Activity Report 2017

Project-Team SECRET

Security, Cryptology and Transmissions

RESEARCH CENTER
Paris

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team SECRET

Creation of the Project-Team: 2008 July 01

Keywords:

Computer Science and Digital Science:

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
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
B9.4.1. - Computer science
B9.4.2. - Mathematics
B9.8. - Privacy

1. Personnel

Research Scientists

Anne Canteaut [Team leader, Inria, Senior Researcher, HDR]
André Chailloux [Inria, Researcher]
Pascale Charpin [Inria, Emeritus, HDR]
Gaëtan Leurent [Inria, Starting Research Position]
Anthony Leverrier [Inria, Researcher, HDR]
María Naya Plasencia [Inria, Researcher, HDR]
Nicolas Sendrier [Inria, Senior Researcher, HDR]
Jean-Pierre Tillich [Inria, Senior Researcher, HDR]

Faculty Member

Christina Boura [Univ de Versailles Saint-Quentin-en-Yvelines, Associate Professor, from Sep 2017, en délégation]

Post-Doctoral Fellow

Leo Perrin [Inria, from Sep 2017, Fondation Sciences Mathématiques de Paris]

PhD Students

Xavier Bonnetain [Univ Pierre et Marie Curie, AMX]
Rémi Bricout [Univ Pierre et Marie Curie, from Sep 2017, AMN]
Rodolfo Canto Torres [Inria]

Kevin Carrier [Ministère de la Défense]
Kaushik Chakraborty [Inria, until Oct 2017]
Julia Chaulet [Thales, until Mar 2017]
Thomas Debris [Univ Pierre et Marie Curie]
Sébastien Duval [Univ Pierre et Marie Curie]
Shouvik Ghorai [Univ Pierre et Marie Curie, from Oct 2017]
Antoine Grospellier [Univ Pierre et Marie Curie, AMN]
Adrien Hauteville [Univ de Limoges, until Sep 2017]
Matthieu Lequesne [Univ Pierre et Marie Curie, from Sep 2017, AMX]
Vivien Londe [Univ de Bordeaux, AMX]
Andrea Olivo [Inria, from Nov 2017]
Yann Rotella [Inria]
Ferdinand Sibleyras [Inria, from Oct 2017, DGA-Inria]
Valentin Vasseur [Univ René Descartes, from Oct 2017]

Interns

Sristy Agrawal [Inria, from Jun 2017 until Aug 2017]
Tim Beyne [Inria, from Aug 2017 until Sep 2017, Univ. Leuven, Belgium]
Mathilde de La Morinerie [Inria, from Apr 2017 until Jul 2017, Ecole Polytechnique]
Anirudh Krishna [Univ. Sherbroke, Canada, from Sep 2017, MITACS]
Matthieu Lequesne [Inria, from Mar 2017 until Aug 2017]
André Schrottenloher [Inria, from Mar 2017 until Aug 2017]
Ferdinand Sibleyras [Inria, from Mar 2017 until Aug 2017]
Valentin Vasseur [Inria, from Mar 2017 until Aug 2017]
Matthieu Vieira [Inria, from May 2017 until Jul 2017]

Administrative Assistants

Laurence Bourcier [Inria]
Christelle Guiziou [Inria]

Visiting Scientists

Christof Beierle [Univ. Bochum, Germany, from Apr 2017 until Jun 2017]
Özgül Küçük [Istanbul Bilgi Univ., Turkey, from Jul 2017 until Aug 2017, bourse SSHN]
Thomas Peyrin [NTU, Singapore, May 2017 and July 2017]

2. Overall Objectives

2.1. Presentation and scientific foundations

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. This work is essential since the current situation of cryptography is rather fragile. Many cryptographic protocols are now known whose security can be formally proved assuming that the involved cryptographic primitives are ideal (random oracle model, ideal cipher model...). However, the security of the available primitives has been either threatened by recent progress in cryptanalysis or by the possible invention of a large quantum computer. In other words, there is usually no concrete algorithm available to instantiate in practice the ideal "black boxes" used in these protocols!

In this context, our research work focuses on both families of cryptographic primitives, *symmetric* and *asymmetric* primitives.

