cryptanalysis [61], proving the popular Even-Mansour construction to be insecure in a strong security model called the superposition model.

This model allows an attacker to query quantumly the block cipher. Simon's algorithm [63] contrarily to Grover's algorithm gives an exponential speedup and can therefore be devastating in this setting.

In the framework of our ERC QUASYModo, we studied in detail this algorithm and possible applications, and we were able to show that Simon's algorithm applies to other schemes as well, such as for instance to the CAESAR candidate AEZ [57]. It also allows to break some well-known modes of operation for MACs and authenticated encryption and provides devastating quantum slide attacks [9]. Other quantum algorithms turned out be useful in this model, such as for instance Kuperberg's algorithm [60]. It allowed to break a tweak [52] to counter the previous attack of [9] or to devise a quantum attack in the superposition model on the POLY1305 MAC primitive [56], which is largely used and claimed to be quantumly secure.

All these results show that in 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 is precisely the first objective of the ERC QUASYModo regarding symmetric cryptanalysis. We plan in the coming years to continue to actively contribute to this toolbox. This goes together with improving or finding new quantum algorithms for cryptanalysis, possibly adapted to some particular situations or scenarios that have not been studied before, like the k-XOR problem. 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. We are namely composed of symmetric and asymmetric cryptologists as well as of experts in quantum computing and we are in a privileged position to perform this kind of research.

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 [62] and RANKSIGN [59], and have devised a partial break of the RLCE encryption scheme [58]. In 2020, we obtained a significant breakthrough in solving more efficiently the MinRank problem and the decoding problem in the rank metric [53, 54] 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

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

[2] Website of the NIST project.

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.

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 Social and environmental responsibility

Impact of research results on standardisation

Our cryptanalysis results on SHA-1 [10] and GEA [55] have helped convince users and industry to deprecate those obsolete standards. Publication of those attacks and discussion with industry has resulted in concrete actions to reduce usage of those ciphers. Leo Perrin participates to the ISO/IEC working group on cryptographic primitives.

Our project is also involved in two NIST competitions: the competition for lightweight cryptography and the competition for standardizing quantum safe cryptosystems. In the first competition, our team has still one candidate among the finalists of the competition, while in the second competition we have two candidates that are fourth round finalists. The outcome of these two competitions will have a strong impact since the standardized solutions will likely replace large parts of the world's infrastructure underpinning secure global communication.

6 Highlights of the year

Lowlights. The work of the team was affected by several problems:

1. Dysfunctions at Inria at large such as for instance
   - Poor functioning of Eksae that complicated significantly the work of our administrative assistant and the preparation of the budget,
   - Very late reimbursement of travel expenses (for instance one of our PhD got his travel expenses reimbursed after nearly one year),
   - Lack of information or late information for several recruitment/bonus campaigns. The latest example being the delegation campaign which is supposed to finish by the end of January and as of January 19 we haven't received any official guidelines.
2. Research is less and less considered as our main mission.
3. The veiled and constant criticisms on our Evaluation Committee we are all proud of.
4. The uncertainty about the future of the Institute which is not able to fulfill legal obligations such as providing its social report in due time or which does not communicate accurately about its budget, except when publicly calling it "intenable" (meaning "unsustainable").

Furthermore, our team has been directly impacted in the following ways:

- Anne Canteaut is head of the Evaluation Committee and Maria Naya-Plasencia is one of the elected members. They have been directly impacted by these continuing criticisms.
- In June 2020, a call for cryptanalysis projects was launched within the Cybersecurity PEPR. Before launching the call, the scientific organizers of the PEPR asked the people in charge of the PEPR at INRIA to consult teams that would be interested by the topic: COSMIQ and CARAMBA. Our team deeply regrets that it has not been informed in due time about this PEPR call.

6.1 Cryptographic Challenges

ZK Hash Function Cryptanalysis Bounties. The Ethereum Foundation has launched a series of bounties to cryptanalyze hash functions optimized for Zero-Knowledge proofs.

Augustin Bariant, Clémence Bouvier, Gaëtan Leurent and Léo Perrin have solved 7 of the challenges, on three different hash functions: Feistel-MIMC, Poseidon, and Rescue Prime [15]

6.2 Awards and Scholarships

ReSCALE. Léo Perrin has obtained a European Research Concil Grant for Starting Researchers called REinventing Symmetric Cryptography for Arithmetization over Large fiElds.

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 $\mathbb{F}_q$, where typically $q > 2^{64}$. However, these procedures also rely on hash functions and other "symmetric" cryptographic algorithms that are defined over $\mathbb{F}_2 = \{0,1\}$. But modeling $\mathbb{F}_2$ operations using $\mathbb{F}_q$ operations is very costly: relying on standard hash functions leads to significant performance overhead, to the point were the protocols mentionned before are unusable in practice.

In order to alleviate this bottleneck, it is necessary to devise symmetric algorithms that are natively described in $\mathbb{F}_q$. This change requires great care: some hash functions described in Fq have already been presented, and subsequently exhibited significant flaws. The inherent structural differences between $\mathbb{F}_2$ and $\mathbb{F}_q$ are the cause behind these problems: our understanding of the construction of symmetric primitives in $\mathbb{F}_2$ does not carry over to $\mathbb{F}_q$.

The aim of this project bring symmetric cryptography into $\mathbb{F}_q$ in a safe and efficient fashion. To this end, we will rebuild the analysis tools and methods that are used both by designers and attackers.

