RESEARCH CENTRE

Paris

2020
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, from Feb 2020]
- Anne Canteaut [Inria, Senior Researcher, HDR]
- André Chailloux [Inria, Researcher]
- Pascale Charpin [Inria, Emeritus, HDR]
- Gaëtan Leurent [Inria, Researcher]
- Anthony Leverrier [Inria, Researcher, HDR]
- María Naya Plasencia [Inria, Senior Researcher, HDR]
- Leo Perrin [Inria, Researcher]
- Nicolas Sendrier [Inria, Senior Researcher, HDR]

Faculty Members

- Magali Bardet [Université de Rouen, Associate Professor]
- Christina Boura [Université de Versailles Saint-Quentin-en-Yvelines, Associate Professor]

Post-Doctoral Fellows

- Simon Apers [Inria, until May 2020]
- Ivan Bardet [Inria, until Jan 2020]
- Ritam Bhaumik [Inria, from Mar 2020]
- Christophe Vuillot [Inria, from Feb 2020]

PhD Students

- Xavier Bonnetain [Inria, until Jan 2020]
- Clemence Bouvier [Inria, from Sep 2020]
- Pierre Briaud [École Normale Supérieure de Lyon, from Oct 2020]
- Rémi Bricout [École Normale Supérieure de Paris]
- Kevin Carrier [Ministère de la Défense, from Feb 2020 until Jun 2020]
- Daniel Coggia [DGA]
- Nicolas David [Inria, from Sep 2020]
- Loic Demange [Thales, CIFRE, from Nov 2020]
- Aurelie Denys [Inria, from Oct 2020]
- Simona Etinski [Université de Paris]
- Antonio Florez Gutierrez [Inria]

- Paul Frixons [Orange Labs, CIFRE]
- Shouvik Ghorai [Sorbonne Université, until Sep 2020]
- Lucien Groues [Sorbonne Université]
- Matthieu Lequesne [Sorbonne Université, until Sep 2020]
- Johanna Loyer [Inria, from Sep 2020]
- Rocco Mora [Sorbonne Université]
- Andrea Olivo [Inria, from Feb 2020]
- Clara Pernot [Inria, from Sep 2020]
- Maxime Remaud [Bull, CIFRE, from May 2020]
- Andre Schrottenloher [Inria]
- Ferdinand Sibleyras [Inria, until Nov 2020]
- Valentin Vasseur [Université de Paris]
- Christophe Vuillot [Inria, until Jan 2020]

Technical Staff

- Yann Barsamian [Inria, Engineer, until Aug 2020]

Interns and Apprentices

- Clemence Bouvier [Inria, from Mar 2020 until Jul 2020]
- Etienne Burle [Inria, from Mar 2020 until Sep 2020]
- Shibam Ghosh [Inria, until Jul 2020]
- Johanna Loyer [Inria, from Mar 2020 until Jul 2020]
- Clara Pernot [Inria, from Mar 2020 until Aug 2020]

Administrative Assistants

- Christelle Guiziou [Inria]
- Mathieu Mourey [Inria]

External Collaborators

- Yann Rotella [Université de Versailles Saint-Quentin-en-Yvelines, from Sep 2020]
- Thomas Vidick [Inria, from Sep 2020]

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 [98], 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 [100] 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 [92]. It also allows to break some well-known modes of operation for MACs and authenticated encryption and provides devastating quantum slide attacks [96]. Other quantum algorithms turned out be useful in this model, such as for instance Kuperberg's algorithm [97]. It allowed to break a tweak [90] to counter the previous attack of [96] or to devise a quantum attack in the superposition model on the POLY1305 MAC primitive [91], 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.

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.

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 Work toward standardization of cryptographic primitives

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 are working to prevent their standardization. We are also working on practical demonstrations of 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 [99] and RANKSIGN [95], and have devised a partial break of the RLCE encryption scheme [93]. In 2020, we obtained a significant

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

breakthrough in solving more efficiently the MinRank problem and the decoding problem in the rank metric [26, 27] 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.

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

5.1 Security analysis of contact tracing applications

During the first wave of the COVID-19 pandemic, several efforts were initiated to develop smartphone applications intended to contribute to contact tracing. The core idea consists in using Bluetooth signal to estimate the distance and the duration of a contact between two app users.

As several such projects became public, an inter-disciplinary collaboration between researchers in cryptography, in security and in technology law, involving the COSMIQ, CARAMBA, PESTO project-teams and other academic institutions, was initiated in order to investigate the consequences of the deployment of such applications in terms of privacy and security. Indeed, a public (and often external) security analysis is always expected for applications dealing with sensitive data such as, in this instance, medical information and each user's social graph. As mentioned in the introduction of Inria's white book on cybersecurity, "the first step in cybersecurity is to identify threats and define a corresponding attacker model. [...] Since zero risk cannot exist, the early detection and mitigation of attacks is as important as the attempt to reduce the risk of successful attacks." Understanding the limits of a system is then necessary to improve its security and to decide whether it can be deployed without taking ill-considered risks, exactly as the side effects of a drug should be documented.

[2] https://csrc.nist.gov/projects/lightweight-cryptography

As political discussions and decisions were taking place, we contributed to these debates by providing an easy to understand description of the security pitfalls that are inherent to bluetooth-based contact tracing: "*le traçage anonyme, un bel oxymore*" [69]. The analysis presented in [69] is, in most cases, independent of the subtleties of the privacy-preserving mechanism, and in particular can be applied to both so-called "centralized" and "decentralized" systems. As a consequence, its authors also worked with researchers based in the UK to provide an English translation https://tracing-risks.com/.

This work had a significant impact (the website received more than 100K unique visitors) and led to further contributions from researchers from the COSMIQ team.

- Anne Canteaut was invited to present the results of [69] to the Commission de la Culture, de l'Education et de la Communication of the Sénat on May 27, 2020 (see https://www.senat.fr/compte-rendu-commissions/20200525/cult.html).

- Gaëtan Leurent identified inconsistencies between the specification of Stopcovid and its implementation pertaining to the amount of data sent to the central server. This was notified to the StopCovid project-team using the bug tracking system[3], and the CNIL required the issue to be fixed in a formal notice[4].

- Anne Canteaut, as the program co-chair of Eurocrypt'20, organized a panel discussion on bluetooth-based contact tracing at this conference. Among the speakers invited at this discussion were designers of such contact tracing applications, including Stopcovid (France), and Swisscovid (Switzerland). This panel discussion was attended by approximately 1900 persons.

- Léo Perrin was invited to present contact tracing applications, their principle, and the corresponding debates at two venues: the seminar of the working group Maths4Covid of the Jacques-Louis Lions lab [87], and to students of the law faculty of Cergy-Pontoise.[5]

- Léo Perrin was invited to a panel on contact tracing at the summer school of the Haifa Technion (Israel)[6] along with designers of the Swiss and Israeli contact tracing applications.

- Anne Canteaut contributed to the definition of an outreach activity for high-school students devoted to epidemics and contact tracing, and initiated by the French Academy of Sciences https://www.academie-sciences.fr/pdf/rapport/guide_module_tracage.pdf.

5.2 Developing a solution for dematerialized lectures, conferences and outreach events

During the first lockdown, Matthieu Lequesne launched the project "ParlonsMaths", which consisted in two hours of mathematical talks live-streamed every day. To organize such an event, together with Fabrice Rouillier from the OURAGAN team, they installed a BigBlueButton server. This solution, allows full dematerialization by broadcasting the videoconferences on a website accompanied by instant messaging to interact with the public. After testing succesfully this solution, they developed for it a complete chain of installations (servers and clients) that are totally free of rights, thus guaranteeing complete control of data circulation. The most important feature is that the solution can easily be deployed on servers of different size, to adapt to events of different scale. Since then, this solution was used to host virtual editions of dozens of outreach events organized by Animath, Inria, and their partners: final of the Alkindi challenge, journée Filles et maths, Rendez-vous des jeunes mathématiciennes, ParlonsMaths, etc. In May 2020, the "Salon des Jeux Mathématiques" was organized on this infrastructure, with over 30 000 virtual visitors in four days, interacting with researchers. This solution was also used by different teaching institutions to organize virtual (or hybrid) classes.

