RESEARCH CENTRE

Paris

2021
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]
- Ritam Bhaumik [Inria, Starting Research Position, from Mar 2021]
- Anne Canteaut [Inria, Senior Researcher, HDR]
- André Chailloux [Inria, Researcher]
- Pascale Charpin [Inria, Emeritus, HDR]
- Nicholas Connolly [Inria, Starting Research Position, from Sep 2021]
- 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]
- Thomas Vidick [Inria, Chair, from May 2021 until Jul 2021, Inria international chair]

Faculty Member

- Magali Bardet [Université de Rouen, Associate Professor, until Aug 2021]

Post-Doctoral Fellows

- Ritam Bhaumik [Inria]
- Dragos Alexandru Cojocaru [Inria]

PhD Students

- Augustin Bariant [Inria, from Mar 2021]
- Jules Baudrin [Inria, from Sep 2021]
- Clemence Bouvier [Sorbonne Université]
- Pierre Briaud [Sorbonne Université]
- Rémi Bricout [Inria, until Apr 2021]
- Daniel Coggia [DGA, until Aug 2021]
- Nicolas David [Inria]
- Loic Demange [UDcast, CIFRE]
- Aurelie Denys [Inria]
- Simona Etinski [Université de Paris]
- Antonio Florez Gutierrez [Inria]

- Paul Frixons [Orange Labs, CIFRE]
- Shouvik Ghorai [Sorbonne Université, until Feb 2021]
- Lucien Groues [Sorbonne Université]
- Johanna Loyer [Inria]
- Charles Meyer-Hilfiger [Inria, from Nov 2021]
- Rocco Mora [Sorbonne Université]
- Andrea Olivo [Inria, until Jun 2021]
- Clara Pernot [Inria]
- Maxime Remaud [Bull, CIFRE]
- Andre Schrottenloher [Inria, until Feb 2021]

Technical Staff

- Valentin Vasseur [Inria, Engineer]

Interns and Apprentices

- Jules Baudrin [Inria, from Mar 2021 until Aug 2021]
- Julien Du Crest [École Normale Supérieure de Lyon, from Mar 2021 until Jul 2021]
- Freja Elbro [Université technique du Danemark, from Sep 2021 until Oct 2021]
- Mathias Joly [Inria, from May 2021 until Aug 2021]
- Charles Meyer-Hilfiger [Inria, from Mar 2021 until Sep 2021]
- Justine Sauvage [Inria, from Mar 2021 until Jul 2021]

Administrative Assistants

- Christelle Guiziou [Inria]
- Mathieu Mourey [Inria, until Oct 2021]
- Scheherazade Rouag [Inria, from Oct 2021]

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 [81], 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 [83] 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 [75]. It also allows to break some well-known modes of operation for MACs and authenticated encryption and provides devastating quantum slide attacks [9]. Other quantum algorithms turned out be useful in this model, such as for instance Kuperberg's algorithm [80]. It allowed to break a tweak [71] to counter the previous attack of [9] or to devise a quantum attack in the superposition model on the POLY1305 MAC primitive [74], which is largely used and claimed to be quantumly secure.

All these results show that in symmetric (and asymmetric) cryptography, the impact of quantum computers goes well beyond Grover's and Shor's algorithms and has to be studied carefully in order to understand if a given cryptographic primitive is secure or not in a quantum world. To correctly evaluate the security of cryptographic primitives in the post-quantum world, it is really desirable to elaborate a quantum cryptanalysis toolbox. This is precisely the first objective of the ERC QUASYModo regarding symmetric cryptanalysis. We plan in the coming years to continue to actively contribute to this toolbox. This goes together with improving or finding new quantum algorithms for cryptanalysis, possibly adapted to some particular situations or scenarios that have not been studied before, like the k-XOR problem. This whole thread of research, that needs to combine techniques from symmetric or asymmetric cryptanalysis together with quantum algorithmic tools, came naturally in our team. We are namely composed of symmetric and asymmetric cryptologists as well as of experts in quantum computing and we are in a privileged position to perform this kind of research.

3.2 Symmetric cryptology

Symmetric techniques are widely used because they are the only ones that can achieve some major features such as high-speed or low-cost encryption, fast authentication, and efficient hashing. It is a very active research area which is stimulated by a pressing industrial demand for low-cost implementations. Even if the block cipher standard AES remains unbroken 20 years after its design, it clearly appears that it cannot serve as a Swiss Army knife in all environments. In particular an important challenge raised by several new applications is the design of symmetric encryption schemes with some additional properties compared to the AES, either in terms of implementation performance (low-cost hardware implementation, low latency, resistance against side-channel attacks...) or in terms of functionalities. The past decade has then been characterized by a multiplicity of new proposals and evaluating their security has become a primordial task which requires the attention of the community.

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

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

3.3 Post-quantum asymmetric cryptology

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

There were 69 (valid) submissions to this call in November 2017, with numerous lattice-based, code-based and multivariate-cryptography submissions and some submissions based either on hashing or on supersingular elliptic curve isogenies. In January 2019, 26 of these submissions were selected for the second round and 7 of them are code-based submissions. In July 2020, 15 schemes were selected as third round finalists/alternate candidates, 3 of them are code-based. NIST has anounced in 2021 that this call for postquantum primitives would be extended specifically for digital signatures based on techniques other than lattices. This new call should be released in the first quarter of 2022.

The research of the project-team in this field is focused on the design and cryptanalysis of cryptosystems making use of coding theory and we have proposed code-based candidates to the NIST call for the first two types of primitives, namely public-key encryption and key-exchange protocols and have two candidates among the finalists/alternate candidates. We are also preparing proposals of code-based signatures schemes for the call which is expected in 2022.

3.4 Quantum information

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

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

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

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

While quantum cryptography is already getting out of the labs, this is not yet the case of quantum computing, with large quantum computers capable of breaking RSA with Shor's algorithms maybe still decades away. The situation is evolving very quickly, however, notably thanks to massive public investments in the past couple of years and all the major software or hardware companies starting to

develop their own quantum computers. One of the main obstacles towards building a quantum computer is the fragility of quantum information: any unwanted interaction with the environment gives rise to the phenomenon of decoherence which prevents any quantum speedup from occurring. In practice, all the hardware of the quantum computer is intrinsically faulty: the qubits themselves, the logical gates and the measurement devices. To address this issue, one must resort to quantum fault-tolerance techniques which in turn rely on the existence of good families of quantum error-correcting codes that can be decoded efficiently. Our expertise in this area lies in the study of a particularly important class of quantum codes called quantum low-density parity-check (LDPC) codes. The LDPC property, which is well-known in the classical context where it allows for very efficient decoding algorithms, is even more crucial in the quantum case since enforcing interactions between a large number of qubits is very challenging. Quantum LDPC codes solve this issue by requiring each qubit to only interact with a constant number of other qubits.

4 Application domains

4.1 Designing, Analyzing and Choosing Cryptographic Standards

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

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

NIST post-quantum competition.

The NIST post-quantum competition[1] aims at standardizing quantum-safe public-key primitives. It is really about offering a credible quantum-safe alternative for the schemes based on number theory which are severely threatened by the advent of quantum computers. It is expected to have a huge and long-term impact on all public-key cryptography. It has received 69 proposals in November 2017, among which five have been co-designed by the project-team. Four of them have made it to the second round in January 2019. One of them was chosen in July 2020 for the third round and another one was chosen as an alternate third round finalist. We have also broken two first round candidates EDON-K [82] and RANKSIGN [79], and have devised a partial break of the RLCE encryption scheme [77]. In 2020, we obtained a significant breakthrough in solving more efficiently the MinRank problem and the decoding problem in the rank metric [72, 73] 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

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

[2] Website of the NIST project.

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.

Monitoring Current Standards

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

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

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

4.2 Large scale deployment of quantum cryptography

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

5 Social and environmental responsibility

5.1 Oversight of COVID Digital Tools

During the course of the COVID-19 pandemic, several digital tools were developped to help mitigating the pandemic. We have not been involved in the developpement of these tools, but we took an active role in analyzing them, and contributing to the political debate.