6.3 Invited Talk

María Naya-Plasencia has given a Keynote talk on *Symmetric Cryptography for Long Term Security* the 2nd June 2022 in Trodheim, Norway, at the flagship cryptography conference, Eurocrypt 2022. video

Abstract. Symmetric cryptography has made important advances in recent years, in part due to new challenges that have appeared, requiring some new developments. During this talk we will discuss these advances and developments, with a particular emphasis on quantum-safe symmetric cryptography and latest results, providing the details of some particularly interesting cases. We will also discuss some related open problems.

7 New software and platforms

7.1 New software

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/

Authors: Nicolas Sendrier, Thomas Debris

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

Participants: Grégory Landais, Nicolas Sendrier

8 New results

8.1 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.

8.2 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.

8.3 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).

8.4 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.

9 Bilateral contracts and grants with industry

9.1 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.

9.2 Bilateral grants with industry

- **Orange Labs Caen** (11/2019 -> 11/2022) Funding for the supervision of Paul Frixon's PhD.
  30 kEuros.
- **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.

10 Partnerships and cooperations

10.1 International research visitors

10.1.1 Visits of international scientists

Inria International Chair

Participant: Thomas Vidick.

10.2 European initiatives

10.2.1 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:

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>2ĝ64. 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."

EQUALITY EQUALITY project on cordis.europa.eu

Title: Efficient QUantum ALgorithms for IndusTrY

Duration: From November 1, 2022 to October 31, 2025

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- UNIVERSITEIT LEIDEN (ULEI), Netherlands
- ALTRAN DEUTSCHLAND SAS & CO KG, Germany
- AIRBUS OPERATIONS SAS (AIRBUS OPERATIONS), France
- FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV (FHG), Germany
- AIRBUS DEFENCE AND SPACE GMBH, Germany
- QU & CO AI BV (Qu & Co AI BV), Netherlands
- DEUTSCHES ZENTRUM FUR LUFT - UND RAUMFAHRT EV (DLR), Germany
- AIRBUS OPERATIONS GMBH, Germany
- CAPGEMINI DEUTSCHLAND GMBH, Germany
- AIRBUS DEFENCE AND SPACE SAS, France
- DA VINCI LABS, France

Inria contact: Harold Olivier

Coordinator:

Summary: A quantum revolution is unfolding, and European scientists are on the lead. Now, it is time to take decisive action and transform our scientific potential into a competitive advantage. Achieving this goal will be critical to ensuring Europe's technological sovereignty in the coming decades. EQUALITY brings together scientists, innovators, and prominent industrial players with the mission of developing cutting-edge quantum algorithms to solve strategic industrial problems. The consortium will develop a set of algorithmic primitives which could be used as modules for various industry-specific workflows. These primitives include differential equation solvers, material simulation algorithms, quantum optimisers, etc. To focus our efforts, we target eight paradigmatic industrial problems. These problems are likely to yield to early quantum advantage and pertain to the aerospace and energy storage industries. They include airfoil aerodynamics, battery and fuel cell design, space mission optimisation, etc. Our goal is to develop quantum algorithms for real industrial problems using real quantum hardware. This requires grappling with the limitations of present-day quantum hardware. Thus, we will devote a large portion of our efforts to developing strategies for optimal hardware exploitation. These low-level implementations will account for the effects of noise and topology and will optimise algorithms to run on limited hardware. EQUALITY will build synergies with Quantum Flagship projects and Europe's thriving ecosystem of quantum start-ups. Use cases will be tested on quantum hardware from three of Europe's leading vendors and two HPC centres. The applications targeted have the potential of creating billions of euros for end-users and technology providers over the coming decades. With EQUALITY, we aim at playing a role in unlocking this value and placing Europe at the centre of this development. The project gathers 9 partners and has a budget of €6M over 3 years.

QIA-Phase1 QIA-Phase1 project on cordis.europa.eu

Title: Quantum Internet Alliance - Phase1

Duration: From October 1, 2022 to March 31, 2026

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- SWABIAN INSTRUMENTS GMBH (SI), Germany
- UNIVERSITA DEGLI STUDI DI PARMA (UNIVERSITA DEGLI STUDI DI PARMA), Italy
- MY CRYO FIRM (MYCRYO), France
- IXBLUE, France
- NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO (NETHERLANDS ORGANISATION FORAPPLIED SCIENTIFIC RESEARCH), Netherlands
- FUNDACIO INSTITUT DE CIENCIES FOTONIQUES (ICFO-CERCA), Spain
- THALES SIX GTS FRANCE SAS (THALES SIX GTS France), France
- COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA), France
- QBLOX BV, Netherlands
- ALPINE QUANTUM TECHNOLOGIES GMBH, Austria
- KOBENHAVNS UNIVERSITET (UCPH), Denmark
- LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (LIST), Luxembourg
- TECHNISCHE UNIVERSITAT BERLIN (TUB), Germany
- SURF BV, Netherlands
- WELINQ SAS, France
- Q* BIRD BV (Q*Bird B.V.), Netherlands
- UNIVERSITAT POLITECNICA DE VALENCIA (UPV), Spain
- UNIVERSITY OF STUTTGART (USTUTT), Germany
- VERIQLOUD, France
- MAX-PLANCK-GESELLSCHAFT ZUR FORDERUNG DER WISSENSCHAFTEN EV (MPG), Germany
- UNIVERSITAET INNSBRUCK (UIBK), Austria
- THALES (THALES), France
- CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS (CNRS), France
- TOPTICA PHOTONICS AG (TOPTICA), Germany
- TECHNISCHE UNIVERSITEIT DELFT (TU Delft), Netherlands
- SORBONNE UNIVERSITE, France
- TECHNISCHE UNIVERSITAET DRESDEN (TUD), Germany