2.2. Main topics

Our domain in cryptology includes the analysis and the design of

- symmetric primitives (a.k.a. secret-key algorithms),
- public-key primitives based on hard problems coming from coding theory which are likely to be resistant against a quantum computer,
- quantum cryptographic protocols whose security does not rely on computational assumptions but on the laws of quantum physics.

3. Research Program

3.1. Scientific foundations

Our approach relies on a competence whose impact is much wider than cryptology. Our tools come from information theory, discrete mathematics, probabilities, algorithmics, quantum physics... Most of our work mixes fundamental aspects (study of mathematical objects) and practical aspects (cryptanalysis, design of algorithms, implementations). Our research is mainly driven by the belief that discrete mathematics and algorithmics of finite structures form the scientific core of (algorithmic) data protection.

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. The process which has led to the new block cipher standard AES in 2001 was the outcome of a decade of research in symmetric cryptography, where new attacks have been proposed, analyzed and then thwarted by some appropriate designs. However, even if its security has not been challenged so far, it clearly appears that the AES cannot serve as a Swiss 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 (like authenticated encryption). The past decade has then been characterized by a multiplicity of new proposals. This proliferation of symmetric primitives has been amplified by several public competitions (eSTREAM, SHA-3, CAESAR...) which have encouraged innovative constructions and promising but unconventional designs. We are then facing up to a very new situation where implementers need to make informed choices among more than 40 lightweight block ciphers [1] or 57 new authenticated-encryption schemes [2]. Evaluating the security of all these proposals has then become a primordial task which requires the attention of the community.

In this context we believe that the cryptanalysis effort cannot scale up without an in-depth study of the involved algorithms. Indeed most attacks are described as ad-hoc techniques dedicated to a particular cipher. To determine whether they apply to some other primitives, it is then crucial to formalize them in a general setting. Our approach relies on the idea that a unified description of generic attacks (in the sense that they apply to a large class of primitives) is the only methodology for a precise evaluation of the resistance of all these new proposals, and of their security margins. In particular, such a work prevents misleading analyses based on wrong estimations of the complexity or on non-optimized algorithms. It also provides security criteria which enable designers to guarantee that their primitive resists some families of attacks. The main challenge is to provide a generic description which captures most possible optimizations of the attack.

[1] 35 are described on https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers.

[2] see http://competitions.cr.yp.to/caesar-submissions.html

3.3. Code-based cryptography

Public-key cryptography is one of the key tools for providing network security (SSL, e-commerce, e-banking...). The security of nearly all public-key schemes used today relies on the presumed difficulty of two problems, namely factorization of large integers or computing the discrete logarithm over various groups. The hardness of those problems was questioned in 1994 [3] when Shor showed that a quantum computer could solve them efficiently. Though large enough quantum computers that would be able to threaten the existing cryptosystems do not exist yet, the cryptographic research community has to get ready and has to prepare alternatives. This line of work is usually referred to as *post-quantum cryptography*. This has become a prominent research field. Most notably, an international call for post-quantum primitives [4] has been launched by the NIST, with a submission deadline in November 2017.

The research of the project-team in this field is focused on the design and cryptanalysis of cryptosystems making use of coding theory. Code-based cryptography is one the main techniques for post-quantum cryptography (together with lattice-based, multivariate, or hash-based cryptography).

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 unconditional 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. The first part builds upon our expertise in classical coding theory whereas the second axis focuses on obtaining security proofs for quantum protocols or on devising quantum cryptographic protocols (and more generally quantum protocols related to cryptography). A close relationship with partners working in the whole area of quantum information processing in the Parisian region has also been developed through our participation to the Fédération de Recherche “PCQC” (Paris Centre for Quantum Computing).

4. Application Domains

4.1. Cryptographic primitives

Our major application domain is the design of cryptographic primitives, especially for platforms with restricting implementation requirements. For instance, we aim at recommending (or designing) low-cost (or extremely fast) encryption schemes, or primitives which remain secure against quantum computers.