Digital Contact Tracing: 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.

Later, venue tracking was implemented in several countries. The core idea is to warn patrons when a public place is detected to be a cluster: patrons scan a QR-code with a random identifier when entering the venue, and a list of identifiers with known clusters is published daily.

In France Bluetooth tracing was implemented in the StopCovid application launched on June 2 2020, and renamed TousAntiCovid on October 22 2020. Venue tracking was added on June 9 2021.

Covid Certificates: At the end of 2020, discussions began in the European Union about vaccine passports and covid certificates, and the first guidelines from European institutions were published in January 2021. A Covid Certificate is a machine-readable document (usually in the form of a QR-code) containing health information with a cryptographic signature from a health autority.

Covid certificates started to be used in France on June 9 2021, and the European version was put in place on July 1st 2021.

Members of the COSMIQ team began to be involved in this topic in April 2020. As several contact tracing 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.

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*" [76]. The analysis presented in [76] 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 [76] 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, 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.

[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/).

- Gaëtan Leurent wrote an analysis of the TAC-W protocol, which was meant to be used for venue tracking[7] in France. TAC-W had serious issues, and was replaced by CLÉA.
- Gaëtan Leurent contributed to an analysis of the statistics collection in TousAntiCovid[8]. This functionality was leaking a lot of private data and has been partially fixed.
- Gaëtan Leurent made several Freedom of Information requests for documents related to those digitals tools and their evaluation:
  - https://madada.fr/demande/analytics_tousanticovid
  - https://madada.fr/demande/aipd_des_outils_numeriques_de_lu
  - https://madada.fr/demande/rapport_sur_le_fonctionnement_de
  - https://madada.fr/demande/statistiques_sur_lutilisation_de

5.2 Footprint of research activities

During this second year of the COVID-19 pandemic, most conferences and workshops have been either cancelled or modified to be online events. Anne Canteaut played a significant role in enabling this transition as the program chair of Eurocrypt 2020 and Eurocrypt 2021. Eurocrypt 2021 was the first flagship conference in cryptography held in a hybrid format. The concomitance of remote talks and of in-person talks required to adapt the format of the conference, the lengths of the talks... This very first experience will motivate discussions on the future format of conferences in our area.

5.3 Impact of research results on standardisation

Our cryptanalysis results on SHA-1 [10] and GEA [28] have helped convince users and industry to deprecate those obsolete standards. Publication of those attacks and discussion with industry has resulted in concrete actions to reduce usage of those ciphers.

Our project is also involved in two NIST competitions: the competition for lightweight cryptography and the competition for standardizing quantum safe cryptosystems. In the first competition, our team has still one candidate in the third 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

PhD thesis of André Schrottenloher: We consider this PhD [53] as a landmark in the domain of quantum cryptanalysis. It contains major results:

- the first proof of an actual quantum time speedup for collision search in case of polynomially bounded quantum memory, solving here a long standing open question;
- optimal quantum algorithms for solving fundamental problems such as k-XOR or k-SUM;
- a general methodology for converting classical research problems into nested quantum research problems, with many applications in cryptanalysis;
- an off-line Simon algorithm which enables to use for the first time Simon's algorithm in the standard attack model;
- a distinguisher on the Gimli lightweight permutation.

[7] https://gitlab.inria.fr/stopcovid19/stopcovid-android/-/issues/65
[8] https://gitlab.inria.fr/stopcovid19/stopcovid-android/-/issues/79

NIST competition on lightweight cryptography: On 2019, the American NIST published the candidates that were submitted by teams from the whole world for a new standardization effort. Its aim is to choose one or several symmetric cryptographic primitives that are intended to run on low power devices (RFID tags, sensor networks, and whatever else will be connected in the Internet of Things). COSMIQ has been heavily involved in this process, co-authoring 3 of the 56 initial submissions (SATURNIN, SPOOK and SPARKLE), and publishing security analysis of many of these candidates. In March 2021, NIST announced the 10 finalists of this competition, among which SPARKLE is listed. This algorithm is the outcome of a collaboration between Léo Perrin, and researchers from the universities of Luxembourg and Edinburgh, as well the company CryptoExperts. Furthermore, our cryptanalysis results had an impact on the list of finalists since, for example, GIMLI and mixFeed did not make it to this list. Our attacks against Gimli had obtained a best paper award at Asiacrypt in 2020 [8], while our results on mixFeed are included in more general results on the AES that received a best paper award at Eurocrypt 2021 [40].

Research highlights in the Communications of the ACM: The *threshold theorem* is a seminal result in the field of quantum computing asserting that arbitrarily long quantum computations can be performed on a faulty quantum computer provided that the noise level is below some constant threshold. This remarkable result comes at the price of increasing the number of qubits (quantum bits) by a large factor that scales polylogarithmically with the size of the quantum computation we wish to realize. In a paper published at FOCS 2018 [23], and highlighted in the Communications of the ACM, Omar Fawzi, Antoine Grospellier and Anthony Leverier improved on this result and showed that the polylogarithmic factor in the standard threshold theorem is in fact not needed and that there is a fault-tolerant construction that uses a number of qubits that is only a constant factor more than the number of qubits of the ideal computation. This result was conjectured by Gottesman who suggested to replace the concatenated codes from the standard threshold theorem by quantum error-correcting codes with a constant encoding rate.

6.1 Awards

Laureate of the Woman Cyber Researcher award 2021:
Anne Canteaut https://cyberwomenday-cefcys.com/en/

Prix de thèse Gilles Kahn 2020:
Thomas Debris-Alazard, *Cryptographie fondée sur les codes: nouvelles approches pour constructions et preuves; contribution en cryptanalyse,* [78]
Sorbonne Universités, UPMC University of Paris 6, 2019, https://www.societe-informatique-de-france.fr/2021/01/recherche-prix-de-these-gilles-kahn-laureats-2020/

Eurocrypt best paper award: [40] Clara Pernot, Gaëtan Leurent, New Representations of the AES Key Schedule, EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, Jun 16, 2021.

7 New software and platforms

7.1 New software

7.1.1 Wave

Name: Wave

Keywords: Cryptography, Error Correction Code

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

URL: `http://wave.inria.fr/en/implementation/`

Authors: Nicolas Sendrier, Thomas Debris

Contact: Nicolas Sendrier

7.1.2 Collision Decoding

Keywords: Algorithm, Binary linear code

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

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

Contact: Nicolas Sendrier

Participants: Grégory Landais, Nicolas Sendrier

8 New results

8.1 Quantum algorithms and cryptanalysis

Participants: Ritam Bhaumik, Rémi Bricout, André Chailloux, Nicolas David, Simona Etinski, Antonio Flórez-Gutiérrez, Paul Frixons, Gaëtan Leurent, 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:

André Schrottenloher PhD thesis This thesis [53] contains major results:

- the first proof of an actual quantum time speedup for collision search in case of polynomially bounded quantum memory, solving here a long standing open question;
- optimal quantum algorithms for solving fundamental problems such as k-XOR or k-SUM;
- a general methodology for converting classical research problems into nested quantum research problems, with many applications in cryptanalysis;
- an off-line Simon algorithm which enables to use for the first time Simon's algorithm in the standard attack model;
- a distinguisher on the Gimli lightweight permutation.

Quantum Linearization Attacks. In 2016, we have shown that many modes widely used in symmetric cryptography are completely broken by quantum superposition queries, using Simon's period-finding algorithm [9]. In a new work published at Asiacrypt this year [30], we generalized those attacks to *quantum linearization attacks*, and broke several modes that were not yet known to be broken in this model (LightMAC, PMAC, OCB, ZMAC ...). We also describe variants of attacks using other quantum algorithms that had not been used previously in symmetric cryptanalysis: Deutsch's, Bernstein-Vazirani's, and Shor's algorithms.