Inria contact: Harold Ollivier

Coordinator:

Summary: The mission of the Quantum Internet Alliance (QIA) is to build a global Quantum Internet made in Europe – by developing a full-stack prototype network, and by driving an innovative European Quantum Internet ecosystem capable of scaling the network to worldleading European technology. Building on its proven track record in teamwork, which has already resulted in world first Quantum Internet technology, QIA advances this mission in two complementary objectives: The first is the realization of a full-stack prototype network able to distribute entanglement between two metropolitan-scale networks via a long-distance backbone (>500 km) using quantum repeaters. The second is the establishment of a European platform for Quantum Internet development, which

will act as a catalyst for a European Quantum Internet Ecosystem including actors all along the value chain.

QIA's network will enable advanced quantum-network applications and prepare the ground for secure quantum computing in the cloud, thanks to our new generation of end nodes including both processing nodes and low-cost photonic client devices. Nodes in the metropolitan network will be interconnected via hubs that allow the scalable connection of hundreds of end nodes, paving the way for early adopters. The long-distance backbone will be realized using fully functional quantum repeaters unlocking Pan-European end-to-end quantum communication. QIA's prototype network will operate on standard optical fibers and serves to validate all key sub-systems, ready to be scaled by European industry.

In this first SGA we will advance towards the long-term objectives set up in the FPA project. Here we present in detail how work will be implemented during this first phase of the SGA.

10.2.2 H2020 projects

HPCQS HPCQS project on cordis.europa.eu

Title: High Performance Computer and Quantum Simulator hybrid

Duration: From December 1, 2021 to November 30, 2025

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- GRAND EQUIPEMENT NATIONAL DE CALCUL INTENSIF (GENCI), France
- NATIONAL UNIVERSITY OF IRELAND GALWAY (NUI GALWAY), Ireland
- FORSCHUNGSZENTRUM JULICH GMBH (FZJ), Germany
- PARITY QUANTUM COMPUTING GMBH (ParityQC), Austria
- FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV (FHG), Germany
- COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA), France
- EURICE EUROPEAN RESEARCH AND PROJECT OFFICE GMBH, Germany
- CONSIGLIO NAZIONALE DELLE RICERCHE (CNR), Italy
- BULL SAS (BULL), France
- FLYSIGHT SRL, Italy
- PARTEC AG (PARTEC), Germany
- UNIVERSITAET INNSBRUCK (UIBK), Austria
- CINECA CONSORZIO INTERUNIVERSITARIO (CINECA), Italy
- CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS (CNRS), France
- CENTRALESUPELEC (CentraleSupélec), France
- BARCELONA SUPERCOMPUTING CENTER CENTRO NACIONAL DE SUPERCOMPUTACION (BSC CNS), Spain
- SORBONNE UNIVERSITE, France

Inria contact: Luc Giraud

Coordinator:

Summary: The aim of HPCQS is to prepare European research, industry and society for the use and federal operation of quantum computers and simulators. These are future computing technologies that are promising to overcome the most difficult computational challenges. HPCQS is developing the programming platform for the quantum simulator, which is based on the European ATOS Quantum Learning Machine (QLM), and the deep, low-latency integration into modular HPC systems based on ParTec's European modular supercomputing concept. A twin pilot system, developed as a prototype by the European company Pasqal, will be implemented and integrated at CEA/TGCC (France) and FZJ/JSC (Germany), both hosts of European Tier-0 HPC systems. The pre-exascale sites BSC (Spain) and CINECA (Italy) as well as ICECH (Ireland) will be connected to the TGCC and JSC via the European data infrastructure FENIX. It is planned to offer quantum HPC hybrid resources to the public via the access channels of PRACE. To achieve these goals, HPCQS brings together leading quantum and supercomputer experts from science and industry, thus creating an incubator for practical quantum HPC hybrid computing that is unique in the world. The HPC-QS technology will be developed in a co-design process together with selected exemplary use cases from chemistry, physics, optimization and machine learning suitable for quantum HPC hybrid calculations. HPCQS fits squarely to the challenges and scope of the call by acquiring a quantum device with two times 100+ neutral atoms. HPCQS develops the connection between the classical supercomputer and the quantum simulator by deep integration in the modular supercomputing architecture and will provide cloud access and middleware for programming and execution of applications on the quantum simulator through the QLM, as well as a Jupyter-Hub platform with safe access guarantee through the European UNICORE system to its ecosystem of quantum programming facilities and application libraries.

10.3 National initiatives

- **ANR DEREC** (10/16→03/22)
  Relativistic cryptography
  ANR Program: jeunes chercheurs
  244 kEuros
  The goal of project DEREC is to demonstrate the feasibility of guaranteeing the security of some cryptographic protocols using the relativistic paradigm, which states that information propagation is limited by the speed of light. We plan to study some two party primitives such as bit commitment and their security against classical and quantum adversaries in this model. We then plan to the integration of those primitives into larger cryptosystems. Finally, we plan on performing a demonstration of those systems in real life conditions.