[3] https://gitlab.inria.fr/stopcovid19/stopcovid-android/-/issues/43

[4] https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042125452/

[5] http://www.droitucp.fr/Conf%c3%a9rences%20de%20culture%20g%c3%a9n%c3%a9rale%202020-2021

[6] The 8th Technion Summer School on Cyber and Computer Security: Privacy in Challenging Times (https://cyber.technion.ac.il/2020-summer-school-on-cyber-computer-security/).

5.3 Footprint of research activities

Due to the COVID-19 pandemic, all conferences and workshop have been either cancelled or been modified to be online events. Anne Canteaut played a significant role in enabling this transition as the chair of Eurocrypt 2020, the first cryptography conference intended to take place after stringent lockdowns and travel restrictions were put into place. While we expect in person conferences to resume once the pandemic is under control, online participation should remain possible and will be eased by the experience gathered during the pandemic.

5.4 Impact of research results

The new cryptanalysis results on SHA-1 [47, 39] have helped convince users and industry to deprecate SHA-1. Since the publication of those results, a number of security software have been updated to reduce the usage of SHA-1:

- GnuPG now considers new SHA-1 based identity signatures as invalid;
- OpenSSL no longer allows X.509 certificates signed using SHA-1 at the default security level;
- OpenSSH has published a “future deprecation notice” explaining that SHA-1 signatures will be disabled in a near-future release.

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 all his three candidates that were kept for the second round of the competition, while in the second competition we have one candidate that is a third round finalist and another one which is an alternate third round finalist. 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

6.1 Achievements

NIST competition on post-quantum cryptography: The members of the project-team submitted in 2017 5 candidates to the NIST competition on post-quantum cryptography. After a first selection, three of our candidates moved in 2019 to the second round of the competition, which includes a total of 26 candidates. One of these candidates **Classic McEliece** was accepted in 2020 as one the 4 third round finalists for public-key encryption and key-establishment. Another one, **BIKE**, was accepted at the same time as one of the 5 alternate candidates.

NIST competition on lightweight cryptography: The members of the project-team are involved in the design of 3 authenticated encryption schemes submitted to the NIST lightweight competition. These three ciphers are among the 32 candidates which have been moved to the second round of the competition. They have also been involved in the cryptanalysis of several candidates, and their attacks against one of them (Gimli) have received the best paper award at Asiacrypt.

Chosen-prefix Collision for SHA-1: Gaëtan Leurent and Thomas Peyrin have been working together on Cryptanalysis of SHA-1 within the Associated Team CHOCOLAT. They have designed and implemented a *chosen-prefix* collision attack, a type of attack more powerful than the the previous collision attacks, with concrete impact on real-world protocols. After two months of computation with 900 GPUs, the obtained chosen-prefix collision can be used to mount an impersonation attack against the PGP/GPG Web-Of-Trust[47, 39].

6.2 Awards

Prix de thèse Gilles Kahn 2020 [94].

Thomas Debris-Alazard, *Cryptographie fondée sur les codes: nouvelles approches pour constructions et preuves; contribution en cryptanalyse*,
Sorbonne Universités, UPMC University of Paris 6, 2019

Asiacrypt best paper award [8] .

Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, Ferdinand Sibleyras, New results on Gimli: full-permutation distinguishers and improved collisions, *Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon / Virtual, South Korea, Dec 7, 2020,

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/

Authors: Grégory Landais, Nicolas Sendrier

Contacts: Grégory Landais, Nicolas Sendrier

Participants: Grégory Landais, Nicolas Sendrier

7.2 New platforms

8 New results

8.1 Quantum algorithms and cryptanalysis

Participants Xavier Bonnetain, Rémi Bricout, André Chailloux, Nicolas David, Simona Etinski, Antonio Flórez-Gutiérrez, Paul Frixons, Johanna Loyer, María Naya-Plasencia, Maxime Remaud, André Schrottenloher.

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:

k-xor and k-sum problem. We proposed [42] new quantum algorithms using merging trees to solve the k-xor and k-sum problems for lists of any size. Such algorithms appear in many cryptanalytic techniques. We could show that in the merging setting, these algorithms are optimal and improve the previously known complexities.

Subset sum problem. In [30] improved classical and quantum algorithms for solving the subset-sum problem are proposed. In the classical setting, more general representations of the Becker-Coron-Joux algorithm are presented, including the value '2'. Quantumly, improved algorithms are proposed in the classical memory scenario, using quantum search, and new quantum walks for the subset sum are also proposed, more performant than previous ones.

Simon's algorithm. In the single track session of QIP 2020, we presented a new family of attacks [45] that showed for the first time that Simon's algorithm could be applied in the standard attack model (the so called Q1 model). Up to now, this algorithm was only useful in a very strong attack model where the attacker is allowed to query the cipher quantumly (the so called Q2 model). At the same time, we could improve all the previously known quantum attacks, in both settings, on quite generic constructions, like the FX and Even-Mansour ones. Showing that Q2 attacks could be pushed to the Q1 setting was a surprise for the community.

CSIDH. In [31] we give a comprehensive quantum security analysis of the CSIDH key exchange protocols, revisiting, adapting the existing quantum algorithms that could be applied. We show here that the parameters chosen by the designers had to be doubled in order to achieve the wanted security resistance.

8.2 Symmetric cryptology

Participants Ritam Bhaumik, Xavier Bonnetain, Christina Boura, Clémence Bouvier, Anne Canteaut, Pascale Charpin, Daniel Coggia, Nicolas David, Shibham Gosh, Gaëtan Leurent, María Naya-Plasencia, Clara Pernot, Léo Perrin, André Schrottenloher, Ferdinand Sibleyras.

A significant part of our work dealt with the NIST lightweight cryptography effort, a competition intended to select new symmetric cryptographic standards that are better suited to the IoT than the current ones.

The papers presenting the submissions of the team to this competition were published in the IACR Transactions in Symmetric Cryptology. These candidates are Saturnin [19], Sparkle [16], and Spook [17]. We have also been heavily involved in the cryptanalysis effort associated to this competition. This work has lead to multiple publications which are listed below, each targetting a different second round candidate.

ForkCipher [15]. This algorithm is based on an innovative variation of the block cipher. We have found attacks against the full round primitive, thus challenging the security claims of its designers.

Gimli [8]. We leveraged the slow diffusion provided by the round function of the permutation used by Gimli to identify full round distinguishers. We have also presented other distinguishers (differential/linear and linear). This paper received a best paper award at Asiacrypt 2020.

Spix and Spoc [23] SLiSCP is a cryptographic permutation used by both Spix and Spoc. We have found limited birthday attacks against round-reduced versions of this algorithm. Our attacks are based on improvement of the rebound attacks that can be of independent interest.

Sparkle [28]. Alzette is the non-linear component of Sparkle. We provided strong results about the security it provides against common attacks (differential, linear, integral), and showed it could be used to construct algorithms other than Sparkle, namely two families of (tweakable) block ciphers: C-RAX and T-RAX.

Spook [34]. We have identified undesirable properties of the permutation used by this algorithm. The full round version is vulnerable to limited birthday attacks; the corresponding properties can then be leveraged to perform practical forgery attacks against a round-reduced version of the corresponding AEAD.

TinyJambu [24]. More accurate estimations of the security provided by the permutation of TinyJambu against differential attack were performed, and found that this attack was more powerful than expected by the designers of this algorithm.

We have also obtained new results not related to this competition:

- New hash functions are being designed in order to be used within sophisticated zero-knowledge protocols. Due to this requirement, they have to be defined using arithmetic operations over large finite fields. Together with an international team of cryptographers, we found flaws in several such hash functions [29]. In a yet unpublished follow-up work, we also investigated another such hash function [71].

- Improving key-recovery in linear attacks [36]. Methods based on the Fast Fourier Transform (FFT) were known to speed up key recovery in linear attacks. We improved upon this method using a matrix-based approach which, when applied to the lightweight block cipher PRESENT, leads to the best attacks against this primitive.