QCB. Since many widely used modes are not secure against quantum superposition queries, we have proposed a new authenticated encryption mode with security against quantum adversaries: QCB [29]. QCB is inspired by TAE and OCB, and is the first mode offering quantum security with high efficiency: it is parallelizable and has rate one.

Quantum Boomerang Attacks and Some Applications. We give in [38] for the first time a quantum speedup for Boomerang attacks. In certain cases, we even obtain quadratic speedups, which results in a similar speedup as for differential attacks. This enlarges the toolbox for attacking quantumly symmetric primitives and results in a better general understanding of the resistance of symmetric ciphers against quantum computers.

Lattice sieving via quantum walks. Lattice-based cryptography is one of the most promising solutions for post-quantum cryptography. For many of the proposed cryptosystems, the best algorithm to attack them is the BKZ algorithm which uses as its core several calls to an algorithm that solves the Shortest Vector Problem. This year, in the Asiacrypt paper [35] André Chailloux and Johanna Loyer improved the best quantum algorithms for SVP using quantum walks. As a direct consequence, this work reduces the quantum security of all lattice-based schemes proposed at the post-quantum NIST competition which must increase their parameters if they want to maintain the level of security they announced.

Quantum Security of the Legendre PRF. In [39], we study the security of the Legendre PRF against quantum attackers, given classical queries only, and without quantum random-access memories. We give two algorithms that recover the key of a shifted Legendre symbol with unknown shift, with a complexity smaller than the exhaustive search of the key. The first one is a quantum variant of the table-based collision algorithm. The second one is an offline variant of Kuperberg's abelian hidden shift algorithm.

8.2 Symmetric cryptology

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

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

8.2.1 Cryptanalysis

AES [40]. We have analyzed the key schedule of the AES cipher, and discovered that it can be split into four independent parallel computations. We show two consequences of this surprising property. First, iterations of the key schedule have short cycles, resulting in breaks of AEAD schemes mixFeed and ALE. Second, some cryptanalytic attacks against AES can be improved slightly, using our observation to efficiently combine information from different subkeys. This paper received a best paper award at Eurocrypt 2021.

Gimli [24]. We leveraged the slow diffusion provided by the round function of the permutation used by Gimli to identify full round distinguishers. This paper was invited to the Journal of Cryptology after receiving a best paper award at Asiacrypt 2020 [8]. The journal version includes new results, in particular a linear distinguisher for the full permutation.

Simon and Simeck [41]. Simon is a lightweight bock cipher designed by the NSA, and Simeck is an academic variant. We have shown that there is a strong clustering effect in these ciphers: a large number of trails contribute to the same differential or linear hull. Using this property we improve significantly the previous analysis based on linear and differential cryptanalysis.

GEA [28]. The GEA-1 and GEA-2 algorithms are used to encrypt data traffic in the 2G telephony standards (GPRS), designed in the late 1990's. We have shown that GEA-1 was deliberately weakened so that it could be broken in practice with very little known plaintext. GEA-2 does not show signs of

deliberate weaknesses, but it can also be broken with more computational resources and a larger amount of known plaintext.

FlexAEAD [22]. FlexAEAD was a first-round candidate in the NIST lightweight cryptography effort, but previous work has shown a forgery attack with complexity 2^{46}. Building upon these results, we obtain a key-recovery attack with practical complexity (around 2^{31} encryptions), that has been verified with the reference implementation.

SHA-1 [36]. Following our work on SHA-1 chosen-prefix collisions [10], we have studied the possibility of a hardware implementation of this attack. We find that the GPU implementation is better suited when running the attack only a few times, but a dedicate hardware cluster requires fewer energy per collision. We estimate that an ASIC cluster costing a few million dollars could generate SHA-1 chosen-prefix collisions in a few days.

Daniel Coggia's PhD thesis This thesis [51] presents several new cryptanalysis results based on different types of attacks: subspace-trail cryptanalysis, MILP models for studying differentials, and algebraic methods related to cube attacks.

Improving Differential-Linear Attacks Differential-linear attacks are a cryptanalysis family that has recently benefited from various technical improvements, mainly in the context of ARX constructions. In [61], we push further this refinement, proposing several new improvements. In particular, we develop a better understanding of the related correlations, improve upon the statistics by using the LLR, and finally use ideas from conditional differentials for finding many right pairs. We illustrate the usefulness of these ideas by presenting the first 7.5-round attack on Chaskey. Finally, we present a new competitive attack on 12 rounds of Serpent, and as such the first cryptanalytic progress on Serpent in 10 years.

Generic Framework for Key-Guessing Improvements In [32], we propose a general technique to improve the key-guessing step of several attacks on block ciphers (linear, differential, rectangle...). This is achieved by defining and studying some new properties of the associated S-boxes and by representing them as a special type of decision trees that are crucial for finding fine-grained guessing strategies for various attack vectors. We also show how to use them in different cryptanalytic scenarii and how this method can be used to speed up significantly the best known attacks.

8.2.2 Design

Tweakable Luby–Rackoff [17]. We have improved the indifferentiability proofs of the 3-round tweakable Luby–Rackoff, from $n/2$ bits to $n - 2\log n$ (with n the size of the branch).

Trojan Resilient Encryption Encryption algorithm may be implemented in hardware, i.e. using dedicated chips that then handle both the sensitive data and the encryption keys used to process them. In the most sensitive applications, this can be an issue. Indeed, manufacturing chips can only be done cheaply by a few countries, and a few companies. What can we do to make sure that an encryption key remains secure even if the hardware using it cannot be trusted? We give a practical solution to this problem in [18] where we present MOE, a block cipher with a special round function that is particularly suitable for secret sharing. Several untrusted chips implement the various operations it requires, and an extremely simple (and thus cheap, even if made inhouse) master chip combines their results to obtain the actual encryption. It ensures that the data sent to each chip is statistically independent from the secrets involved.

DLCT of Sboxes The differential-linear connectivity table (DLCT) is a tool introduced by BarOn *et al.* at Eurocrypt'19, for taking into account the dependency between the two subciphers involved in differential-linear attacks. In [33], we have proved that the DLCT actually corresponds (up to a constant factor) to the autocorrelation table. The DLCT of some important families of Sboxes are then studied in light of the notion of autocorrelation.

Extended-affine equivalence of Sboxes Extended-Affine (EA) equivalence is the equivalence relation between two vectorial Boolean functions F and G such that there exist two affine permutations

A, B and an affine function C satisfying $G = A \circ F \circ B + C$. In [62], we have proposed, in the case of quadratic functions, a new efficient algorithm for recovering (A, B, C) if it exists, and a method for simply deciding whether F and G are EA-equivalent. This last method enabled us to sort tens of thousands of quadratic APN functions of 8 variables into distinct EA-classes

Crooked functions [65] is an extensive study of crooked functions, which are vectorial Boolean functions with remarkable properties since they form a subclass of almost bent functions.

8.3 Post-quantum asymmetric cryptology

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

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

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

Our main contributions during the period are given below

Algebraic attacks A series of works are related to algebraic attacks and Gröbner basis. An effective attack on the SIDON cryptosystem [31], an improvement on the best known attacks against the RSL (Rank Support Learning) problem [26], and also other cryptanalytic works in progress which relate to the NIST competition, either rank metric-based or multivariate cryptography [55, 58]. This research also has applications in algebraic coding theory [27].

NIST competition Two of our NIST candidates are still in the third round of the competition. First ClassicMcEliece, which is a KEM (Key Encapsulation Mechanism) finalist and is a stabilized system which does not require further research work. Also BIKE, which is a KEM alternative candidate. The state-of-the-art about the decoding failure rate (DFR) of BIKE [68] is part of Valentin Vasseur's PhD [54], and is one of the key points to estimate the the security of the scheme. Another work in progress about BIKE [67] considers the protection against some side-channel attacks (timing, cache).