- **ANR CBCRYPT** (10/17→03/22)
  Code-based cryptography
  ANR Program: AAP Générique 2017
  Partners: Inria COSMIQ (coordinator), XLIM, Univ. Rouen, Univ. Bordeaux.
  197 kEuros
  The goal of CBCRYPT is to propose code-based candidates to the NIST call aiming at standardizing public-key primitives which resist to quantum attacks. These proposals are based either on code-based schemes relying on the usual Hamming metric or on the rank metric. The project does not deal solely with the NIST call. We also develop some other code-based solutions: these are either primitives that are not mature enough to be proposed in the first NIST call or whose functionalities are not covered by the NIST call, such as identity-based encryption, broadcast encryption, attribute based encryption or functional encryption. A third goal of this project is of a more fundamental nature: namely to lay firm foundations for code-based cryptography by developing thorough and rigorous security proofs together with a set of algorithmic tools for assessing the security of code-based cryptography.

- **ANR quBIC** (10/17→03/22)
  Quantum Banknotes and Information-Theoretic Credit Cards
  ANR Program: AAP Générique 2017
  Partners: Univ. Paris-Diderot (coordinator), Inria COSMIQ, UPMC (LIP6), CNRS (Laboratoire

Kastler Brossel)
87 kEuros
For a quantum-safe future, classical security systems as well as quantum protocols that guarantee security against all adversaries must be deployed. Here, we will study and implement one of the most promising quantum applications, namely unforgeable quantum money. A money scheme enables a secure transaction between a client, a vendor and a bank via the use of a credit card or via the use of banknotes, with maximal security guarantees. Our objectives are to perform a theoretical analysis of quantum money schemes, in realistic conditions and for encodings in both discrete and continuous variables, and to demonstrate experimentally these protocols using state-of-the-art quantum memories and integrated detection devices.

- **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.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- WCC 2022: March 7-13, 2022, Rostock (Allemagne): co-chair, L. Perrin;
- Dagstuhl seminar 22141 "Symmetric Cryptography": April 3-8, 2022, Dagstuhl (Germany): M. Naya-Plasencia co-chair;
- IEEE ITW 2023: April 23-28, 2023, St-Malo (France): A. Canteaut, co-chair.

Member of the organizing committees

- Journées C2 2022: April 10-15 2022, Hendaye (France): G. Leurent, L. Perrin.

11.1.2 Scientific events: selection

Chair of conference program committees

- WCC 2022: March 7-13, 2022, Rostock, Germany (L. Perrin) ;
- ITW 2023: April 23-28, 2023, Saint-Malo, France (A. Canteaut);

Member of the conference program committees

- WCC 2022: March 7-13, 2022, Rostock, Germany (A. Canteaut, N. Sendrier, J.-P. Tillich);
- Eurocrypt 2022: May 30-June 3, 2022, Trondheim, Norway, (G. Leurent);
- Crypto 2022: August 13-18, 2022, Santa Barbara, USA, (M. Naya-Plasencia);
- QCrypt 2022: August 29 - September 2, 2022, Taipei city, Taiwan (A. Leverrier);
- PQCrypto 2022: September 28 - September 30, 2022, virtual, (N. Sendrier, J.-P. Tillich);
- Colloquium of the GDR IQFA, November 16-18, 2022, Palaiseau, France (A. Leverrier);
- QIP 2023: February 4-10, 2023, Ghent, Belgium (A. Leverrier);
- ITW 2023: April 23-28, 2023, Saint-Malo, France (J.-P. Tillich);
- PKC 2023: May 7-10, 2023, Atlanta, USA, (J.P. Tillich);
- ISIT 2023: June 25-30, 2023, Taipei city, Taiwan (J.-P. Tillich);

11.1.3 Journal

Member of the editorial boards

- *Advances in Mathematics of Communications*, associate editors: N. Sendrier and J.P. Tillich.
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut
- *Designs, Codes and Cryptography*, associate editors: P. Charpin M. Naya-Plasencia.
- *Finite Fields and their Applications*, associate editors: A. Canteaut, P. Charpin.
- *IACR Transactions in Symmetric Cryptology*, editorial board member editor: G. Leurent, L. Perrin.
- *IEEE Transactions on Information Theory*, area editor (for cryptography and sequences): A. Canteaut.
- *Journal of Cryptology*, associate editor: A. Canteaut.
- *Quantum Journal*, editor: A. Leverrier.

11.1.4 Invited talks

- A. Canteaut, *Integral attacks on some arithmetization-friendly primitives*, The Ernst Selmer International Workshop, Geiranger, Norway, August 21-27, 2022.
- A. Canteaut, *Peut-on rêver d'une écriture impénétrable ?*, Colloque de rentrée du Collège de France : Déchiffrement(s) : des hiéroglyphes à l'ADN, Paris, France, October 20-21, 2022.
- A. Leverrier, *Calcul quantique tolérant aux fautes*, Journéees du GDR IM, Lille, France, 28 March-2 April 2022.
- A. Leverrier, *The quantum LDPC manifesto*, Simons Institute quantum colloquium, online, 26 April 2022.
- A. Leverrier, *Quantum LDPC codes*, Summer School on Quantum Information and Quantum Technology - 2022, Kolkota, India (online), 1 June-4 July 2022.
- A. Leverrier, *Multimode bosonic cats*, Workshop on Continuous-Variable Quantum Correlations, Copenhagen, Denmark, 6-8 September 2022.

- G. Leurent, *Generic Attacks against MAC Algorithms and Hash Functions*, IACR-CROSSING School on Combinatorial Techniques in Cryptography, Valetta, Malta, 25-28 April 2022.
- G.Leurent, *(Symmetric) Cryptanalysis in Practice*, Cyber in Nancy, Nancy, France, 4-8 July 2022.
- M. Naya-Plasencia, *Quantum Safe Symmetric Cryptography*, WCC 2022, Rostock, Germany 7-11 March 2022.
- M. Naya-Plasencia, *Symmetric Cryptography for Long Term Security*, Eurocrypt 2022 Keynote talk, Trondheim, Norway 30 May-3 June 2022.