- The Boomerang Connectivity Table (BCT) is a tool used to assess the resistance that an S-box offers against boomerang attacks. We have investigated the BCT of S-boxes constructed using the most common design strategies [25].

- Improvement of the MILP modeling of differential and linear trails [18]. Both designers and cryptanalysts rely more and more on MILP solvers to find the best differential and linear trails in a cipher. The process leading from the specification of the round function to the description of a MILP system was substantially improved.

- Iterated FX construction to construct tweakable block ciphers [44]. A generic technique for constructing a tweakable block cipher using only a regular block cipher is presented along with security bounds. The tightness of these bounds is also established.

- We have obtained the first *chosen-prefix* collision attack against SHA-1, a type of attack more powerful than the the previous collision attacks, with concrete impact on real-world protocols. In particular, it can be used to mount an impersonation attack against the PGP/GPG Web-Of-Trust[47, 39].

8.3 Post-quantum asymmetric cryptology

Participants Magali Bardet, Pierre Briaud, Rémi Bricout, Etienne Burle, Kevin Carrier, André Chailloux, Loïc Demange, Matthieu Lequesne, Rocco Mora, Maxime Remaud, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur.

Our work in this area can be decomposed as follows

- involvement in the NIST competition aiming at standardizing quantum safe public key cryptosystems, by developing our solutions that are/were still in the competition, namely `BIKE`, `Classic McEliece` and `ROLLO` and attacking other schemes;
- design and analysis of new code-based solutions.

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).

NIST competition.

- Development of our second round candidates BIKE, Classic McEliece and ROLLO. The most mature scheme `Classic McEliece` was only marginally improved and modified. It was promoted in 2020 to a third round finalist. On the other hand, there were several concerns and NIST requests with BIKE that we addressed (narrowing down to a single variant, security proof, estimating the decoding failure rate, hardware design), see `BIKE`, [43, 79]. BIKE was promoted to an alternate third round finalist and the NIST has made it clear that it was its intention to standardize either BIKE or HQC depending on whether it will be possible to give a convincing argument for estimating the decoding failure rate of BIKE or not.

- Improvement of algorithms for decoding a code in the rank metric and solving the MinRank problem by using Gröbner basis techniques [26, 27]. This gave an attack on all second round rank metric code-based schemes. As a result of this, all rank metric based proposals which were second round candidates at the NIST competition were dismissed for the third round. These results were also used more recently to attack the third round signature candidate Rainbow [7] and the alternate third round signature candidate GeMSS[8].

Design and analysis of new code-based schemes.

There was no code-based signature scheme that went to the second round of the NIST competition: all of them got broken during the first round. This is a pity, since it would be desirable to have several candidates relying on different computational assumptions. The situation at the third round is even worse. We have only lattice-based and multivariate finalists left here. Moreover as mentioned above, the third round multivariate candidate was attacked by using our improved MinRank solver. This improved solver also attacked the alternate third round multivariate candidate.

However, since 2017 there has been steady progress for constructing secure code-based signature schemes and there are now potentially several strong candidates: Wave [9], Durandal or schemes based on the Fiat-Shamir paradigm. We have worked on obtaining tight security reductions in the classical and quantum model that apply in particular to Wave [32] and on reducing drastically the rejection rate in it [81]. We have also improved slightly the best generic decoding algorithms [63].

8.4 Quantum information

Participants Simon Apers, Ivan Bardet, Rémi Bricout, André Chailloux, Aurélie Denys, Shouvik Gorai, Lucien Grouès, Anthony Leverrier, Andrea Olivo, Jean-Pierre Tillich, Christophe Vuillot.

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

[7] W. Beullens, *Improved Cryptanalysis of UOV and Rainbow*, IACR eprint Oct. 2020 `https://eprint.iacr.org/2020/1343`.

[8] C. Tao, A. Petzoldt, J. Ding, *Improved Key Recovery of the HFEv- Signature Scheme*, eprint Nov. 2020 `https://eprint.iacr.org/2020/1424`.

[9] T. Debris, N. Sendrier, J.P. Tillich, *Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes*, ASIACRYPT 2019 (best paper), LNCS 11921, pp. 21–51.

- A major challenge in the field of quantum key distribution is to improve the range of the protocols, and communication via satellites offers a promising approach compared to fiber-based implementations. We have studied the feasibility of continuous-variable quantum key distribution with satellites in [21] and found that low-orbit satellites can indeed realistically help distribute secret keys. In parallel, we continue the development of security proofs for continuous-variable quantum key distribution, notably in the context of the European project CiViQ, and gave an invited talk at the major annual conference on quantum cryptography, QCRYPT 2020 [49].

- In the context of quantum error correcting codes, we have been developing several new decoding algorithms for constant rate quantum LDPC codes. A theoretical result demonstrating that quantum fault-tolerance can be obtained with constant overhead was invited as a research highlight of the Communications of the ACM [22]. We have tested numerically the corresponding codes and decoder in[76] and found them to be competitive with the state-of-the-art decoders for quantum LDPC codes, while displaying a reduced complexity. Recently, we considered an alternative decoder consisting in formulating the decoding problem as a linear program, and also obtained encouraging numerical results [35].

- Our work on quantum error correction also focuses on the construction of interesting quantum LDPC codes. In particular, we have devised a family of locally testable quantum codes with a record soundness parameter[40]. More recently, we initiated the systematic study of a general class of quantum LDPC codes generalizing the hypergraph product code construction, and obtain constant rate quantum LDPC codes with a conjectured minimum distance that would beat the $\sqrt{n}$ bound for the minimum distance [77].

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

LOTUS:(02/2021 → 30/06/2021) 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 Inria international partners

Informal International Partners

- Nanyang Technological University (Singapore): cryptanalysis of symmetric primitives.

- Ruhr-Universität Bochum (Germany): design and cryptanalysis of symmetric primitives.

- NTT Secure Platforms Laboratories (Japan): quantum cryptanalysis, symmetric cryptography.

- CWI (the Netherlands): links between lattice based and code based cryptography.

10.1.1 Participation in International Programs

- **ANR SELECT** (07/21→06/24)
  Security Evaluation of Lightweight Encryption using new Cryptanalysis Techniques
  ANR Program: AAP Générique 2020 (PRCI)
  Partners: Inria COSMIQ, Nanyang Technological University (Singapour)
  476 kEuros
  In the last decades, we have seen a large deployment of smart devices and contact-less smart cards, with applications to the Internet of Things and smart cities. These devices have strong security requirements as they communicate sensitive data by radio, but they have very low resources available: constrained computing capabilities and limited energy. This led to security disasters with the use of weak home-made cryptography such as KeeLoq or MIFARE. More recently, the academic cryptography community has come up with dedicated lightweight designs such as PRESENT or Skinny, and the NIST is currently organizing a competition to select the next worldwide standards. The goal of this project is to perform a wide security evaluation of the designs submitted to the NIST competition, and of lightweight cryptographic algorithms in general. We will use latest cryptanalysis advances, but also propose new attacks; study classical attacks, but also physical ones (very powerful in such scenarios).

10.2 International research visitors

Thomas Vidick holds an Inria International Chair on the 2020-2024 period, hosted by our team. Thomas' research revolves around the understanding the capabilities, and limitations, of quantum devices for computation and secure communication. He is a leading expert in this domain, in particular he has developed and shown the security of schemes for (post-quantum) randomness extraction, certified randomness, key distribution, and delegated computation. His work on quantum interactive proofs has led to a deeper understanding of entanglement, including better entanglement tests and security proofs in device-independent cryptography. The aim is to develop a long-lasting collaboration with our team on the themes of quantum complexity, error-correcting codes, and cryptography. He gave a very inspiring FSMP course held at the Institute Henri Poincaré on interactive proofs with quantum devices this fall. See http://users.cms.caltech.edu/~vidick/teaching/fsmp/index.html.