4.2. Code Reconstruction

To evaluate the quality of a cryptographic algorithm, it is usually assumed that its specifications are public, as, in accordance with Kerckhoffs principle, it would be dangerous to rely, even partially, on the fact that the adversary does not know those specifications. However, this fundamental rule does not mean that the specifications are known to the attacker. In practice, before mounting a cryptanalysis, it is necessary to strip off the data. This reverse-engineering process is often subtle, even when the data formatting is not concealed on purpose. A typical case is interception: some raw data, not necessarily encrypted, is observed out of a noisy channel. To access the information, the whole communication system has first to be disassembled and every

[3] P. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, FOCS 1994.

[4] http://csrc.nist.gov/groups/ST/post-quantum-crypto/

constituent reconstructed. A transmission system actually corresponds to a succession of elements (symbol mapping, scrambler, channel encoder, interleaver...), and there exist many possibilities for each of them. In addition to the “preliminary to cryptanalysis” aspect, there are other links between those problems and cryptology. They share some scientific tools (algorithmics, discrete mathematics, probability...), but beyond that, there are some very strong similarities in the techniques.

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. NIST post-quantum cryptography standardisation

The end of this year was the deadline to submit proposals to the NIST competition [5], whose purpose is to standardize quantum-safe public-key primitives. This call concerns all three major cryptographic primitives, namely public-key cryptosytems, key-exchange protocols and digital signature schemes. The most promising techniques today for addressing this issue are code-based cryptography, lattice-based cryptography, mutivariate cryptography, and hash-based cryptography.

We have contributed to three proposals to the NIST call. In two of them, “BIKE” [67] and “Big Quake” [69], our action is central and we also have a marginal participation in another, “Classic McEliece”. Those projects are of great importance for us because they are a means to demonstrate our long lasting expertise in code-based cryptography. They are the product of numerous research works, including several PhD theses, on the design, the implementation, and the cryptanalysis of code-based cryptographic primitives. There are 69 projects in that call, which will be evaluated by the NIST and the academic cryptographic community in the next three to five years and whose outcome will certainly influence cryptographic applications for one or several decades.

5.1.2. Quantum symmetric cryptanalysis and collision search

The resistance of symmetric primitives to quantum computers is a topic that has received recently a lot of attention from our community. The ERC starting grant QUASYModo on this subject, awarded to M. Naya-Plasencia, has started in September 2017. We have continued the work started last year obtaining new results, as cryptanalysis of concrete proposals [44], or analysis on attacks considering modular additions (preliminary described in [14]). In particular, we have proposed in [47] a new quantum algorithm for finding collisions. This new algorithm, based on BHT, exploits distinguished points as well as an improved optimization of the parameters, and allows to find for the first time, collisions on n bits with a better time complexity than $2^{n/2}$. Its time and query complexity are of about $2^{2n/5}$, needing $2^{n/5}$ classical memory and a polynomial amount of quantum memory. As collision search is a tool widely used in symmetric cryptanalysis, this algorithm, that also can be applied to multiple preimage search, considerably improves the best known previous attacks when having a relatively small quantum computer available.

5.1.3. Émergences grant on quantum money

André Chailloux was awarded an Émergences grant from the city of Paris for a project on quantum money. This project aims at providing a comprehensive theoretical and experimental study of unforgeable quantum money, one of the most powerful protocols in quantum information science, and historically the first. A quantum money scheme enables a secure transaction between a client, a vendor and a bank via the use of a credit card or banknotes, with maximal security guarantees, unreachable with classical technologies. This application is central in the context of the emerging quantum network infrastructures guaranteeing the long-term security of data and communications against all-powerful adversaries.

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

Quantum money has been largely considered difficult to bring to the experimental realm, but a demonstration became more accessible recently, thanks to the conception of new practical schemes. The goal of our project will be to perform a theoretical analysis of such schemes, both in the discrete and continuous-variable frameworks, to adapt them to realistic conditions, and to implement them using state-of-the-art photonic quantum technologies. The project, centered around Inria, is interdisciplinary at its core, bringing together young partners with world leading expertise in all aspects of the proposed work, including theoretical and experimental quantum cryptography.