11.1.5 Leadership within the scientific community

- A. Canteaut serves as a chair of the steering committee of Fast Software Encryption (FSE), M. Naya-Plasencia and G. Leurent also serve on the committee.
- A. Canteaut serves on the International Scientific Advisory Board of the Flemish Strategic Research Program on Cybersecurity.
- N. Sendrier serves in the steering committee of the PQCrypto conference series.
- P. Charpin, N. Sendrier, and J.-P. Tillich serve in the steering committee of the WCC conference series.

11.1.6 Scientific expertise

- Member of the French CE39 ANR panel in 2022 (M. Naya-Plasencia);
- External reviewer of DFG-grant proposals (J.-P. Tillich);
- External reviewer of an ISF-research proposal (J.-P. Tillich);
- External reviewer of Step 2 proposals of PE6 panel from ERC-2021-STG (M. Naya-Plasencia)
- External reviewer for the Natural Sciences and Engineering Research Council of Canada (A. Canteaut)
- External reviewer for the Vienna Science and Technology Fund (A. Canteaut)

11.1.7 Research administration

- A. Canteaut serves as Head of Inria Evaluation Committee since September 2019. She served on the following hiring juries: jury d'admissibilité DR2 (president), jury d'admission CRCN, jury d'admission DR2. d'admission DR2.
- A. Chailloux serves in the Inria CES (Commission des emplois Scientifiques).
- A. Leverrier serves on the steering committee of the Domaine d'Intérêt Majeur SIRTEQ since 2018.
- A. Leverrier is the coordinator of the Inria challenge EQIP on Quantum Technologies.
- A. Leverrier serves in the scientific board of the GdR IQFA;
- H. Ollivier was a committee member of the Chaire de Professeur Junior INRIA Saclay;
- H. Ollivier is Co-head of the PEPR Quantique;
- H. Ollivier is Co-head of the Hybrid HPC Quantum Initiative;
- M. Naya-Plasencia serves as elected member in the Inria Evaluation Committee since September 2019.

As Head of Inria Evaluation Committee, A. Canteaut has been invited to give a presentation or to participate to a panel discussion to the following events:

- *Journées non-thématiques du GDR Réseaux, Systèmes Distribués*, Rennes, April 28, 2022
- *Journées du doctorat de la SIF*, December 13, 2022
- *Open Science Days@UGA*, Grenoble, December 13-14, 2022.

11.2 Teaching - Supervision - Juries

11.2.1 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.

11.2.2 Supervision

- PhD: Andrea Olivo, Leveraging small quantum states: applications to linear optics and position verification, Université Paris-Saclay, June 15, 2022, supervisors: A. Chailloux, F. Grosshans (laboratoire Aimé Cotton), J. Robert (Université Paris-Saclay).
- PhD: Antonio Florez Gutierrez, Improved Techniques in the Cryptanalysis of Symmetric Primitives, Sorbonne Université, September 30, 2022, supervisor: M. Naya Plasencia.
- PhD: Paul Frixons, Cryptographie à clé secrète et impact d'un attaquant quantique sur le monde des télécommunications, Sorbonne Université, November 25, supervisor: M. Naya Plasencia.
- PhD: Lucien Grouès, Decoding of quantum LDPC codes, December 19, 2022, supervisors: A. Leverrier and O. Fawzi (Ecole Normale Supérieure de Lyon).
- PhD in progress: Simona Etinski, Quantum algorithms and protocols, since October 2019, supervisors: A. Chailloux, A. Leverrier and F. Magniez (Université de Paris).
- PhD in progress: Rocco Mora, Algebraic structures in code-based cryptography, since October 2019, supervisor: J.-P. Tillich.
- PhD in progress: Maxime Remaud, Quantum cryptanalysis in code-based and lattice-based cryptography, since July 2020, supervisor: J.-P. Tillich.
- PhD in progress: Clémence Bouvier, Analyse de la sécurité de primitives symétriques dédiées à divers usages émergents, since September 2020, supervisors: A. Canteaut, L. Perrin.
- PhD in progress: Nicolas David, Secure primitives and the post-quantum world, since September 2020, supervisor: M. Naya Plasencia.

- PhD in progress: Clara Pernot, Cryptanalyse des algorithmes de cryptographie symétrique, since September 2020, supervisors: L. Perrin, M. Naya Plasencia.
- PhD in progress: Pierre Briaud, Cryptosystems based on the MinRank problem, since October 2020, supervisor: J.-P. Tillich.
- PhD in progress: Aurélie Denys, Security proofs for continuous variable quantum cryptography protocols, since October 2020, supervisor: A. Leverrier.
- PhD in progress: Johanna Loyer, Quantum algorithms on lattices, since October 2020, supervisor: A. Chailloux.
- 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.