10.3 European initiatives

10.3.1 FP7 & H2020 Projects

ERC QUASYModo

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

Program: ERC starting grant

- Duration: September 2017 - August 2023

  PI: María Naya-Plasencia

  As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover's algorithm, which allows exhaustive key searches in the square root of the normal complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post- quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which neither exists nor has ever been studied. This is the big gap I have identified and that I plan to fill with this project. Next, doubling the key length is not a trivial task and needs to be carefully studied. My ultimate aim is to propose efficient solutions secure in the post-quantum world with the help of our previously obtained quantum symmetric cryptanalysis toolbox. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications. The main challenge of QUASYModo is to redesign symmetric cryptography for the post-quantum world.

H2020 FET Flagship on Quantum Technologies - CiViQ

Title: CiViQ *Continuous Variable Quantum Communications*

Program: H2020 FET Flagship on Quantum Technologies

Duration: October 2018 - September 2021

PI: Anthony Leverrier

The goal of the CiViQ project is to open a radically novel avenue towards flexible and cost-effective integration of quantum communication technologies, and in particular Continuous-Variable QKD, into emerging optical telecom- munication networks. CiViQ aims at a broad technological impact based on a systematic analysis of telecom-defined user-requirements. To this end CiViQ unites for the first time a broad interdisciplinary community of 21 partners with unique breadth of experience, involving major telecoms, integrators and developers of QKD. The work targets advancing both the QKD technology itself and the emerging "software network" approach to lay the foundations of future seamless integration of both. CiViQ will culminate in a validation in true telecom network environment. Project-specific network integration and software development work will empower QKD to be used as a physical-layer-anchor securing critical infrastruc- tures, with demonstration in QKD-extended software-defined networks.

10.3.2 Collaborations in European programs, except FP7 and H2020

QCDA

Program: QuantERA ERA-NET Cofund in Quantum Technologies

Project acronym: QCDA

Project title: Quantum Code Design and Architecture

Duration: February 2018 - November 2021

Coordinator: Earl Campbell, University of Sheffield, UK

Other partners: University of Sheffield (UK), TU Delft (Netherlands), TU Munich (Germany), University College London (UK)

Inria contact: Anthony Leverrier

General purpose quantum computers must follow a fault-tolerant design to prevent ubiquitous decoherence processes from corrupting computations. All approaches to fault-tolerance demand extra physical hardware to perform a quantum computation. Kitaev's surface, or toric, code is a popular idea that has captured the hearts and minds of many hardware developers, and has given many people hope that fault-tolerant quantum computation is a realistic prospect. Major industrial hardware developers include Google, IBM, and Intel. They are all currently working toward a fault-tolerant architecture based on the surface code. Unfortunately, however, detailed resource analysis points towards substantial hardware requirements using this approach, possibly millions of qubits for commercial applications. Therefore, improvements to fault-tolerant designs are a pressing near-future issue. This is particularly crucial since sufficient time is required for hardware developers to react and adjust course accordingly.

This consortium will initiate a European co-ordinated approach to designing a new generation of codes and protocols for fault-tolerant quantum computation. The ultimate goal is the development of high-performance architectures for quantum computers that offer significant reductions in hardware requirements; hence accelerating the transition of quantum computing from academia to industry. Key directions developed to achieve these improvements include: the economies of scale offered by large blocks of logical qubits in high-rate codes; and the exploitation of continuous-variable degrees of freedom.

The project further aims to build a European community addressing these architectural issues, so that a productive feedback cycle between theory and experiment can continue beyond the lifetime of the project itself. Practical protocols and recipes resulting from this project are anticipated to become part of the standard arsenal for building scalable quantum information processors.

10.4 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.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- PQCrypto 2020, April 2020, Paris (France): N. Sendrier: general chair; J.-P. Tillich: program co-chair
- Dagstuhl seminar 21421 "Quantum Cryptanalysis": October 17-22, 2021, Dagstuhl (Germany): M. Naya-Plasencia co-organizer
- Dagstuhl seminar 22141 "Symmetric Cryptography": April 3-8, 2022, Dagstuhl (Germany): M. Naya-Plasencia co-organizer

Member of the organizing committees

- PQCrypto 2020, April 2020, M. Lequesne, V. Vasseur

11.1.2 Scientific events: selection

Chair of conference program committees

- Co-editor-in-chief of IACR Transactions on Symmetric Cryptology starting from 2019: Gaëtan Leurent.
- Co-chair of the Program Committee of Eurocrypt 2020, virtual, May 2020: Anne Canteaut
- Co-chair of the Program Committee of FSE 2020, Athens, Greece, March 2020: Gaëtan Leurent.
- Co-chair of the Program Committee of Eurocrypt 2021, Zagreb, Croatia, October 2021: Anne Canteaut
- Co-chair of the Program Committee of WCC 2021 (post-poned to March 2022), Rostock, Germany: Léo Perrin.

Member of the conference program committees

- FSE 2020: March 22-26, 2020, Athens, Greece, (C. Boura, A. Canteaut, G. Leurent co-chair, L. Perrin)
- PQCrypto 2020: April 15-17, 2020, Paris, France (A. Chailloux, M. Naya-Plasencia, N. Sendrier, J.P. Tillich);
- CBCrypto 2020: May 9-10, 2020, Zagreb, Croatia, (J.-P. Tillich);
- Eurocrypt 2020: May 10-14, 2020, virtual, (A. Canteaut co-chair, M. Naya-Plasencia);
- ISIT 2020: June 21-26, 2020, virtual, Los Angeles, USA, (J.-P. Tillich);
- Crypto 2020: August 17-21, 2020, virtual, Santa-Barbara, USA, (M. Naya-Plasencia);
- ISIT 2021: July 12-20, 2021, Melbourne, Australia, (J.-P. Tillich);
- PQCrypto 2021: July 20-22, 2021, Daejeon, South Korea (A. Chailloux, N. Sendrier, J.P. Tillich);
- Eurocrypt 2021: October 17-21, 2020, Zagreb, Croatia, (A. Canteaut co-chair, M. Naya-Plasencia);

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 editor: P. Charpin.
- *Finite Fields and Applications*, associate editors: A. Canteaut, P. Charpin.
- *IACR Transactions on Symmetric Cryptology*, associate editors: C. Boura, G. Leurent (co-editor in chief), M. Naya-Plasencia, L. Perrin.
- *Quantum (the open journal for quantum science)*, associate editor: A. Leverrier.
- *IEEE Transactions on Information Theory*, associate editor: A. Canteaut.
- *Designs, Codes and Cryptography*, guest co-editor of the special issue on *Coding and Cryptography*, A. Canteaut.

11.1.4 Invited talks

- L. Perrin was invited to a panel discussion on contact tracing at the 8th Technion Summer School on Cyber and Computer Security, September 7-10, 2020.
- A. Leverrier gave an invited talk *Security proofs for continuous-variable quantum key distribution*, at QCrypt 2020, virtual, August 10-14, 2020 [49].
- M. Naya-Plasencia gave a tutorial on *New results on Symmetric Quantum Cryptanalysis and Perspectives*at Qcrypt 2020, virtual, August 10-14, 2020, [].
- N. Sendrier gave an invited talk on *Code-Based Cryptography Designs, the Ancient and the Modern*, Indian Workshop on Post-Quantum Cryptography, November 17-18, 2020 [50].

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.
- N. Sendrier serves on the steering committee of Post-quantum cryptography (PQCrypto).
- P. Charpin, N. Sendrier and JP Tillich serve on the steering committee of the WCC conference series.
- A. Canteaut serves on the International Scientific Advisory Board of the Flemish Strategic Research Program on Cybersecurity.
- A. Canteaut served on the IACR test-of-time award Committee for 2020.

11.1.6 Research administration

- A. Canteaut serves as Head of Inria Evaluation Committee since September 2019.
- P. Charpin serves on the Comité Parité at Inria.
- G. Leurent serves on the Inria Paris CSD Committee (Comité de suivi doctoral).
- M. Naya-Plasencia serves on the Inria Evaluation Committee since September 2019.
- A. Leverrier serves on the steering committee of the Domaine D'Intérêt Majeur SIRTEQ (Quantum Technologies in IdF).