6. New Software and Platforms

6.1. CFS

FUNCTIONAL DESCRIPTION: Reference implementation of parallel CFS (reinforced version of the digital signature scheme CFS). Two variants are proposed, one with a « bit-packing » finite field arithmetic and an evolution with a « bit-slicing » finite-field arithmetic (collaboration with Peter Schwabe). For 80 bits of security the running time for producing one signature with the « bit-packing » variant is slightly above one second. This is high but was still the fastest so far. The evolution with the « bit-slicing » arithmetic produces the same signature in about 100 milliseconds.

- Participants: Grégory Landais and Nicolas Sendrier
- Contact: Nicolas Sendrier
- URL: https://gforge.inria.fr/projects/cfs-signature/

6.2. 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.

- Participants: Grégory Landais and Nicolas Sendrier
- Contact: Nicolas Sendrier
- URL: https://gforge.inria.fr/projects/collision-dec/

6.3. ISDF

FUNCTIONAL DESCRIPTION: Implementation of the Stern-Dumer decoding algorithm, and of a varaint of the algorithm due to May, Meurer and Thomae.

- Participants: Grégory Landais and Nicolas Sendrier
- Contact: Anne Canteaut
- URL: https://gforge.inria.fr/projects/collision-dec/

7. New Results

7.1. Symmetric cryptology

Participants: Xavier Bonnetain, Christina Boura, Anne Canteaut, Pascale Charpin, Sébastien Duval, Gaëtan Leurent, María Naya Plasencia, Yann Rotella, Ferdinand Sibleyras, Tim Beyne, Mathilde de La Morinerie, André Schrottenloher.

7.1.1. Primitives: block ciphers, stream ciphers, ...

Our recent results mainly concern either the analysis and design of lightweight block ciphers.

Recent results:

- Analysis of linear invariant attacks [41], [54], [28], [29]: C. Beierle, A. Canteaut, G. Leander and Y. Rotella have studied SPN ciphers with a very simple key schedule, such as PRINCE. They introduce properties of the linear layer and of the round constants than can be used to prove that there are no nonlinear invariants.
- Analysis of the probability of differential characteristics for unkeyed constructions [19]: This work shows that the probabilities of some fixed-key differential characteristics are higher than expected when assuming independent S-Boxes. This leads to improved attacks against ROADRUNNER and Minalpher.
- Design and study of a new construction for low-latency block ciphers, named *reflection ciphers*, which generalizes the so-called α-reflection property exploited in PRINCE. This construction aims at reducing the implementation overhead of decryption on top of encryption [15].
- Modular construction of primitives with code-hardness, time-hardness or memory-hardness [42]. A. Biryukov and L. Perrin have introduced new definitions to formalize hardness, and constructions that are hard to compute for common users, but easy for users knowing a secret.
- Design of encryption schemes for efficient homomorphic-ciphertext compression: A. Canteaut, M. Naya-Plasencia together with their coauthors have investigated the constraints on the symmetric cipher imposed by this application and they have proposed some solutions based on additive IV-based stream ciphers [17].

7.1.2. Cryptographic properties and construction of appropriate building blocks

The construction of building blocks which guarantee a high resistance against the known attacks is a major topic within our project-team, for stream ciphers, block ciphers and hash functions. The use of such optimal objects actually leads to some mathematical structures which may be at the origin of new attacks. This work involves fundamental aspects related to discrete mathematics, cryptanalysis and implementation aspects. Actually, characterizing the structures of the building blocks which are optimal regarding to some attacks is very important for finding appropriate constructions and also for determining whether the underlying structure induces some weaknesses or not. For these reasons, we have investigated several families of filtering functions and of S-boxes which are well-suited for their cryptographic properties or for their implementation characteristics.

Recent results:

- Boolean functions with restricted input: Y. Rotella, together with C. Carlet and P. Méaux, has introduced some new criteria on filtering Boolean functions, which measure the security of the recent stream cipher proposal FLIP. Indeed, in this context, the inputs of the filtering function are not uniformly distributed but have a fixed Hamming weight. Then, the main properties of filtering functions (e.g. nonlinearity, algebraic immunity...) have been revisited [20].
- Differential Equivalence of Sboxes: C. Boura, A. Canteaut and their co-authors have studied two notions of differential equivalence of Sboxes corresponding to the case when the functions have the same difference table, or when their difference tables have the same support [45]. They proved that these two notions do not coincide, and that they are invariant under some classical equivalence relations like EA and CCZ equivalence. They also proposed an algorithm for determining the whole equivalence class of a given function.
- A. Canteaut, S. Duval and L. Perrin proposed a construction of a new family of permutations over binary fields of dimension $(4k+2)$ with good cryptographic properties. An interesting property is that this family includes as a specific case the only known APN permutation of an even number of variables [55], [18].