11.2.3 Juries

- V. Mollimard, *Algorithms for differential cryptanalysis*, IRISA Rennes, January 11, 2022, committee: M. Naya-Plasencia (reviewer).
- K. Ivanov, *Symmetry in design and decoding of polar-like codes*, EPFL, February 1, 2022, committee: J.-P. Tillich (reviewer).
- C. Bouillaguet [HDR], *Les attaques cryptographiques sont-elles toujours meilleures que la force brute ?*,Sorbonne Université, March 17, 2022, committee: A. Canteaut (reviewer).
- L. Colisson, *Study of Protocols Between Classical Clients and a Quantum Server*, Sorbonne Université, March 28, 2022, committee: M. Naya-Plasencia (examiner).
- C. Chaliba, *Error correction and reconciliation techniques for lattice-based key generation protocols*, CY Cergy Paris Université, May 22, 2022, committee: N. Sendrier (president).
- K. Stoffelen, *Optimizations in Symmetric Cryptography*, Radboud University, NL, June 1, 2022, committee: A. Canteaut.
- P. Derbez [HDR], *Algorithmes et outils pour la cryptanalyse*, IRISA Rennes, June 6, 2022, committee: A. Canteaut (Reviewer), M. Naya-Plasencia (examiner).
- M. Rivain [HDR], *On the Provable Security of Cryptographic Implementations*, Université PSL, June 21, 2022, committee: A. Canteaut (president)
- O. Ruatta [HDR], *Polynomes : du discret (codes correcteurs et cryptographie basée sur les codes) et du continu (autour des trajectoires optimales)*, University of Limoges, June 29, 2022, J.-P. Tillich (reviewer).
- A. Florez-Gutierrez, *Algorithms for differential cryptanalysis*, Sorbonne Université, September 30, 2022, committee: M. Naya-Plasencia (supervisor), A. Canteaut (president).
- L. Rouquette, *Improving scalability and reusability of differential cryptanalysis models using constraint programming* , INSA Lyon, November 15, 2022, committee: M. Naya-Plasencia (reviewer).

- P. Frixons, *Secret-key cryptography and impact of a quantum attacker on the telecommunication world*, Sorbonne Université, November 25, 2022, committee: M. Naya-Plasencia (supervisor).
- M. Bros, *Algebraic Cryptanalysis and Contributions to Post-Quantum Cryptography based on Error-Correcting Codes in the Rank-metric*, Université de Limoges, December 8, 2022, committee: J.-P. Tillich (examiner).
- M. Bardet [HDR], *Algebraic cryptanalysis in code-based and multivariate cryptography*, December 12, 2022, Université de Rouen Normandie, committee: J.-P. Tillich (examiner).
- M. Bertin, *Matricial Algebraic Systems and Application to the DAGS Cryptanalysis*, December 12, 2022, Université de Rouen Normandie, committee: J.-P. Tillich (reviewer).
- L. Grouès, *Decoding of LDPC quantum codes*, Sorbonne Université, December 19, 2022, committee: A. Leverrier (supervisor).

11.3 Popularization

11.3.1 Internal or external Inria responsibilities

- A. Leverrier, coordinator of Inria challenge *Engineering for Quantum Information Processors* (EQIP).

11.3.2 Articles and contents

- *Maria Naya-Plasencia : son combat pour préserver la sécurité numérique* https://www.inria.fr/fr/maria-naya-plasencia-cryptographie-postquantique-securite-numerique
- Maxime Garnier and Harold Ollivier, *Prospects for Practical Verified and Blind Delegated Quantum Computations*, ERCIM News 128, January 2022 Special theme: Quantum Computing, https://ercim-news.ercim.eu/images/stories/EN128/EN128-web.pdf

11.3.3 Interventions

- A. Canteaut, table ronde *Métiers du numérique : ces femmes d'exception*, Congrès Femmes En Sciences, February 18-20, 2022, La Villette, Paris (France) http://femmes-en-sciences.fr/congres-femmes-en-sciences-2022/.
- A. Canteaut, intervention auprès des élèves de 3e du collège Gaspard Malo à Dunkerque, February 24, 2022.

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. 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.

12.2 Publications of the year

International journals

[14] I. Bardet, A. Capel and C. Rouzé. 'Approximate tensorization of the relative entropy for noncommuting conditional expectations'. In: *Annales Henri Poincaré* 23.1 (Jan. 2022), pp. 101–140. DOI: 10.1007/s00023-021-01088-3. URL: https://hal.archives-ouvertes.fr/hal-03140651.

[15] A. Bariant, C. Bouvier, G. Leurent and L. Perrin. 'Algebraic Attacks against Some Arithmetization-Oriented Primitives'. In: *IACR Transactions on Symmetric Cryptology* (9th Sept. 2022), pp. 73–101. DOI: 10.46586/tosc.v2022.i3.73-101. URL: https://hal.inria.fr/hal-03901594.

[16] J. Baudrin, A. Canteaut and L. Perrin. 'Practical Cube Attack against Nonce-Misused Ascon'. In: *IACR Transactions on Symmetric Cryptology* (7th Dec. 2022), pp. 120–144. DOI: 10.46586/tosc.v2022.i4.120-144. URL: https://hal.inria.fr/hal-03901680.

[17] C. Beierle, M. Broll, F. Canale, N. David, A. Flórez-Gutiérrez, G. Leander, M. Naya-Plasencia and Y. Todo. 'Improved Differential-Linear Attacks with Applications to ARX Ciphers'. In: *Journal of Cryptology* 35.4 (Oct. 2022), p. 29. DOI: 10.1007/s00145-022-09437-z. URL: https://hal.inria.fr/hal-03947756.

[18] C. Beierle, C. Carlet, G. Leander and L. Perrin. 'A further study of quadratic APN permutations in dimension nine'. In: *Finite Fields and Their Applications* 81 (Aug. 2022), p. 102049. DOI: 10.1016/j.ffa.2022.102049. URL: https://hal.inria.fr/hal-03901618.