Follow-up of the NIST competition on signatures We are also working to prepare the extension of the NIST call to digital signatures. Code-based signatures were not ready in 2017 when the first call was made, and all code-based signatures were discarded. There has been considerable progress since then. The project-team has been preparing to submit new proposals using WAVE [6], or other techniques[60].

Fundamental issues in code-based cryptography We have also been working on fundamental and prospective topics. For instance, we have devised a general framework [34] for the computation of the complexity of classical and quantum information set decoding techniques, and have applied for the Lee metric in particular, or through various fundamental works exploring the weaknesses involved by the use of codes with algebraic structure in cryptography [19, 52]. Some of this work was motivated by effective attacks on existing cryptosystems, but the scope of the results often went beyond that. Another fundamental problem, especially if one wants to build signature schemes is to understand the difficulty of the low weight codeword search problem. One possible path for achieving this is to relate it to the decoding problem. In lattice-based cryptography, this is analoguous to relate the LWE problem to the SIS problem. A fundamental tool is here Regev's quantum reduction from SIS to LWE. We have obtained a similar reduction in the context of coding theory in [66] for various code-based metrics.

8.4 Quantum information

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

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

Security of continuous-variable protocols A major question in the field of quantum key distribution is to prove the security of practical continuous-variable protocols. The main advantage of these protocols is that they can be implemented with standard equipment from optical telecommunications, and do not require specific hardware such as single-photon detectors. Up until now, all security proofs were restricted to protocols exploiting *Gaussian modulation* of coherent states. In contrast, practical protocols rely on discrete modulation where the coherent states are chosen from a finite constellation. In [20], Aurélie Denys, Peter Brown and Anthony Leverrier establish for the first time the security of such protocols in the asymptotic regime, and give explicit closed-form expressions for the secret key rate of these protocols for arbitrary constellations. This work was presented at QCrypt 2021 [44] and ICQOM 2021 [43].

Feasibility of quantum key distribution with satellites Another 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.

Decoding algorithms for quantum error correcting codes 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 [23]. We have tested numerically the corresponding codes and decoder in [25] 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 [37].

Locally testable quantum LDPC codes 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 [42].

Quantum information theory We also study very fundamental questions in quantum information theory and have derived new quantum information theoretic inequalities such as the approximate tensorization of the relative entropy [15]. We also provide there estimates on the constants in terms of conditions of clustering of correlations in the setting of quantum lattice spin systems. A related functional approach is also used to get estimations of the decoherence times, of private and quantum capacities, of entanglement-assisted classical capacities, as well as estimation of entanglement breaking times [16] or a better understanding of the heat-bath dynamics of 1D systems [14].

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

LOTUS:(01/2021 -> 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 International initiatives

10.1.1 Participation in other 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

10.2.1 Visits of international scientists

Inria International Chair

Thomas Vidick

Status: Professor

Institution of origin: Caltech

Country: USA

Dates: 2020–2024

Context of the visit: 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 last fall. See http://users.cms.caltech.-edu/ vidick/teaching/fsmp/index.html.

Mobility program/type of mobility: Research stay and lectures.

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.

10.3 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 Other european programs/initiatives

- **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.

- **MCCL** – Modular Code Cryptanalysis Library

  Collaboration between CWI and Inria whose purpose is to improve the state of the art of the implementation of ISD (Information Set Decoding). In particular by solving new decoding challenges.

This intiative is a follow-up of the July 2021 Inria-CWI workshop. The first meeting took place in Paris in November 2021 and gathered 12 people from both institutions.

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.

- **ANR SWAP** (02/22→01/26)
  Sboxes for Symmetric-Key Primitives
  ANR Program: AAP Générique 2021
  Partners: UVSQ (coordinateur), Inria COSMIQ, ANSSI, CryptoExperts, Univ. of Rouen, Univ. of Toulon.

  172 kEuros
  Sboxes are small nonlinear functions that are crucial components of most symmetric-key designs and their properties are highly related to the security of the overall construction. The development of new attacks has given rise to many Sbox design criteria. However, the emerge of new contexts,

applications and environments requires the development of new design criteria and strategies. The SWAP project aims first at investigating such criteria for emerging use cases like whitebox cryptography, fully homomorphic encryption and side-channel resistance. Then, we wish for analyzing the impact of these particular designs on cryptanalysis and see how the use of Sboxes with some special mathematical structures can accelerate some known attacks or introduce new ones. Finally, we aim at studying Sboxes from a mathematical point of view and provide new directions to the Big APN problem, an old conjecture on the existence of a particular type of optimal permutations.

10.5 Regional initiatives

DIM SIRTEQ The SIRTEQ project labeled Major Interest Domain (DIM) is funded by the Ile-de-France Region. SIRTEQ brings together the largest European concentration of academic teams in the field of quantum technologies. Its main objective is to promote an excellent academic research in the field of quantum technologies in Ile de France, taking into account the actual current societal challenges and the importance of the transfer of knowledge and technologies.

We are involved in this project in the quantum communications (quantum cryptography) and quantum computation (quantum error codes, quantum cryptanalysis) themes.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Dagstuhl seminar 21421 "Quantum Cryptanalysis": October 17-22, 2021, Dagstuhl (Germany): M. Naya-Plasencia co-chair.
- WCC 2022: March 7-13, 2022, Rostock (Allemagne): co-chair, L. Perrin.
- Dagstuhl seminar 22141 "Symmetric Cryptography": April 3-8, 2022, Dagstuhl (Germany): M. Naya-Plasencia co-chair.

Member of the organizing committees

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

11.1.2 Scientific events: selection

Chair of conference program committees

- PQCrypto 2021: July 20-22, 2021, Daejeon, South Korea, co-chair: J.-P. Tillich.
- Eurocrypt 2021: October 17-21, 2021, Zagreb, Croatia, co-chair: A. Canteaut.
- WCC 2022: March 7-13, 2022, Rostock (Allemagne): co-chair, L. Perrin.

Member of the conference program committees

- TQC 2021: July 5-8, ,2021, Riga, Latvia (Online), (A. Leverrier).
- ISIT 2021: July 12-20, 2021, Melbourne, Australia (Online), (J.-P. Tillich).
- PQCrypto 2021: July 20-22, 2021, Daejeon, South Korea (M. Bardet, A. Chailloux, N. Sendrier, J.P. Tillich).
- TQC 2021: July 5-8, ,2021, Riga, Latvia (Online), (A. Leverrier).

- CFail 2021: August 14, 2021, Santa-Barbara, USA (Online), (M. Naya-Plasencia).
- BFA 2021: September 6-10, 2021, Rosendal, Norway (L. Perrin).
- Eurocrypt 2021: October 17-21, 2021, Zagreb, Croatia, (M. Naya-Plasencia).
- Indocrypt 2021: December 12-15, 2021, Jaipur, India (G. Leurent).
- IMACC 2021: December 14-15, 2021, Online Event (L. Perrin).
- WCC 2022: March 7-11, 2022, Rostock, Germany, (A. Canteaut, N. Sendrier, J.P. Tillich).
- Eurocrypt 2022: May 30-June 3, 2022, Trondheim, Norway, (G. Leurent).

11.1.3 Journal

Member of the editorial boards

- *Advances in Mathematics of Communications*, associate editors: N. Sendrier and J.P. Tillich.
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut
- *Designs, Codes and Cryptography*, associate editors: P. Charpin M. Naya-Plasencia.
- *Finite Fields and their Applications*, associate editors: A. Canteaut, P. Charpin.
- *IACR Transactions in Symmetric Cryptology*, editorial board member editor: L. Perrin.
- *IEEE Transactions on Information Theory*, associate editor until Oct. 2021 and area editor since July 2021 (for cryptography and sequences): A. Canteaut.
- *Journal of Cryptology*, associate editor: A. Canteaut.
- *Quantum*, editor: A. Leverrier.