- Construction of cryptographic permutations over finite fields with a sparse representation: P. Charpin, together with N. Cepak and E. Pasalic, exhibited permutations which are derived from sparse functions via linear translators [21].
- New methods for determining the differential spectrum of an Sbox: P. Charpin and G. Kyureghyan have proved that the whole differential spectrum of an Sbox can be determined without examining all derivatives of the mapping, but only the derivatives with respect to an element within a hyperplane [23]. Also, they have proved that, for mappings of a special shape, it is enough to consider the derivatives with respect to all elements within a suitable multiplicative subgroup of $\mathbb{F}_{2^n}$.

7.1.3. Side-channel attacks

Physical attacks must be taken into account in the evaluation of the security of lightweight primitives. Indeed, these primitives are often dedicated to IoT devices in pervasive environments, where an attacker has an easy access to the devices where the primitive is implemented.

Recent results:

- Differential fault attack against LS-designs and SCREAM [52]: this attack generalized previous work on PRIDE to the class of LS-Designs.

7.1.4. Modes of operation and generic attacks

In order to use a block cipher in practice, and to achieve a given security notion, a mode of operation must be used on top of the block cipher. Modes of operation are usually studied through security, and we now that their use is secure as long as the underlying primitive are secure, and we respect some limits on the amount of data processed. The analysis of generic attack helps us understand what happens when the hypothesis of the security proofs do not hold, or the corresponding limits are not respected. Comparing proofs and attack also shows gaps where our analysis is incomplete, and improved proof or attacks are required.

Recent results:

- Use of block ciphers operating on small blocks with the CBC mode [31]: it is well-known that CBC is not secure if the same key is used for encrypting $2^{n/2}$ blocks of plaintext, but this threat has traditionally been dismissed as impractical, even for 64-bit blocks. K. Bhargavan and G. Leurent demonstrated concrete attacks that exploit such short block ciphers in CBC mode.
- Use of block ciphers operating on small blocks with the CTR mode [77]: the security proof of the CTR mode also requires that no more than $2^{n/2}$ blocks are encrypted with the same key, but the known attacks reveal very little information and are considered even less problematic than on CBC. During his internship with G. Leurent, F. Sibleyras has studied concrete attacks against the CTR mode when processing close to $2^{n/2}$ blocks of data, and has shown that an attacker can actually extract as much information as in the case of CBC encryption.
- Improved generic attacks against hash-based MAC [25].
- Modes of operation for full disk encryption [51]: L. Khati, N. Mouha and D. Vergnaud have classified various FDE modes of operation according to their security in a setting where there is no space to store additional data, like an IV or a MAC value. They also introduce the notion of a diversifier, which does not require additional storage, but allows the plaintext of a particular sector to be encrypted into different ciphertexts.

7.2. Code-based cryptography

Participants: Rodolfo Canto Torres, Julia Chaulet, André Chailloux, Thomas Debris, Adrien Hauteville, Nicolas Sendrier, Jean-Pierre Tillich, Matthieu Lequesne, Valentin Vasseur, Matthieu Vieira.

The first cryptosystem based on error-correcting codes was a public-key encryption scheme proposed by McEliece in 1978; a dual variant was proposed in 1986 by Niederreiter. We proposed the first (and only) digital signature scheme in 2001. Those systems enjoy very interesting features (fast encryption/decryption, short signature, good security reduction) but also have their drawbacks (large public key, encryption overhead, expensive signature generation). Some of the main issues in this field are

- security analysis, including against a quantum adversary, implementation and practicality of existing solutions,
- reducing the key size, *e.g.*, by using rank metric instead of Hamming metric, or by using structured codes,
- addressing new functionalities, like identity-based encryption, hashing or symmetric encryption.