[19] C. Beierle, G. Leander and L. Perrin. 'Trims and extensions of quadratic APN functions'. In: *Designs, Codes and Cryptography* 90.4 (Apr. 2022), pp. 1009–1036. DOI: 10.1007/s10623-022-01024-4. URL: https://hal.inria.fr/hal-03901649.

[20] C. Bouvier, A. Canteaut and L. Perrin. 'On the algebraic degree of iterated power functions'. In: *Designs, Codes and Cryptography* (27th Oct. 2022). DOI: 10.1007/s10623-022-01136-x. URL: https://hal.inria.fr/hal-03901713.

[21] A. Canteaut, A. Couvreur and L. Perrin. 'Recovering or Testing Extended-Affine Equivalence'. In: *IEEE Transactions on Information Theory* 68.9 (Sept. 2022), pp. 6187–6206. DOI: 10.1109/TIT.2022.3166692. URL: https://hal.inria.fr/hal-03156177.

[22] P. Charpin. 'The crooked property'. In: *Finite Fields and Their Applications* (22nd Mar. 2022). DOI: 10.1016/j.ffa.2022.102032. URL: https://hal.inria.fr/hal-03091422.

[23] O. Dunkelman, M. Eichlseder, D. Kales, N. Keller, G. Leurent and M. Schofnegger. 'Practical Key Recovery Attacks on FlexAEAD'. In: *Designs, Codes and Cryptography* (2022). DOI: 10.1007/s10623-022-01023-5. URL: https://hal.inria.fr/hal-03528899.

[24] A. Leverrier, S. Apers and C. Vuillot. 'Quantum XYZ Product Codes'. In: *Quantum* (14th July 2022). DOI: 10.22331/q-2022-07-14-766. URL: https://hal.inria.fr/hal-03108325.

[25] A. Leverrier, V. Londe and G. Zémor. 'Towards local testability for quantum coding'. In: *Quantum* 6 (18th Feb. 2022), p. 661. DOI: 10.22331/q-2022-02-24-661. URL: https://hal.inria.fr/hal-03926985.

[26] 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* (22nd Nov. 2022). DOI: 10.1007/s10623-022-01153-w. URL: https://hal.inria.fr/hal-03919898.

[27] H. Ollivier. 'Emergence of Objectivity for Quantum Many-Body Systems'. In: *Entropy* 24.2 (Feb. 2022), p. 277. DOI: 10.3390/e24020277. URL: https://hal.inria.fr/hal-03938839.

International peer-reviewed conferences

[28] J. Baena, P. Briaud, D. Cabarcas, R. Perlner, D. Smith-Tone and J. Verbel. 'Improving Support-Minors rank attacks: applications to GeMSS and Rainbow'. In: *Lecture Notes in Computer Science*. CRYPTO 2022. 13509. Santa Barbara (CA), United States: Springer, 8th Feb. 2023. DOI: 10.1007/978-3-031-15982-4_13. URL: https://hal.science/hal-03533455.

[29] L. Bidoux, P. Gaborit, M. Kulkarni and N. Sendrier. 'Quasi-Cyclic Stern Proof of Knowledge'. In: ISIT 2022 - IEEE International Symposium on Information Theory. Espoo, Finland: IEEE, 26th June 2022, pp. 1459–1464. DOI: 10.1109/ISIT50566.2022.9834642. URL: https://hal.inria.fr/hal-03978139.

[30] M. Broll, F. Canale, N. David, A. Flórez-Gutiérrez, G. Leander, M. Naya-Plasencia and Y. Todo. 'New Attacks from Old Distinguishers Improved Attacks on Serpent'. In: CT-RSA 2022: Cryptographers' Track at the RSA Conference. Vol. LNCS-13161. Topics in Cryptology – CT-RSA 2022. Virtual, France: Springer International Publishing, 29th Jan. 2022, pp. 484–510. DOI: 10.1007/978-3-030-95312-6_20. URL: https://hal.inria.fr/hal-03947766.

[31] K. Carrier, T. Debris-Alazard, C. Meyer-Hilfiger and J.-P. Tillich. 'Statistical Decoding 2.0: Reducing Decoding to LPN'. In: ASIACRYPT 2022 - 28th Annual International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.inria.fr/hal-03919778.

[32] A. Florez Gutierrez. 'Optimising Linear Key Recovery Attacks with Affine Walsh Transform Pruning'. In: ASIACRYPT 2022 - 28th Annual International Conference on the Theory and Application of Cryptology and Information Security. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.inria.fr/hal-03878737.

[33] A. Leverrier and G. Zemor. 'Quantum Tanner codes'. In: FOCS 2022 - IEEE 63rd Annual Symposium on Foundations of Computer Science. Denver, United States: IEEE, 31st Oct. 2022, pp. 872–883. DOI: 10.1109/FOCS54457.2022.00117. URL: https://hal.inria.fr/hal-03926730.

Conferences without proceedings

[34] A. Canteaut. 'Integral attacks on some arithmetization-friendly primitives'. In: The Ernst Selmer International Workshop. Geirangen, Norway, 21st Aug. 2022. URL: https://hal.inria.fr/hal-03970836.

[35] M. Naya-Plasencia. 'Quantum Safe Symmetric Cryptography'. In: WCC 2022: The Twelfth International Workshop on Coding and Cryptography. Rostock, Germany, 7th Mar. 2022. URL: https://hal.inria.fr/hal-03947915.

[36] M. Naya-Plasencia. 'Symmetric Cryptography for Long Term Security'. In: Eurocrypt 2022. Trondheim, Norway, 1st June 2022. URL: https://hal.inria.fr/hal-03947777.