11.1.4 Invited talks

- A. Canteaut, *Recovering or Testing Extended-Affine Equivalence*, Carleton Finite Fields eSeminar, Ottawa, Canada (on-line), April 14, 2021.
- M. Naya-Plasencia *Quantum Safe Symmetric Cryptography* - Keynote speaker, Indocrypt 2021, Jaipur, India, December 12-15, 2021.

11.1.5 Leadership within the scientific community

- A. Canteaut serves as a chair of the steering committee of Fast Software Encryption (FSE), M. Naya-Plasencia and G. Leurent also serve on the committee.
- A. Canteaut serves on the International Scientific Advisory Board of the Flemish Strategic Research Program on Cybersecurity.

11.1.6 Scientific expertise

- Reviewer ERC starting Grant 2021 (A. Leverrier, M. Naya-Plasencia).
- Reviewer for EIC (European Innovation Council) Pathfinder (A. Leverrier).

11.1.7 Research administration

- A. Canteaut serves as Head of Inria Evaluation Committee since September 2019.
- A. Chailloux serves in the Inria CES (Commission des emplois Scientiiques).
- A. Leverrier serves on the steering committee of the Domaine d'Intérêt Majeur SIRTEQ since 2018.
- A. Leverrier is the coordinator of the Inria challenge EQIP on Quantum Technologies.

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

- 2021 Head of the jury d'admissibilité Inria DR2, (A. Canteaut)
- 2021 Jury d'admissibilité Inria DR2, (M. Naya-Plasencia)
- 2021 Jury d'admissibilité Inria de Paris CRCN/ISFP, (J.-P. Tillich)
- 2021 Jury d'admission Inria CRCN, (A. Canteaut)
- 2021 Jury d'admission Inria DR2, (A. Canteaut)
- 2021 Tenure Track hiring jury at DTU, Denmark, (A. Canteaut)

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Master: A. Canteaut, Error-correcting codes and applications to cryptology, 12 hours, M2, University Paris-Diderot (MPRI), France;
- Master: A. Chailloux, Quantum Circuits and Logic Gates, 12 hours, M1, Sorbonne Université
- Master: A. Chailloux, Quantum information, 12 hours, M2, University Paris-Diderot (MPRI), France;
- Master: A. Chailloux, Quantum algorithms, 4 hours, M2, Ecole Normale Supérieure de Lyon, France;
- Master: A. Leverrier, Quantum information 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 : André Schrottenloher, Long-term security of symmetric primitives, Sorbonne Université, February 8, 2021 supervisors: A. Chailloux and M. Naya-Plasencia.
- PhD : Shouvik Ghorai, Continuous-variable quantum cryptographic protocols, February 12, 2021, supervisors: E. Diamanti (UPMC), A. Leverrier.
- PhD : Rémi Bricout, Quantum algorithms for the knapsack problem and decoding, March 30,2021, supervisors: A. Chailloux and A. Leverrier.
- PhD : Valentin Vasseur, Post-quantum cryptography: study on the decoding of QC-MDPC codes, March 29, 2021, supervisor: N. Sendrier.

- PhD : Matthieu Lequesne, Analysis of code-based post-quantum cryptosystems, Sorbonne Univ, May 25, 2021 supervisor: N. Sendrier.
- PhD : Daniel Coggia, Techniques of cryptanalysis for symmetric-key primitives, Sorbonne Université, October 8, 2021, supervisors: A. Canteaut and C. Boura.
- 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: 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: J.-P. 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: J.-P. Tillich.
- PhD in progress: Clémence Bouvier, Analyse de la sécurité de primitives symétriques dédiées à divers usages émergents, since September 2020, supervisors: A. Canteaut, L. Perrin.
- PhD in progress: Nicolas David, Secure primitives and the post-quantum world, since September 2020, supervisor: M. Naya Plasencia.
- PhD in progress: Clara Pernot, Cryptanalyse des algorithmes de cryptographie symétrique, since September 2020, supervisors: L. Perrin, M. Naya Plasencia.
- PhD in progress: Pierre Briaud, Cryptosystems based on the MinRank problem, since October 2020, supervisor: J.-P. Tillich.
- PhD in progress: Aurélie Denys, Security proofs for continuous variable quantum cryptography protocols, since October 2020, supervisor: A. Leverrier.
- PhD in progress: Johanna Loyer, Quantum algorithms on lattices, since October 2020, supervisor: A. Chailloux.
- PhD in progress: Loïc Demange, Implementation of BIKE, since November 2020, supervisor: N. Sendrier.
- PhD in progress: Augustin Bariant, Sécurité des algorithmes cryptographiques à bas coût, since March 2021, supervisors: A. Canteaut, G. Leurent.
- PhD in progress: Jules Baudrin, Analyse de la sécurité de primitives symétriques légères, since September 2021, supervisors: A. Canteaut, L. Perrin.
- PhD in progress: Charles Meyer-Hilfiger, Cryptographie post-quantique : Conception, analyse et mise œuvre d'algorithmes de décodage générique, since November 2021, supervisor: N. Sendrier.

11.2.3 Juries

- I. Villa, *Analysis, classification and construction of optimal cryptographic Boolean functions*, University of Bergen (Norway), January 4, 2021, committee: A. Canteaut (reviewer).
- A. Schrottenloher, *Long-term security of symmetric primitives*, Sorbonne Univ., February 8, 2021, committee: A. Chailloux (supervisor), M. Naya-Plasencia (supervisor).
- S. Ghorai, *Continuous-variable quantum cryptographic protocols*, Sorbonne Univ, February 12, 2021, committee: A. Leverrier (supervisor).
- C. Kaspers, *Equivalence problems of Almost Perfect Nonlinear Functions and Disjoint Difference Families*, Otto-von-Guericke Universität Magdeburg (Germany), March 22, 2021, committee: A. Canteaut (reviewer).
- V. Vasseur, *Post-quantum cryptography: study on the decoding of QC-MDPC codes*, Univ. of Paris, March 29, 2021, committee: N. Sendrier (supervisor), J.-P. Tillich.
- R. Bricout, Quantum algorithms for the knapsack problem and decoding, Sorbonne Univ., March 30, 2021, committee: M. Bardet, A. Chailloux (supervisor), A. Leverrier (supervisor), J.-P. Tillich.
- Y. Shen, *Classical and quantum cryptanalysis for Euclidean lattices and subset sums*, Univ. of Paris, May 11, 2021, committee: M. Naya-Plasencia, J.-P. Tillich (chair).
- M. Lequesne, *Analysis of code-based post-quantum cryptosystems*, Sorbonne Univ, May 25, 2021, committee: M. Bardet, N. Sendrier (supervisor).
- A. Langlois, *On the hardness of the Learning With Errors problem and its variants*, HDR, Univ. Rennes, Rennes, June 22, 2021, committee: M. Naya-Plasencia.
- V. Savin, *Contributions to the construction and decoding of LDPC and polar codes*, HDR, Univ. Grenoble Alpes, June 24, 2021, committee: J.-P. Tillich (reviewer).
- Y. Hamoudi, *Quantum Algorithms for the Monte Carlo Method*, Univ. de Paris, July 7, 2021, committee: M. Naya-Plasencia.
- N. Kaleyski, *Towards a deeper understanding of APN functions and related longstanding problems*, University of Bergen (Norway), August 24, 2021, committee: A. Canteaut (reviewer).
- J. Lin, *Security Analysis of Quantum Key Distribution: Methods and Applications*, Univ. Waterloo (Canada), September 8, 2021, committee: A. Leverrier (external examiner).
- S. Pal, *Cryptanalysis of Stream Ciphers*, Homi Bhabha National Institute, Inde, September, 2021, committee: M. Naya-Plasencia. (reviewer).
- D. Coggia, *Techniques de cryptanalyse dédiées au chiffrement à bas coût*, Sorbonne Univ., October 8, 2021, committee: A. Canteaut (supervisor).
- A. Goswami, *Quantum polar codes*, Univ. Grenoble Alpes, October 25, 2021, committee: J.-P. Tillich (chair).
- H. Nguyen, *Cryptographic aspects of orthogonal lattices*, November 15, 2021, committee: J.-P. Tillich (reviewer).
- Z. Van Herstraeten, *Majorization theoretical approach to quantum uncertainty*, Univ. Libre Bruxelles (Belgium), November 18, 2021, committee: A. Leverrier (examiner).
- F. Centrone, *Practical protocols for quantum communication networks*, Sorbonne Univ., November 25, 2021, committee: A. Leverrier (reviewer).
- I. Panaccione, *On decoding algorithms for algebraic geometry codes beyond half the minimum distance*, Inst. Polyt. Paris, December 3, 2021, committee: J.-P. Tillich (chair).