As mentioned in Section 5.1.1, the NIST is currently running a standardization effort for quantum-safe cryptography, where code based cryptography is a promising technique.

Our work in this area can be decomposed as follows:

- suggesting code-based solutions to the NIST competition;
- cryptanalyzing code-based schemes;
- fundamental work on code-based cryptography.

7.2.1. Code-based solutions to the NIST competition

We have proposed two key-exchange protocols to the NIST competition:

- the first one [67] is based on quasi-cyclic MDPC codes and the work [40];
- the second one [69] is based on quasi-cyclic Goppa codes.

Both of them are able to reduce significantly the keysizes by relying on quasi-cyclic codes.

7.2.2. Cryptanalysis of code-based cryptography

Here our work can be summarized as follows:

- cryptanalysis of McEliece schemes based on wild Goppa codes over quadratic extension fields [24];
- improving generic attacks on rank metric codes [68];
- side-channel attacks on quasi-cyclic MDPC bit flipping decoder [74].

7.2.3. Fundamental work on code-based cryptography

- studying precisely the complexity of statistical decoding techniques [71], [48];
- suggesting the first code-based identity-based encryption by using rank metric codes [49];
- suggesting a code-based signature scheme [43];
- analysing and improving the decoding of quasi-cyclic MDPC codes [12], [78];
- studying families of codes that might be used in a cryptographic setting [53].
- improving the complexity of quantum decoding algorithms [50];
- studying [70], [56], [30] whether security reductions for signature schemes are quantum safe when considering the quantum random oracle model (QROM). We were particularly interested in code-based Full Domain Hash constructions. We show that if the underlying correcting code we use has good pseudo random properties then it is possible to perform a quantum security reduction in the QROM.

7.3. Quantum Information

Participants: Xavier Bonnetain, Rémi Bricout, Kaushik Chakraborty, André Chailloux, Shouvik Ghorai, Antoine Grospellier, Anirudh Krishna, Gaëtan Leurent, Anthony Leverrier, Vivien Londe, María Naya Plasencia, Andrea Olivo, Jean-Pierre Tillich, Sristy Agrawal, André Schrottenloher.

Our research in quantum information focusses on several axes: quantum codes with the goal of developing better error correction strategies to build large quantum computers, quantum cryptography which exploits the laws of quantum mechanics to derive security guarantees, relativistic cryptography which exploits in addition the fact that no information can travel faster than the speed of light and finally quantum cryptanalysis which investigates how quantum computers could be harnessed to attack classical cryptosystems.

7.3.1. Quantum codes

Protecting quantum information from external noise is an issue of paramount importance for building a quantum computer. It also worthwhile to notice that all quantum error-correcting code schemes proposed up to now suffer from the very same problem that the first (classical) error-correcting codes had: there are constructions of good quantum codes, but for the best of them it is not known how to decode them in polynomial time.

Recent results:

- Decoding algorithm for quantum expander codes [72], [57], [58], [59], [73], [35]. In this work, A. Grospellier, A. Leverrier and O. Fawzi analyze an efficient decoding algorithm for quantum expander codes and prove that it suppresses errors exponentially in the local stochastic noise model. As an application, this shows that this family of codes can be used to obtain quantum fault-tolerance with only a constant overhead in terms of qubits, compared to a polylogarithmic overhead as in previous schemes. This is a crucial step in order to eventually build large universal quantum computers.
- Construction of quantum LDPC codes from regular tessellations of hyperbolic 4-space [64], [62]. In this work, V. Londe proposes a variant of a construction of Guth and Lubotzky that yields a family of constant rate codes with a polynomial minimum distance. The main interest of this construction is that is is based on a regular tessellation of hyperbolic 4-space by hypercubes. This nice local structure is exploited to design and analyze an efficient decoding algorithm that corrects arbitrary errors of weight logarithmic in the code length.
- Construction of quantum codes based on the real projective space [63]. In this work, V. Londe studies a family of almost LDPC codes with a large minimum distance and another efficient decoding algorithm.
- We were also awarded a European Quantera project “QCDA” to investigate and develop better quantum error-correcting codes and schemes for fault-tolerance.