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

- 2020 Jury d'admissibilité Inria CRCN national (A. Canteaut);
- 2020 Head of the jury d'admissibilité Inria DR2, (A. Canteaut);
- 2020 Jury d'admissibilité Inria DR2, (M. Naya-Plasencia)
- 2020 Jury d'admission Inria CRCN, (A. Canteaut);
- 2020 Jury d'admission Inria DR2, (A. Canteaut);
- 2020 Head of the jury d'admissibilité CRCN/ISFP of Inria Saclay (M. Naya-Plasencia);
- 2020 Jury d'admissibilité CRCN/ISFP of Inria de Paris (J.-P.Tillich);
- 2021 Jury d'admissibilité CRCN/ISFP of Inria de Paris (J.-P.Tillich);
- 2021 Head of the jury d'admissibilité Inria DR2, (A. Canteaut);
- 2021 Jury d'admissibilité Inria DR2, (M. Naya-Plasencia)

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 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 and quantum cryptography, 12 hours, M2, University Paris-Diderot (MPRI), 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 : Kevin Carrier, *Presque-collisions et applications au décodage générique et à la reconnaissance de codes correcteurs d'erreurs*, Sorbonne Université, June 19, 2020, supervisor: N. Sendrier and JP Tillich
- PhD : Ferdinand Sibleyras, *Security of modes of operation*, Sorbonne Université, October 23, 2020, supervisor: G. Leurent and A. Canteaut
- PhD : André Schrottenloher, *Long-term security of symmetric primitives*, Sorbonne Université, February 8, 2021 supervisors: A. Chailloux and M. Naya-Plasencia
- PhD : Rémi Bricout, *Etude de scénarios non-locaux quantiques à l'aide d'outils de la théorie de l'information quantique*, March 30,2021, supervisors: A. Chailloux and A. Leverrier
- PhD in progress: Matthieu Lequesne, *Attaques par canaux cachés sur les cryptosystèmes à base de codes MDPC quasi-cycliques*, since September 2017, supervisor: N. Sendrier

- PhD in progress: Valentin Vasseur, *Etude du décodage des codes QC-MDPC*, March 29, 2021, supervisor: N. Sendrier.

- PhD in progress: Shouvik Ghorai, *Continuous-variable quantum cryptographic protocols*, February 12, 2021, supervisors: E. Diamanti (UPMC), A. Leverrier

- PhD in progress: Andrea Olivo, *Partir de contraintes relativistes pour faire de la cryptographie quantique*, since November 2017, supervisors: A. Chailloux and F. Grosshans (laboratoire Aimé Cotton).

- PhD in progress: Daniel Coggia, *Cryptanalysis techniques for lightweight ciphers*, since September 2018, supervisors: A. Canteaut and C. Boura.

- 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: A. Florez Gutierrez, *Secure Symmetric Primitives and the Post-Quantum World*, since September 2019, supervisor: M. Naya Plasencia

- PhD in progress: Lucien Grouès, *Decoding algorithms for quantum LDPC codes*, since October 2019, supervisors: A. Leverrier and O. Fawzi (Ecole Normale Supérieure de Lyon)

- PhD in progress: Rocco Mora, *Algebraic structures in code-based cryptography*, since October 2019, supervisor: JP Tillich

- PhD in progress: Paul Frixons, *Impact d'un attaquant quantique dans les télécommunications*, since November 2019, supervisor: M. Naya Plasencia

- PhD in progress: Maxime Remaud, *Quantum cryptanalysis in code-based and lattice-based cryptography*, since July 2020, supervisor: JP Tillich

- PhD in progress: Clémence Bouvier, *Analyse de la sécurité de primitives symétriques dédiées à divers usages émergents*, since September 2020, supervisor: 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: JP Tillich

- PhD in progress: Aurélie Denys, *Preuves de sécurité pour des protocoles de cryptographie quantique à variables continues*, since October 2020, supervisor: A. Leverrier

- PhD in progress: Johanna Loyer, *Algorithmes quantiques sur les réseaux euclidiens*, since October 2020, supervisor: A. Chailloux

- PhD in progress: Loïc Demange, *Mise en œuvre de BIKE : vulnérabilités et contre-mesures*, since November 2020, supervisor: N. Sendrier

11.2.3 Juries

- Shouvik Ghorai, Continuous-variable quantum cryptographic protocols, Sorbonne Université, February 12, 2021, supervisors: A. Leverrier (supervisor)

- Valentin Vasseur, Etude du décodage des codes QC-MDPC, Université de Paris, March 29, 2021, supervisor: N. Sendrier (supervisor), J.P. Tillich

- C. Vuillot, *Fault-tolerant quantum computation: theory and practice*, TU Delft, January 15, 2020, A. Leverrier

- P. Lacharme, HDR *Études en sécurité informatique*, Université Normandie, February 6, 2020, M. Naya-Plasencia (reviewer)

- N. Bardeh, *New Approaches to the Cryptanalysis of Block Ciphers* , Bergen University, Norway, March 10, 2020, M. Naya-Plasencia (reviewer)

- Aurélien Bonvard, *Algorithmes de détection et de reconstruction de codes correcteurs basés sur des informations souples*, May 25, 2020, J.-P. Tillich (reviewer)

- Kevin Carrier, *Presque-collisions et applications au décodage générique et à la reconnaissance de codes correcteurs d'erreurs*, Sorbonne Université, June 19, 2020, N. Sendrier and J.-P. Tillich (supervisors)

- U. Chabaud, *Continuous Variable Quantum Advantages and Applications in Quantum Optics*, Sorbonne Université, July 22, 2020, A. Leverrier (reviewer)

- Ferdinand Sibleyras, *Security of modes of operation*, Sorbonne Université, October 23, 2020, G. Leurent and A. Canteaut (supervisors)

- Gilbert Ndollane Dione, *Schéma d'identification et Mécanisme d'encapsulation de clé* University Cheikh Anta DIOP of Dakar, November 30, 2020, N. Sendrier (reviewer)

- Riad Ladjel, *Secure Distributed Computations for the Personal Cloud*, Univ. Paris Saclay, December 8, 2020, A. Canteaut.

- Vincent Corlay, *Decoding algorithms for lattices*, Télécom Paris, December 9, 2020, J.-P. Tillich (reviewer)

- Nicolas Aragon, *Cryptographie à base de codes correcteurs d'erreurs en métrique rang et applications*, University of Limoges, December 11, 2020, J.-P. Tillich

- Irene Villa, *Analysis, classification and construction of optimal cryptographic Boolean functions*, Univ. of Bergen, Norway, January 4, 2021, A. Canteaut (opponent).

- André Schrottenloher, *Long-term security of symmetric primitives*, Sorbonne Université, February 8, 2021, A. Chailloux and M. Naya-Plasencia (supervisors)

11.3 Popularization

11.3.1 Internal or external Inria responsibilities

- **Association Animath**: M. Lequesne serves on the board of Animath.

- M. Lequesne is also member of the scientific committee of the French Tournament of Young Mathematicians: designing the problems for the competition, jury member (chair of a jury) ; member of the scientific committee of the International Tournament of Young Mathematicians: designing the problems for the competition, jury member (chair of a jury) ; Member of the scientific committee of the Correspondances des Jeunes Mathématicien.ne.s: designing the problems for the competition.

11.3.2 Articles and contents

M. Naya-Plasencia wrote the chapter *La cryptanalyse des fonctions algébriques* of the book *"13 Défis de la cybersécurité"*. Ed. Gildas Avoine et Marc-Olivier Killijian, CNRS Editions, 2020.

11.3.3 Education

- **Alkindi cipher challenge:** Several members of the project-team are involved in the cipher challenge for high-school students "concours Alkindi" http://www.concours-alkindi.fr/. Mathieu Lequesne serves as a co-organizer of the challenge, preparing the three rounds and the final. He is also involved in the conception of the exercises.