- N. Bordes, *Sécurité des primitives symétriques et de leurs implémentations*, Université Grenoble Alpes, December 9, 2021, committee: A. Canteaut (reviewer).
- B. Viguier, *A Panorama on Classical Cryptography*, Radboud University, The Netherlands, December 13, 2021, committee: M. Naya-Plasencia (reviewer).
- G. Rezgui, *Error-control codes and coded modulations for the optical fiber communication*, Cergy Paris Uni., December 14, committee: J.-P. Tillich (reviewer).
- M. Chenu de la Morinerie, *Supersingular Group Actions and Post-quantum Key Exchange*, Institut Polytechnique de Paris, December 17, 2021, committee: A. Canteaut (chair), N. Sendrier.
- J. Yang, *Contributions to Confidentiality and Integrity Algorithms for 5G*, Lund University, Sweden, December 17, 2021, committee: M. Naya-Plasencia.
- K. W. Stoffelen, *Optimizations in Symmetric cryptography*, Radboud Univ. The Netherlands, December 27, 2021, committee: A. Canteaut (reviewer).
- V. Mollimard, *Algorithmes pour la Cryptanalyse Differentielle*, Rennes Univ., January 11, 2022, committee: M. Naya-Plasencia (reviewer).

11.3 Popularization

11.3.1 Articles and contents

- A. Chailloux *Quand la sécurité informatique repose sur la limite de la vitesse de la lumière* Science et Vie, online, https://www.science-et-vie.com/technos-et-futur/quand-la-securite-informatique-repose-sur-la-limite-de-la-vitesse-de-la-lumiere-65201
- M. Naya-Plasencia *La cryptanalyse, la base de la confiance 1* - Blog binaire - Le Monde, April 9, 2021.
- M. Naya-Plasencia *La cryptanalyse, la base de la confiance 2* - Blog binaire - Le Monde, April 13, 2021.
- G. Leurent *Que sait-on aujourd'hui de l'efficacité de TousAntiCovid ?* - Atlantico, December 15, 2021

11.3.2 Education

Organization of the event "Rendez-vous des Jeunes Mathématiciennes et Informaticiennes" at Inria Paris (November 2-3) by C. Bouvier and A. Denys, a 2-day camp for 24 high-school girls interested in mathematics and computer science. J. Baudrin and C. Pernot conducted sessions there.

11.3.3 Interventions

C. Pernot gave a talk in the event "Rendez-vous des Jeunes Mathématiciennes et Informaticiennes" at ENS on November 28.

12 Scientific production

12.1 Major publications

[1] C. Beierle, A. Canteaut, G. Leander and Y. Rotella. 'Proving Resistance Against Invariant Attacks: How to Choose the Round Constants.' In: *Crypto 2017 - Advances in Cryptology*. Ed. by J. Katz and H. Shacham. Vol. 10402. LNCS - Lecture Notes in Computer Science. Steven Myers. Santa Barbara, United States: Springer, Aug. 2017, pp. 647–678. DOI: 10.1007/978-3-319-63715-0_22. URL: https://hal.inria.fr/hal-01631130.

[2] A. Canteaut and L. Perrin. 'On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting'. In: *Finite Fields and Their Applications* 56 (Mar. 2019), pp. 209–246. DOI: 10.1016/j.ffa.2018.11.008. URL: https://hal.inria.fr/hal-01953353.

[3] A. Chailloux, M. Naya-Plasencia and A. Schrottenloher. 'An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography'. In: *Asiacrypt 2017 - Advances in Cryptology*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. LNCS - Lecture Notes in Computer Science. Hong Kong, China: Springer, Dec. 2017, pp. 211–240. DOI: 10.1007/978-3-319-70697-9_8. URL: https://hal.inria.fr/hal-01651007.

[4] K. Chakraborty, A. Chailloux and A. Leverrier. 'Arbitrarily Long Relativistic Bit Commitment'. In: *Physical Review Letters* 115 (Dec. 2015). DOI: 10.1103/PhysRevLett.115.250501. URL: https://hal.inria.fr/hal-01237241.

[5] P. Charpin, G. M. Kyureghyan and V. Suder. 'Sparse Permutations with Low Differential Uniformity'. In: *Finite Fields and Their Applications* 28 (Mar. 2014), pp. 214–243. DOI: 10.1016/j.ffa.2014.02.003. URL: https://hal.archives-ouvertes.fr/hal-01068860.

[6] T. Debris-Alazard, N. Sendrier and J.-P. Tillich. 'Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes'. In: *ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 11921. LNCS. Kobe, Japan: Springer, Dec. 2019, pp. 21–51. DOI: 10.1007/978-3-030-34578-5_2. URL: https://hal.inria.fr/hal-02424057.

[7] O. Fawzi, A. Grospellier and A. Leverrier. 'Constant overhead quantum fault-tolerance with quantum expander codes'. In: *FOCS 2018 - 59th Annual IEEE Symposium on Foundations of Computer Science*. Paris, France, Oct. 2018, pp. 743–754. DOI: 10.1109/FOCS.2018.00076. URL: https://hal.archives-ouvertes.fr/hal-01895430.

[8] A. Flórez Gutiérrez, G. Leurent, M. Naya-Plasencia, L. Perrin, A. Schrottenloher and F. Sibleyras. 'New results on Gimli: full-permutation distinguishers and improved collisions'. In: *Asiacrypt 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Daejeon / Virtual, South Korea, Dec. 2020. URL: https://hal.inria.fr/hal-03045986.

[9] M. Kaplan, G. Leurent, A. Leverrier and M. Naya-Plasencia. 'Breaking Symmetric Cryptosystems Using Quantum Period Finding'. In: *Crypto 2016 - 36th Annual International Cryptology Conference*. Ed. by M. Robshaw and J. Katz. Vol. 9815. LNCS - Lecture Notes in Computer Science. Santa Barbara, United States: Springer, Aug. 2016, pp. 207–237. DOI: 10.1007/978-3-662-53008-5_8. URL: https://hal.inria.fr/hal-01404196.

[10] G. Leurent and T. Peyrin. 'SHA-1 is a Shambles'. In: *USENIX 2020 - 29th USENIX Security Symposium*. Boston / Virtual, United States, Aug. 2020. URL: https://hal.inria.fr/hal-03136301.

[11] A. Leverrier. 'Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction'. In: *Physical Review Letters* 118.20 (May 2017), pp. 1–24. DOI: 10.1103/PhysRevLett.118.200501. URL: https://hal.inria.fr/hal-01652082.

[12] R. Misoczki, J.-P. Tillich, N. Sendrier and P. S. L. M. Barreto. 'MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes'. In: *IEEE International Symposium on Information Theory - ISIT 2013*. Istanbul, Turkey, July 2013, pp. 2069–2073. URL: https://hal.inria.fr/hal-00870929.

[13] L. Perrin. 'Partitions in the S-Box of Streebog and Kuznyechik'. In: *IACR Transactions on Symmetric Cryptology* 2019.1 (Mar. 2019), pp. 302–329. DOI: 10.13154/tosc.v2019.i1.302-329. URL: https://hal.inria.fr/hal-02396814.