7.3.2. Quantum cryptography

Quantum cryptography exploits the laws of quantum physics to establish the security of certain cryptographic primitives. The most studied one is certainly quantum key distribution, which allows two distant parties to establish a secret using an untrusted quantum channel. Our activity in this field is particularly focussed on protocols with continuous variables, which are well-suited to implementations. Another primitive is quantum money and was in fact the first proposed idea of quantum cryptography in the 70s. However, this primitive hasn’t received much attention because its implementation requires quantum memories, which weren’t available until now.

Recent results:

- Full security proof for BB84 [27]. In this work A. Leverrier, with M. Tomamichel, give a detailed and self-contained security proof for BB84, the most studied quantum key distribution protocol. Many simplified proofs appear in the literature, but are usually incomplete and fail to address the whole protocol.
- Security proof of continuous-variable quantum key distribution [26], [36], [37]. In this work, A. Leverrier establishes for the first time a security reduction from general attacks to a class of simple attacks called “collective Gaussian” attacks. This result exploits in a crucial way a recent Gaussian de Finetti theorem that applies to quantum systems of infinite dimension [75], [61], [34].

- In [22], A. Chailloux and I. Kerenidis present an extended version on results for optimal quantum bit commitment and coin flipping. Those results show what is the best way to quantumly perform those protocols in the information-theoretic setting. In the extended version, we also show that the bound for quantum bit commitment cannot be achieved classically, even with an access to an ideal coin flipping primitive.
- We were also awarded an ANR project quBIC and an "Émergence" project from Ville de Paris to study quantum money schemes in collaboration with UPMC, LKB and IRIF.

7.3.3. Relativistic cryptography

Two-party cryptographic tasks are well-known to be impossible without complexity assumptions, either in the classical or the quantum world. Remarkably, such no-go theorems become invalid when adding the physical assumption that no information can travel faster than the speed of light. This additional assumption gives rise to the emerging field of relativistic cryptography. We worked on this topic for several years and Andrea Olivo was recruited as a PhD student to continue working on both theoretical and practical aspects of relativistic cryptography.

Recent results:

- Relativistic zero-knowledge: In [46], A. Chailloux and A. Leverrier construct a relativistic zero-knowledge protocol for any NP complete problem. The main technical tool is the analysis of quantum consecutive measurements, which allows us to prove security against quantum adversaries. While this technique is applied to the relativistic setting, it also has implications for more standard quantum cryptography.
- In [16], R. Bricout and A. Chailloux study relativistic multi-round bit commitment schemes. They show optimal classical cheating strategies for the canonical F_Q commitment scheme. This shows that the security proof derived last year on the relativistic F_Q commitment scheme is essentially optimal against classical adversaries.

7.3.4. Quantum cryptanalysis of symmetric primitives

Symmetric cryptography seems at first sight much less affected in the post-quantum world than asymmetric cryptography: its main known threat seemed for a long time Grover's algorithm, which allows for an exhaustive key search in the square root of the normal complexity. For this reason, it was usually believed that doubling key lengths suffices to maintain an equivalent security in the post-quantum world. However, a lot of work is certainly required in the field of symmetric cryptography in order to "quantize" the classical families of attacks in an optimized way, as well as to find new dedicated quantum attacks. M. Naya Plasencia has recently been awarded an ERC Starting grant for her project named QUASYModo on this topic, that has started on september 2017.

Recent results:

- In a result published in Asiacrypt 2017 [47] and done during the internship of André Schrottenloher [76] a new quantum algorithm for finding collisions is proposed. The algorithm is based on BHT and exploits distinguished points as well as an improved optimization of the parameters, and allows to find, for the first time, collisions on n bits with a better time complexity than $2^{n/2}$ while needing a polynomial amount of quantum memory.
- Two of the most popular symmetric cryptanalysis families are differential and linear cryptanalysis. In [60] (also presented in [33]), G. Leurent, M. Kaplan, A. Leverrier and M. Naya-Plasencia have proposed efficient ways of quantizing these attacks in different models, obtaining some non-intuitive results: just quantizing the best classical attack does not always provide the best quantum attack.
- X. Bonnetain and M. Naya-Plasencia have obtained some new results, preliminarily described in [14] and presented at [38], that consider the tweak proposed at Eurocrypt this year of using modular additions to counter Simon's attacks. They have studied the best attacks on these constructions, that use Kuperberg's algorithm. They have also simulated the cost of such attacks, improved the algorithm, applied this to a widely-used construction and to some slide attacks, and finally

dimensionated the symmetric construction in order to stay secure to these attacks. They have concluded that the proposed tweak does not seam realistic.