- **Parlons Maths** During the first lockdown, Matthieu Lequesne launched the project "ParlonsMaths", which consisted in two hours of mathematical talks live-streamed every day. Several members of the project team contributed by giving a talk. This project is part of Inria's Covid mission. https://www.inria.fr/en/parlonsmaths-dematherialization

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] ***Best Paper***
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, B. Collins and G. Sapra. 'Characterization of Equivariant Maps and Application to Entanglement Detection'. In: *Annales Henri Poincaré* 21.10 (Oct. 2020), pp. 3385–3406. DOI: 10.1007/s00023-020-00941-1. URL: https://hal.archives-ouvertes.fr/hal-03140648.

[15] A. Bariant, N. David and G. Leurent. 'Cryptanalysis of Forkciphers'. In: *IACR Transactions on Symmetric Cryptology* 2020.1 (7th May 2020), pp. 233–265. DOI: 10.13154/tosc.v2020.i1.233-265. URL: https://hal.inria.fr/hal-03135299.

[16] C. Beierle, A. Biryukov, L. Cardoso dos Santos, J. Großschädl, L. Perrin, A. Udovenko, V. Velichkov and Q. Wang. 'Lightweight AEAD and Hashing using the Sparkle Permutation Family'. In: *IACR Transactions on Symmetric Cryptology*. Special Issue on Designs for the NIST Lightweight Standardisation Process 2020.S1 (22nd June 2020), pp. 208–261. DOI: 10.13154/tosc.v2020.iS1.208-261. URL: https://hal.inria.fr/hal-03135807.

[17] D. Bellizia, F. Berti, O. Bronchain, G. Cassiers, S. Duval, C. Guo, G. Leander, G. Leurent, I. Levi, C. Momin, O. Pereira, T. Peters, F.-X. Standaert, B. Udvarhelyi and F. Wiemer. 'Spook: Sponge-Based Leakage-Resistant Authenticated Encryption with a Masked Tweakable Block Cipher'. In: *IACR Transactions on Symmetric Cryptology*. Special Issue on Designs for the NIST Lightweight Standardisation Process 2020.S1 (22nd June 2020), pp. 295–349. DOI: 10.13154/tosc.v2020.iS1.295-349. URL: https://hal.inria.fr/hal-03136493.

[18] C. Boura and D. Coggia. 'Efficient MILP Modelings for Sboxes and Linear Layers of SPN ciphers'. In: *IACR Transactions on Symmetric Cryptology* 2020.3 (28th Sept. 2020), pp. 327–361. DOI: 10.13154/tosc.v2020.i3.327-361. URL: https://hal.inria.fr/hal-03046211.

[19] A. Canteaut, S. Duval, G. Leurent, M. Naya-Plasencia, L. Perrin, T. Pornin and A. Schrottenloher. 'Saturnin: a suite of lightweight symmetric algorithms for post-quantum security'. In: *IACR Transactions on Symmetric Cryptology*. Special Issue on Designs for the NIST Lightweight Standardisation Process 2020.S1 (22nd June 2020), pp. 160–207. DOI: 10.13154/tosc.v2020.iS1.160-207. URL: https://hal.inria.fr/hal-03046716.

[20] D. Coggia and A. Couvreur. 'On the security of a Loidreau rank metric code based encryption scheme'. In: *Designs, Codes and Cryptography* 88.9 (Sept. 2020), pp. 1941–1957. DOI: 10.1007/s10623-020-00781-4. URL: https://hal.archives-ouvertes.fr/hal-03049694.

[21] D. Dequal, L. T. Vidarte, V. R. Rodriguez, G. Vallone, P. Villoresi, A. Leverrier and E. Diamanti. 'Feasibility of satellite-to-ground continuous-variable quantum key distribution'. In: *npj Quantum Information* 7.1 (4th Jan. 2021), p. 10. DOI: 10.1038/s41534-020-00336-4. URL: https://hal.archives-ouvertes.fr/hal-03093471.

[22] O. Fawzi, A. Grospellier and A. Leverrier. 'Constant overhead quantum fault tolerance with quantum expander codes'. In: *Communications of the ACM* 64.1 (Jan. 2021), pp. 106–114. DOI: 10.1145/3434163. URL: https://hal.inria.fr/hal-03135932.

[23] A. Hosoyamada, M. Naya-Plasencia and Y. Sasaki. 'Improved Attacks on sLiSCP Permutation and Tight Bound of Limited Birthday Distinguishers'. In: *IACR Transactions on Symmetric Cryptology* 2020.4 (10th Dec. 2020), pp. 147–172. DOI: 10.46586/tosc.v2020.i4.147-172. URL: https://hal.inria.fr/hal-03135330.

[24] D. Saha, Y. Sasaki, D. Shi, F. Sibleyras, S. Sun and Y. Zhang. 'On the Security Margin of TinyJAMBU with Refined Differential and Linear Cryptanalysis'. In: *IACR Transactions on Symmetric Cryptology* 2020.3 (28th Sept. 2020), pp. 152–174. DOI: 10.13154/tosc.v2020.i3.152-174. URL: https://hal.inria.fr/hal-03135912.

[25] S. Tian, C. Boura and L. Perrin. 'Boomerang Uniformity of Popular S-box Constructions'. In: *Designs, Codes and Cryptography* 88.9 (Sept. 2020), pp. 1959–1989. DOI: 10.1007/s10623-020-00785-0. URL: https://hal.inria.fr/hal-03136148.

International peer-reviewed conferences

[26] 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, 10th May 2020, pp. 64–93. DOI: 10.1007/978-3-030-45727-3_3. URL: https://hal-unilim.archives-ouvertes.fr/hal-02303015.

[27] 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: *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part {I}*. 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, 6th Dec. 2020, pp. 507–536. DOI: 10.1007/978-3-030-64837-4_17. URL: https://hal.inria.fr/hal-03133479.

[28] C. Beierle, A. Biryukov, L. Cardoso dos Santos, J. Großschädl, L. Perrin, A. Udovenko, V. Velichkov and Q. Wang. 'Alzette: A 64-Bit ARX-box: (feat. CRAX and TRAX)'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. 12172. Lecture Notes in Computer Science. Santa Barbara, United States, 10th Aug. 2020, pp. 419–448. DOI: 10.1007/978-3-030-56877-1_15. URL: https://hal.inria.fr/hal-03135836.

[29] T. Beyne, A. Canteaut, I. Dinur, M. Eichlseder, G. Leander, G. Leurent, M. Naya-Plasencia, L. Perrin, Y. Sasaki, Y. Todo and F. Wiemer. 'Out of Oddity – New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems'. In: *Advances in Cryptology – CRYPTO 2020, Part III*. CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. 12172. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 299–328. DOI: 10.1007/978-3-030-56877-1_11. URL: https://hal.inria.fr/hal-03090185.

[30] X. Bonnetain, R. Bricout, A. Schrottenloher and Y. Shen. 'Improved Classical and Quantum Algorithms for Subset-Sum'. 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, 7th Dec. 2020, pp. 633–666. DOI: 10.1007/978-3-030-64834-3_22. URL: https://hal.inria.fr/hal-03046017.

[31] X. Bonnetain and A. Schrottenloher. 'Quantum Security Analysis of CSIDH'. In: EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 12106. Lecture Notes in Computer Science. Zagreb / Virtual, Croatia, 11th May 2020, pp. 493–522. DOI: 10.1007/978-3-030-45724-2_17. URL: https://hal.inria.fr/hal-01896046.

[32] A. Chailloux and T. Debris-Alazard. 'Tight and Optimal Reductions for Signatures Based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures'. In: PKC 2020 - IACR International Conference on Public-Key Cryptography. Vol. 12111. Lecture Notes in Computer Science. Edinburgh / Virtual, United Kingdom, 29th Apr. 2020, pp. 453–479. DOI: 10.1007/978-3-030-45388-6_16. URL: https://hal.inria.fr/hal-03138441.

[33] P. Charpin. 'Crooked functions'. In: *Finite Fields Applications*. Proceedings of the 14th International Conference on Finite Fields and their Applications. Vancouver, Canada, 26th Oct. 2020, pp. 87–102. DOI: 10.1515/9783110621730-007. URL: https://hal.inria.fr/hal-02969132.