12.2 Publications of the year

International journals

[14] I. Bardet, A. Capel, A. Lucia, D. Pérez-García and C. Rouzé. 'On the modified logarithmic Sobolev inequality for the heat-bath dynamics for 1D systems'. In: *Journal of Mathematical Physics* 62.6 (1st June 2021), p. 061901. DOI: 10.1063/1.5142186. URL: https://hal.archives-ouvertes.fr/hal-02436766.

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

[16] I. Bardet, M. Junge, N. LaRacuente, C. Rouzé and D. S. França. 'Group transference techniques for the estimation of the decoherence times and capacities of quantum Markov semigroups'. In: *IEEE Transactions on Information Theory* 67.5 (May 2021), pp. 2878–2909. DOI: 10.1109/TIT.2021.3065452. URL: https://hal.archives-ouvertes.fr/hal-02436767.

[17] R. Bhaumik, M. Nandi and A. Raychaudhuri. 'Improved indifferentiability security proof for 3-round tweakable Luby–Rackoff'. In: *Designs, Codes and Cryptography* 89.10 (Oct. 2021), pp. 2255–2281. DOI: 10.1007/s10623-021-00913-4. URL: https://hal.inria.fr/hal-03530983.

[18] O. Bronchain, S. Faust, V. Lallemand, G. Leander, L. Perrin and F.-X. Standaert. 'MOE: Multiplication Operated Encryption with Trojan Resilience'. In: *IACR Transactions on Symmetric Cryptology* 2021.1 (19th Mar. 2021), pp. 78–129. DOI: 10.46586/tosc.v2021.i1.78-129. URL: https://hal.inria.fr/hal-03453550.

[19] A. Couvreur and M. Lequesne. 'On the security of subspace subcodes of Reed-Solomon codes for public key encryption'. In: *IEEE Transactions on Information Theory* 68.1 (15th Oct. 2021), pp. 632–648. DOI: 10.1109/TIT.2021.3120440. URL: https://hal.archives-ouvertes.fr/hal-02938812.

[20] A. Denys, P. Brown and A. Leverrier. 'Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation'. In: *Quantum* 5 (13th Sept. 2021), p. 540. DOI: 10.22331/q-2021-09-13-540. URL: https://hal.inria.fr/hal-03344133.

[21] D. Dequal, L. Trigo Vidarte, V. Roman 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. Dunkelman, M. Eichlseder, D. Kales, N. Keller, G. Leurent and M. Schofnegger. 'Practical Key Recovery Attacks on FlexAEAD'. In: *Designs, Codes and Cryptography* (2022). URL: https://hal.inria.fr/hal-03528899.

[23] 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.

[24] A. Florez-Gutierrez, G. Leurent, M. Naya-Plasencia, L. Perrin, A. Schrottenloher and F. Sibleyras. 'Internal Symmetries and Linear Properties: Full-permutation Distinguishers and Improved Collisions on Gimli'. In: *Journal of Cryptology* 34.4 (Oct. 2021), p. 45. DOI: 10.1007/s00145-021-09413-z. URL: https://hal.inria.fr/hal-03528843.

[25] A. Grospellier, L. Grouès, A. Krishna and A. Leverrier. 'Combining hard and soft decoders for hypergraph product codes'. In: *Quantum* 5.432 (Apr. 2021). DOI: 10.22331/q-2021-04-15-432. URL: https://hal.inria.fr/hal-03108332.

International peer-reviewed conferences

[26] M. Bardet and P. Briaud. 'An algebraic approach to the Rank Support Learning problem'. In: PQCrypto 2021 - Post-Quantum Cryptography 12th International Workshop. Vol. 12841. Lecture Notes in Computer Science. Daejeon, South Korea: Springer, 20th July 2021, pp. 442–462. DOI: 10.1007/978-3-030-81293-5_23. URL: https://hal.inria.fr/hal-03158460.

[27] M. Bardet, R. Mora and J.-P. Tillich. 'Decoding Reed-Solomon codes by solving a bilinear system with a Gröbner basis approach'. In: ISIT 2021 - IEEE International Symposium on Information Theory. Proceedings of the IEEE Symposium on Information Theory. Melbourne, Australia: IEEE, 12th July 2021, pp. 872–877. DOI: 10.1109/ISIT45174.2021.9517838. URL: https://hal.inria.fr/hal-03533311.

[28] C. Beierle, P. Derbez, G. Leander, G. Leurent, H. Raddum, Y. Rotella, D. Rupprecht and L. Stennes. 'Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2'. In: EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 12697. Lecture Notes in Computer Science. Zagreb, Croatia: Springer, 16th June 2021, pp. 155–183. DOI: 10.1007/978-3-030-77886-6_6. URL: https://hal.inria.fr/hal-03529373.

[29] R. Bhaumik, X. Bonnetain, A. Chailloux, G. Leurent, M. Naya-Plasencia, A. Schrottenloher and Y. Seurin. 'QCB: Efficient Quantum-Secure Authenticated Encryption'. In: ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, 1st Dec. 2021, pp. 668–698. DOI: 10.1007/978-3-030-92062-3_23. URL: https://hal.inria.fr/hal-03516739.

[30] X. Bonnetain, G. Leurent, M. Naya-Plasencia and A. Schrottenloher. 'Quantum Linearization Attacks'. In: ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13090. Lecture Notes in Computer Science. Singapore / Virtual, Singapore: Springer International Publishing, 1st Dec. 2021, pp. 422–452. DOI: 10.1007/978-3-030-92062-3_15. URL: https://hal.inria.fr/hal-03516730.

[31] P. Briaud, J.-P. Tillich and J. Verbel. 'A polynomial time key-recovery attack on the Sidon cryptosystem'. In: SAC 2021 - Selected Areas in Cryptography. Victoria, Canada, 29th Sept. 2021. URL: https://hal.archives-ouvertes.fr/hal-03533464.

[32] M. Broll, F. Canale, A. Florez-Gutierrez, G. Leander and M. Naya-Plasencia. 'Generic Framework for Key-Guessing Improvements'. In: ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13090. Lecture Notes in Computer Science. Singapour, Singapore, 1st Dec. 2021, pp. 453–483. DOI: 10.1007/978-3-030-92062-3_16. URL: https://hal.inria.fr/hal-03528777.

[33] A. Canteaut, L. Kölsch, C. Li, C. Li, K. Li, L. Qu and F. Wiemer. 'Autocorrelations of Vectorial Boolean Functions'. In: *Progress in Cryptology – LATINCRYPT 2021*. LATINCRYPT 2021 - 7th International Conference on Cryptology and Information Security in Latin America. Vol. 12912. Lecture Notes in Computer Science. Bogota, Colombia: Springer International Publishing, 30th Sept. 2021, pp. 233–253. DOI: 10.1007/978-3-030-88238-9_12. URL: https://hal.inria.fr/hal-03520200.

[34] A. Chailloux, T. Debris-Alazard and S. Etinski. 'Classical and Quantum Algorithms for Generic Syndrome Decoding Problems and Applications to the Lee Metric'. In: *Post-Quantum Cryptography*. PQCrypto 2021 - Post-Quantum Cryptography 12th International Workshop. Vol. 12841. Lecture Notes in Computer Science. Daejeon, South Korea: Springer International Publishing, 15th July 2021, pp. 44–62. DOI: 10.1007/978-3-030-81293-5_3. URL: https://hal.inria.fr/hal-03529777.

[35] A. Chailloux and J. Loyer. 'Lattice Sieving via Quantum Random Walks'. In: ASIACRYPT 2021 - 27th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13093. Lecture Notes in Computer Science. Virtual, Singapore: Springer International Publishing, 1st Dec. 2021, pp. 63–91. DOI: 10.1007/978-3-030-92068-5_3. URL: https://hal.inria.fr/hal-03536963.