Doctoral dissertations and habilitation theses

[37] A. Florez Gutierrez. 'Improved Techniques in the Cryptanalysis of Symmetric Primitives'. Sorbonne Université, 30th Sept. 2022. URL: https://hal.inria.fr/tel-03878739.

[38] P. Frixons. 'Secret-key cryptography and impact of a quantum attacker on the telecommunication world'. Sorbonne Université, 25th Nov. 2022. URL: https://hal.inria.fr/tel-03878611.

[39] A. Olivo. 'De l'utilité des petits états quantiques : applications à l'optique linéaire et à la vérification de la position'. Université Paris-Saclay, 15th June 2022. URL: https://theses.hal.science/tel-03889983.

Reports & preprints

[40] 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*. 21st Jan. 2022. URL: https://hal.archives-ouvertes.fr/hal-03538315.

[41] I. Bardet, Á. Capel, L. Gao, A. Lucia, D. Pérez-García and C. Rouzé. *Rapid thermalization of spin chain commuting Hamiltonians*. 21st Jan. 2022. URL: https://hal.archives-ouvertes.fr/hal-03538313.

[42] A. Bariant, C. Bouvier, G. Leurent and L. Perrin. *Practical Algebraic Attacks against some Arithmetization-oriented Hash Functions*. Inria, 10th Jan. 2022. URL: https://hal.archives-ouvertes.fr/hal-03518757.

[43] L. Bidoux, P. Gaborit and N. Sendrier. *Quasi-Cyclic Stern Proof of Knowledge*. 19th Jan. 2022. URL: https://hal.inria.fr/hal-03533965.

[44] P. Briaud and M. Øygarden. *A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions*. 12th Feb. 2023. URL: https://hal.science/hal-03984470.

[45] T. Debris-Alazard, M. Remaud and J.-P. Tillich. *Quantum Reduction of Finding Short Code Vectors to the Decoding Problem*. 17th Jan. 2022. URL: https://hal.inria.fr/hal-03529802.

[46] T. Debris-Alazard, N. Sendrier and J.-P. Tillich. *SURF: A new code-based signature scheme*. 29th Apr. 2022. URL: https://hal.inria.fr/hal-01661786.

[47] T. Kapourniotis, E. Kashefi, D. Leichtle, L. Music and H. Ollivier. *Unifying Quantum Verification and Error-Detection: Theory and Tools for Optimisations*. 17th Nov. 2022. URL: https://hal.science/hal-03857850.

[48] R. Mora and J.-P. Tillich. *On the dimension and structure of the square of the dual of a Goppa code*. 18th Jan. 2022. URL: https://hal.archives-ouvertes.fr/hal-03533235.

[49] N. Sendrier. *Secure Sampling of Constant-Weight Words -Application to BIKE*. 19th Jan. 2022. URL: https://hal.inria.fr/hal-03534005.

[50] V. Vasseur. *QC-MDPC codes DFR and the IND-CCA security of BIKE*. 19th Jan. 2022. URL: https://hal.inria.fr/hal-03534003.

12.3 Other

Scientific popularization

[51] A. Canteaut. 'Peut-on rêver d'une écriture impénétrable ?' In: Déchiffrement(s) : des hiéroglyphes à l'ADN - colloque de rentrée du Collège de France. Paris, France, 20th Oct. 2022. URL: https://hal.inria.fr/hal-03970826.

12.4 Cited publications

[52] G. Alagic and A. Russell. 'Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts'. In: *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*. Ed. by J.-S. Coron and J. B. Nielsen. Vol. 10212. Lecture Notes in Computer Science. 2017, pp. 65–93. DOI: 10.1007/978-3-319-56617-7_3. URL: https://doi.org/10.1007/978-3-319-56617-7%5C_3.

[53] 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.

[54] 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.

[55] C. Beierle, P. Derbez, G. Leander, G. Leurent, H. Raddum, Y. Rotella, D. Rupprecht and L. Stennes. 'Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2'. In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by A. Canteaut and F.-X. Standaert. Cham: Springer International Publishing, 2021, pp. 155–183.

[56] D. J. Bernstein. 'The Poly1305-AES Message-Authentication Code'. In: *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*. Ed. by H. Gilbert and H. Handschuh. Vol. 3557. Lecture Notes in Computer Science. Springer, 2005, pp. 32–49. DOI: 10.1007/11502760_3. URL: https://doi.org/10.1007/11502760%5C_3.

[57] X. Bonnetain. 'Quantum Key-Recovery on full AEZ'. In: *SAC 2017 - Selected Areas in Cryptography*. Ottawa, Canada, Aug. 2017. URL: https://hal.inria.fr/hal-01650026.

[58] 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.

[59] 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.

[60] G. Kuperberg. 'A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem'. In: *SIAM J. Comput.* 35.1 (2005), pp. 170–188. DOI: 10.1137/S0097539703436345. URL: https://doi.org/10.1137/S0097539703436345.

[61] H. Kuwakado and M. Morii. 'Security on the quantum-type Even-Mansour cipher'. In: *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*. IEEE, 2012, pp. 312–316. URL: http://ieeexplore.ieee.org/document/6400943/.

[62] 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.

[63] D. R. Simon. 'On the Power of Quantum Computation'. In: *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*. IEEE Computer Society, 1994, pp. 116–123. DOI: 10.1109/SFCS.1994.365701. URL: https://doi.org/10.1109/SFCS.1994.365701.