[34] P. Derbez, P. Huynh, V. Lallemand, M. Naya-Plasencia, L. Perrin and A. Schrottenloher. 'Cryptanalysis Results on Spook: Bringing Full-round Shadow-512 to the Light'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Vol. 12172. Lecture Notes in Computer Science. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 359–388. DOI: 10.1007/978-3-030-56877-1_13. URL: https://hal.inria.fr/hal-02944908.

[35] O. Fawzi, L. Grouès and A. Leverrier. 'Linear programming decoder for hypergraph product quantum codes'. In: IEEE ITW 2020 - IEEE Information theory workshop 2020. Riva del Garda / Virtual, Italy, 11th Apr. 2021. URL: https://hal.inria.fr/hal-03135797.

[36] A. Florez Gutierrez and M. Naya-Plasencia. 'Improving Key-Recovery in Linear Attacks: Application to 28-Round PRESENT'. In: EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic. Vol. 12105. Lecture Notes in Computer Science. Zagreb / Virtual, Croatia, 1st May 2020, pp. 221–249. DOI: 10.1007/978-3-030-45721-1_9. URL: https://hal.inria.fr/hal-03139574.

[37] 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. Vol. 12491. Lecture Notes in Computer Science. Daejeon / Virtual, South Korea, 7th Dec. 2020, pp. 33–63. DOI: 10.1007/978-3-030-64837-4_2. URL: https://hal.inria.fr/hal-03045986.

[38] S. Jaques and A. Schrottenloher. 'Low-gate Quantum Golden Collision Finding'. In: SAC 2020 - Selected Areas in Cryptography. Halifax / Virtual, Canada, 19th Oct. 2020. URL: https://hal.inria.fr/hal-03046039.

[39] G. Leurent and T. Peyrin. 'SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust'. In: USENIX 2020 - 29th USENIX Security Symposium. Boston / Virtual, United States: https://www.usenix.org/conference/usenixsecurity20, 12th Aug. 2020, pp. 1839–1856. URL: https://hal.inria.fr/hal-03136301.

[40] A. Leverrier, V. Londe and G. Zémor. 'Towards Local Testability for Quantum Coding'. In: ITCS 2021 - 12th Conference on Innovations in Theoretical Computer Science. Vol. 185. Leibniz International Proceedings in Informatics (LIPIcs). Washington / Virtual, United States, 6th Jan. 2021, 65:1–65:11. DOI: 10.4230/LIPIcs.ITCS.2021.65. URL: https://hal.inria.fr/hal-03135738.

[41] Y. Li, G. Leurent, M. Wang, W. Wang, G. Zhang and Y. Liu. 'Universal Forgery Attack against GCM-RUP'. In: CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020. Vol. 12006. Lecture Notes in Computer Science. San Francisco, United States, 24th Feb. 2020, pp. 15–34. DOI: 10.1007/978-3-030-40186-3_2. URL: https://hal.inria.fr/hal-02424899.

[42] M. Naya-Plasencia and A. Schrottenloher. 'Optimal Merging in Quantum k-xor and k-sum Algorithms'. In: EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic. Vol. 12106. Lecture Notes in Computer Science. Zagreb / Virtual, Croatia, 11th May 2020, pp. 311–340. DOI: 10.1007/978-3-030-45724-2_11. URL: https://hal.inria.fr/hal-03046540.

[43] N. Sendrier and V. Vasseur. 'About Low DFR for QC-MDPC Decoding'. In: PQCrypto 2020 - Post-Quantum Cryptography 11th International Conference. Vol. 12100. Lecture Notes in Computer Science. Paris / Virtual, France, 10th Apr. 2020, pp. 20–34. DOI: 10.1007/978-3-030-44223-1_2. URL: https://hal.inria.fr/hal-03139672.

[44] F. Sibleyras. 'Generic Attack on Iterated Tweakable FX Constructions'. In: CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020. Vol. 12006. Lecture Notes in Computer Science. San Francisco, United States, 24th Feb. 2020, pp. 1–14. DOI: 10.1007/978-3-030-40186-3_1. URL: https://hal.inria.fr/hal-02424953.

Conferences without proceedings

[45] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki and A. Schrottenloher. 'Quantum Attacks without Superposition Queries: The Offline Simon's Algorithm'. In: QIP 2020 - 23rd Annual Conference on Quantum Information Processing. Shenzhen, China, 6th Jan. 2020. URL: https://hal.inria.fr/hal-03142816.

[46] A. Canteaut, T. Beyne, I. Dinur, M. Eichlseder, G. Leander, G. Leurent, M. Naya Plasencia, L. Perrin, Y. Sasaki, Y. Todo and F. Wiemer. 'Security of the STARK-friendly hash functions'. In: Dagstuhl Seminar 20041 - Symmetric Cryptography. Dagstuhl, Germany, 19th Jan. 2020. URL: https://hal.inria.fr/hal-03143904.

[47] G. Leurent and T. Peyrin. 'The First Chosen-Prefix Collision on SHA-1'. In: Real World Crypto 2020 - Real World Crypto Symposium. New York, United States: https://rwc.iacr.org/2020/, 8th Jan. 2020. URL: https://hal.inria.fr/hal-03136460.

[48] G. Leurent and T. Peyrin. 'The First Chosen-Prefix Collision on SHA-1'. In: Dagstuhl Seminar 20041 - Symmetric Cryptography. Dagstuhl, Germany, 19th Jan. 2020. URL: https://hal.inria.fr/hal-03146187.

[49] A. Leverrier. 'Security proofs for continuous-variable quantum key distribution'. In: QCrypt 2020 - 10th International Conference on Quantum Cryptography. Amsterdam / Virtual, Netherlands, 10th Aug. 2020. URL: https://hal.inria.fr/hal-03135753.

[50] N. Sendrier. 'Code-Based Cryptography Designs, the Ancient and the Modern'. In: Indian Workshop on Post-Quantum Cryptography. Kharagpur / Virtual, India, 17th Nov. 2020. URL: https://hal.inria.fr/hal-03146525.

Scientific book chapters

[51] M. Naya-Plasencia. 'La cryptanalyse des fonctions cryptographiques'. In: *13 défis de la cybersécurité*. 18th June 2020. URL: https://hal.inria.fr/hal-03141665.

Edition (books, proceedings, special issue of a journal)

[52] A. Canteaut and Y. Ishai, eds. *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part I*. Vol. 12105. Lecture Notes in Computer Science. 4th May 2020. DOI: 10.1007/978-3-030-45721-1. URL: https://hal.inria.fr/hal-03090162.

[53] A. Canteaut and Y. Ishai, eds. *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part II*. Vol. 12106. Lecture Notes in Computer Science. 4th May 2020. DOI: 10.1007/978-3-030-45724-2. URL: https://hal.inria.fr/hal-03090164.

[54] A. Canteaut and Y. Ishai, eds. *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part III*. Vol. 12107. Lecture Notes in Computer Science. 4th May 2020. DOI: 10.1007/978-3-030-45727-3. URL: https://hal.inria.fr/hal-03090170.

[55] A. Canteaut, G. M. Kyureghyan, A. Pott and F. Ulmer. *Coding and Cryptography 2019*. Vol. 88. 9. Sept. 2020. DOI: 10.1007/s10623-020-00791-2. URL: https://hal.inria.fr/hal-03090182.

[56] J. Ding and J.-P. Tillich, eds. *Post-Quantum Cryptography11th International Conference, PQCrypto 2020.* Post-Quantum Cryptography 11th International Conference, PQCrypto 2020. Vol. 12100. Lecture Notes in Computer Science. Paris, France, 2020, p. 560. DOI: 10.1007/978-3-030-44223-1. URL: https://hal.inria.fr/hal-03135373.

[57] I. Dinur and G. Leurent. *IACR Transactions on Symmetric Cryptology: Special Issue on Designs for the NIST Lightweight Standardisation Process.* Vol. 2020. S1. https://tosc.iacr.org/index.php/ToSC/issue/view/182, 22nd June 2020. URL: https://hal.inria.fr/hal-03141018.