[36] A. Chattopadhyay, M. Khairallah, G. Leurent, Z. Najm, T. Peyrin and V. Velichkov. 'On the Cost of ASIC Hardware Crackers: A SHA-1 Case Study'. In: CT-RSA 2021 - The Cryptographer's Track at the RSA Conference. Vol. 12704. Lecture Notes in Computer Science. Virtual, United States: Springer, 11th May 2021, pp. 657–681. DOI: 10.1007/978-3-030-75539-3_27. URL: https://hal.inria.fr/hal-03529193.

[37] 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. DOI: 10.1109/ITW46852.2021.9457611. URL: https://hal.inria.fr/hal-03135797.

[38] P. Frixons, M. Naya-Plasencia and A. Schrottenloher. 'Quantum Boomerang Attacks and Some Applications'. In: SAC 2021 - Selected Areas in Cryptography. Virtual, Canada, 29th Sept. 2021. URL: https://hal.inria.fr/hal-03528590.

[39] P. Frixons and A. Schrottenloher. 'Quantum Security of the Legendre PRF'. In: MathCrypt 2021. Santa Barbara / Virtual, United States, 16th Aug. 2021. URL: https://hal.inria.fr/hal-03529834.

[40] G. Leurent and C. Pernot. 'New Representations of the AES Key Schedule'. In: EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 12696. Lecture Notes in Computer Science. Zagreb, Croatia: Springer, 16th June 2021, pp. 54–84. DOI: 10.1007/978-3-030-77870-5_3. URL: https://hal.inria.fr/hal-03529224.

[41] G. Leurent, C. Pernot and A. Schrottenloher. 'Clustering Effect in Simon and Simeck'. In: ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security. Vol. 13090. Lecture Notes in Computer Science. Virtual, Singapore: Springer, 1st Dec. 2021, pp. 272–302. DOI: 10.1007/978-3-030-92062-3_10. URL: https://hal.inria.fr/hal-03529507.

[42] 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: Schloss Dagstuhl, 6th Jan. 2021, 65:1–65:11. DOI: 10.4230/LIPIcs.ITCS.2021.65. URL: https://hal.inria.fr/hal-03135738.

Conferences without proceedings

[43] A. Denys, P. J. Brown and A. Leverrier. 'Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation'. In: ICQOM 2021 - International Conference on Quantum Communication. Paris, France, 18th Oct. 2021. URL: https://hal.inria.fr/hal-03537907.

[44] A. Denys, P. J. Brown and A. Leverrier. 'Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation'. In: QCrypt 2021 - 11th International Conference on Quantum Cryptography. Amsterdam / Virtual, Netherlands, 23rd Aug. 2021. URL: https://hal.inria.fr/hal-03537655.

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

[45] A. Canteaut and F.-X. Standaert. *Advances in Cryptology – EUROCRYPT 2021 - Part I*. Vol. 12696. Lecture Notes in Computer Science. Springer International Publishing, 2021. DOI: 10.1007/978-3-030-77870-5. URL: https://hal.inria.fr/hal-03520155.

[46] A. Canteaut and F.-X. Standaert. *Advances in Cryptology – EUROCRYPT 2021 - Part II*. Vol. 12697. Lecture Notes in Computer Science. Springer International Publishing, 2021. DOI: 10.1007/978-3-030-77886-6. URL: https://hal.inria.fr/hal-03520156.

[47] A. Canteaut and F.-X. Standaert. *Advances in Cryptology – EUROCRYPT 2021 - Part III*. Vol. 12698. Lecture Notes in Computer Science. Springer International Publishing, 2021. DOI: 10.1007/978-3-030-77883-5. URL: https://hal.inria.fr/hal-03520158.

[48] J. H. Cheon and J.-P. Tillich, eds. *PQCrypto 2021: International Conference on Post-Quantum Cryptography*. PQCrypto 2021. Vol. 12841. Lecture Notes in Computer Science. Daejeon, South Korea: Springer International Publishing, July 2021. DOI: 10.1007/978-3-030-81293-5. URL: https://hal.inria.fr/hal-03536710.

[49] M. Naya-Plasencia, R. Steinwand, M. Mosca and S. Jeffery. *Quantum Cryptanalysis (Dagstuhl Seminar 21421). Dagstuhl Report*. 2021. URL: https://hal.inria.fr/hal-03537617.

Doctoral dissertations and habilitation theses

[50] R. Bricout. 'How to use quantum algorithms to solve the knapsack problem and the syndrome decoding problem.' Sorbonne Université, 30th Mar. 2021. URL: https://hal.inria.fr/tel-03536935.

[51] D. Coggia. 'Techniques of cryptanalysis for symmetric-key primitives'. Sorbonne Université, 8th Oct. 2021. URL: https://tel.archives-ouvertes.fr/tel-03515131.

[52] M. Lequesne. 'Analysis of code-based post-quantum cryptosystems'. Sorbonne Université, 25th May 2021. URL: https://tel.archives-ouvertes.fr/tel-03467937.

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

[54] V. Vasseur. 'Post-quantum cryptography: a study of the decoding of QC-MDPC codes'. Université de Paris, 29th Mar. 2021. URL: https://tel.archives-ouvertes.fr/tel-03254461.

Reports & preprints

[55] J. Baena, P. Briaud, D. Cabarcas, R. Perlner, D. Smith-Tone and J. Verbel. *Improving Support-Minors rank attacks: applications to GeMSS and Rainbow*. 18th Jan. 2022. URL: https://hal.archives-ouvertes.fr/hal-03533455.

[56] I. Bardet, Á. Capel, L. Gao, A. Lucia, D. Pérez-García and C. Rouzé. *Entropy decay for Davies semigroups of a one dimensional quantum lattice*. 21st Jan. 2022. URL: https://hal.archives-ouvertes.fr/hal-03538315.

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

[58] 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.

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

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

[61] M. Broll, F. Canale, N. David, A. Florez-Gutierrez, G. Leander, M. Naya-Plasencia and Y. Todo. *Further Improving Differential-Linear Attacks: Applications to Chaskey and Serpent*. IACR Cryptology ePrint Archive, 15th June 2021. URL: https://hal.inria.fr/hal-03528725.

[62] A. Canteaut, A. Couvreur and L. Perrin. *Recovering or Testing Extended-Affine Equivalence*. 2nd Mar. 2021. URL: https://hal.inria.fr/hal-03156177.

[63] 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.

[64] 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.

[65] P. Charpin. *The crooked property*. Aug. 2021. URL: https://hal.inria.fr/hal-03091422.

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

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

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

Other scientific publications

[69] J. Baudrin. 'Cryptanalysis of a lightweight primitive submitted to the NIST standardization process: ASCON'. Université de Versailles Saint-Quentin (Paris Saclay), 28th Sept. 2021. URL: https://hal.inria.fr/hal-03521218.

[70] A. Denys, P. Brown and A. Leverrier. 'Explicit asymptotic secret key rate of continuous-variable QKD with an arbitrary modulation'. In: IQFA - 12ème Colloque du DGR IQFA. Lyon, France, 3rd Nov. 2021. URL: https://hal.inria.fr/hal-03537979.

12.3 Cited publications

[71] 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.

[72] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta and J.-P. Tillich. 'An Algebraic Attack on Rank Metric Code-Based Cryptosystems'. In: *EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Vol. 12107. Lecture Notes in Computer Science. Zagreb / Virtual, Croatia: Springer, May 2020, pp. 64–93. DOI: 10.1007/978-3-030-45727-3_3. URL: https://hal-unilim.archives-ouvertes.fr/hal-02303015.

[73] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich and J. Verbel. 'Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems'. In: *ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security*. Vol. 12491. Lecture Notes in Computer Science. Daejeon / Virtual, South Korea: Springer, Dec. 2020, pp. 507–536. DOI: 10.1007/978-3-030-64837-4_17. URL: https://hal.inria.fr/hal-03133479.

[74] 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.

[75] 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.

[76] 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'. working paper or preprint. Apr. 2020. URL: https://hal.inria.fr/hal-02997228.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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/.

[82] 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.

[83] 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.