[58] I. Dinur and G. Leurent. *IACR Transactions on Symmetric Cryptology: Volume 2020, Issue 2.* Vol. 2020. 2. https://tosc.iacr.org/index.php/ToSC/issue/view/185, 24th July 2020. URL: https://hal.inria.fr/hal-03141015.

[59] I. Dinur and G. Leurent. *IACR Transactions on Symmetric Cryptology: Volume 2020, Issue 3.* Vol. 2020. 3. https://tosc.iacr.org/index.php/ToSC/issue/view/187, 28th Sept. 2020. URL: https://hal.inria.fr/hal-03141016.

[60] I. Dinur and G. Leurent. *IACR Transactions on Symmetric Cryptology: Volume 2020, Issue 4.* Vol. 2020. 4. France: https://tosc.iacr.org/index.php/ToSC/issue/view/194, 10th Dec. 2020. URL: https://hal.inria.fr/hal-03141017.

[61] G. Leurent and Y. Sasaki. *IACR Transactions on Symmetric Cryptology: Volume 2019, Issue 4.* Vol. 2019. 4. https://tosc.iacr.org/index.php/ToSC/issue/view/173, 31st Jan. 2020. URL: https://hal.inria.fr/hal-03141012.

[62] G. Leurent and Y. Sasaki. *IACR Transactions on Symmetric Cryptology: Volume 2020, Issue 1.* Vol. 2020. 1. https://tosc.iacr.org/index.php/ToSC/issue/view/179, 7th May 2020. URL: https://hal.inria.fr/hal-03141014.

Doctoral dissertations and habilitation theses

[63] K. Carrier. 'Near-collisions finding problem for decoding and recognition of error correcting codes'. Sorbonne Université, 19th June 2020. URL: https://hal.archives-ouvertes.fr/tel-02955488.

[64] A. Schrottenloher. 'Quantum Algorithms for Cryptanalysis and Quantum-safe Symmetric Cryptography'. Sorbonne Université, 8th Feb. 2021. URL: https://hal.inria.fr/tel-03142366.

[65] F. Sibleyras. 'Security of Modes of Operation and other provably secure cryptographic schemes'. Sorbonne Université, 23rd Oct. 2020. URL: https://hal.archives-ouvertes.fr/tel-03058306.

Reports & preprints

[66] I. Bardet, A. Capel and C. Rouzé. *Approximate tensorization of the relative entropy for noncommuting conditional expectations.* 13th Feb. 2021. URL: https://hal.archives-ouvertes.fr/hal-03140651.

[67] 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.* 9th Feb. 2021. URL: https://hal.archives-ouvertes.fr/hal-02475356.

[68] M. Bardet, R. Mora and J.-P. Tillich. *Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach.* 6th Feb. 2021. URL: https://hal.inria.fr/hal-03133484.

[69] X. Bonnetain, A. Canteaut, V. Cortier, P. Gaudry, L. Hirschi, S. Kremer, S. Lacour, M. Lequesne, G. Leurent, L. Perrin, A. Schrottenloher, E. Thomé, S. Vaudenay and C. Vuillot. *Le traçage anonyme, dangereux oxymore: Analyse de risques à destination des non-spécialistes.* 21st Apr. 2020. URL: https://hal.inria.fr/hal-02997228.

[70] L. Brotcorne, A. Canteaut, A. C. Viana, C. Grandmont, B. Guedj, S. Huot, V. Issarny, G. Pallez, V. Perrier, V. Quema, J.-B. Pomet, X. Rival, S. Salvati and E. Thomé. *Indicateurs de suivi de l'activité scientifique de l'Inria.* Inria, 1st Dec. 2020. URL: https://hal.inria.fr/hal-03033764.

[71] A. Canteaut, T. Beyne, I. Dinur, M. Eichlseder, G. Leander, G. Leurent, M. Naya-Plasencia, L. Perrin, Y. Sasaki, Y. Todo and F. Wiemer. *Report on the Security of STARK-friendly Hash Functions (Version 2.0)*. 29th June 2020. URL: https://hal.inria.fr/hal-02883253.

[72] A. Canteaut, M. A. Fernández, L. Maranget, S. Perin, M. Ricchiuto, M. Serrano and E. Thomé. *Évaluation des Logiciels*. Inria, 14th Jan. 2021. URL: https://hal.inria.fr/hal-03110723.

[73] A. Canteaut, M. A. Fernández, L. Maranget, S. Perin, M. Ricchiuto, M. Serrano and E. Thomé. *Software Evaluation*. Inria, 14th Jan. 2021. URL: https://hal.inria.fr/hal-03110728.

[74] P. Charpin. *The crooked property*. 2020. URL: https://hal.inria.fr/hal-03091422.

[75] A. Couvreur and M. Lequesne. *On the security of subspace subcodes of Reed-Solomon codes for public key encryption*. 15th Sept. 2020. URL: https://hal.archives-ouvertes.fr/hal-02938812.

[76] A. Grospellier, L. Grouès, A. Krishna and A. Leverrier. *Combining hard and soft decoders for hypergraph product codes*. 2020. URL: https://hal.inria.fr/hal-03108332.

[77] A. Leverrier, S. Apers and C. Vuillot. *Quantum XYZ Product Codes*. Nov. 2020. URL: https://hal.inria.fr/hal-03108325.

[78] A. Olivo, U. Chabaud, A. Chailloux and F. Grosshans. *Breaking simple quantum position verification protocols with little entanglement*. 17th Aug. 2020. URL: https://hal.archives-ouvertes.fr/hal-02915994.

[79] N. Sendrier and V. Vasseur. *On the Existence of Weak Keys for QC-MDPC Decoding*. 6th Oct. 2020. URL: https://hal.inria.fr/hal-03139708.

Other scientific publications

[80] C. Bouvier. 'Analyse de la sécurité de primitives symétriques dédiées à diverses techniques de preuves'. Université de Rennes 1, 2nd Sept. 2020. URL: https://hal.inria.fr/hal-03136157.

[81] É. Burle. 'Optimisation de la méthode de rejet de la signature Wave'. Telecom ParisTech; Sorbonne Universite, 8th Sept. 2020. URL: https://hal.inria.fr/hal-03142671.

[82] S. Ghosh. 'On the QIC of quadratic APN functions'. Indiant Statistical Institute, Kolkata, 9th July 2020. URL: https://hal.inria.fr/hal-03135737.

[83] J. Loyer. 'Quantum cryptanalysis on euclidean lattices'. Limoges University, 2nd Sept. 2020. URL: https://hal.inria.fr/hal-03140995.

[84] M. Naya-Plasencia. *Qcrypt Tutorial: New results on Symmetric Quantum Cryptanalysis and Perspectives*. 14th Aug. 2020. URL: https://hal.inria.fr/hal-03141654.

[85] C. Pernot. 'New Representations of the AES Key Schedules'. Université de Bordeaux, 4th Sept. 2020. URL: https://hal.inria.fr/hal-03135597.

[86] L. Perrin. *How to Take a Function Apart with SboxU*. Loen, Norway, 15th Sept. 2020. URL: https://hal.inria.fr/hal-03136551.

[87] L. Perrin. *On Bluetooth-Based Contact-Tracing Smartphone Applications: Principles and Controversies*. Paris / Virtual, France, 2nd June 2020. URL: https://hal.inria.fr/hal-03136524.

[88] L. Perrin. *Towards New International Cryptographic Standards*. Lille, France, 28th Jan. 2020. URL: https://hal.inria.fr/hal-03136274.

12.3 Other

Educational activities

[89] L. Perrin. 'L'application "Stop-Covid" : théorie et pratique d'un dispositif de traçage numérique'. 5th Oct. 2020. URL: https://hal.inria.fr/hal-03136538.

12.4 Cited publications

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] T. Debris-Alazard. 'Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves ; contribution en cryptanalyse'. Theses. Sorbonne Université, Dec. 2019. URL: https://tel.archives-ouvertes.fr/tel-02424234.

[95] 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.

[96] 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.

[97] 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.

[98] 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/.

[99] 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.

[100] 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.