- In [44], an attack on the superposition model of the CAESAR cadidate AEZ is proposed, showing that this construction would be completely broken in that scenario.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

- **Thales** ($02/14 \rightarrow 01/17$)
  Funding for the supervision of Julia Chaulet's PhD.
  30 kEuros.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- **ANR BRUTUS** ($10/14 \rightarrow 09/18$)
  Authenticated Ciphers and Resistance against Side-Channel Attacks
  ANR program: Défi Société de l'information et de la communication
  Partners: ANSSI, Inria (project-team SECRET and project-team MARELLE), Orange, University of Lille, University of Rennes, University Versailles-Saint Quentin
  160 kEuros
  The Brutus project aims at investigating the security of authenticated encryption systems. We plan to evaluate carefully the security of the most promising candidates to the CAESAR competition, by trying to attack the underlying primitives or to build security proofs of modes of operation. We target the traditional black-box setting, but also more "hostile" environments, including the hardware platforms where some side-channel information is available.
- **ANR DEREC** ($10/16 \rightarrow 09/21$)
  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 (**$10/17 \to 09/21$**)**
  Code-based cryptography
  ANR Program: AAP Générique 2017
  Partners: Inria SECRET (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 (**$10/17 \to 09/21$**)**
  Quantum Banknotes and Information-Theoretic Credit Cards
  ANR Program: AAP Générique 2017
  Partners: Univ. Paris-Diderot (coordinator), Inria SECRET, 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.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

NXP Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

Online banking, e-commerce, telemedicine, mobile communication, and cloud computing depend fundamentally on the security of the underlying cryptographic algorithms. Public-key algorithms are particularly crucial since they provide digital signatures and establish secure communication without requiring in-person meetings. Essentially all applications today are based on RSA or on the discrete-logarithm problem in finite fields or on elliptic curves. Cryptographers optimize parameter choices and implementation details for these systems and build protocols on top of these systems; cryptanalysts fine-tune attacks and establish exact security levels for these systems. Alternative systems are far less visible in research and unheard of in practice. It might seem that having three systems offers enough variation, but these systems are all broken as soon as large quantum computers are built. The EU and governments around the world are investing heavily in building quantum computers; society needs to be prepared for the consequences, including cryptanalytic attacks accelerated by these computers. Long-term confidential documents such as patient health-care records and state secrets have to guarantee security for many years, but information encrypted today using RSA or elliptic curves and stored until quantum computers are available will then be as easy to decipher as Enigma-encrypted messages are today. PQCRYPTO will allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet of Things. PQCRYPTO will provide efficient implementations of high-security post-quantum cryptography for a broad spectrum of real-world applications.

9.2.1.2. QCALL

Title: Quantum Communications for ALL

Programm: H2020-MSCA-ITN-2015

Duration: December 2016 - November 2020

Coordinator: University of Leeds (UK)

Other partners: see http://www.qcall-itn.eu/

Inria contact: Anthony Leverrier

QCALL is a European Innovative Training Network that endeavors to take the next necessary steps to bring the developing quantum technologies closer to the doorsteps of end users. QCALL will empower a nucleus of 15 doctoral researchers in this area to provide secure communications in the European continent and, in the long run, to its connections worldwide.

9.2.1.3. ERC QUASYModo

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

Program: ERC starting grant

Duration: September 2017 - August 2022

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.

9.2.2. Collaborations in European Programs, Except FP7 & H2020

9.2.2.1. COST Action IC1306

Program: COST

Project acronym: ICT COST Action IC1306

Project title: Cryptography for Secure Digital Interaction

Duration: January 2014 - November 2017

Coordinator: Claudio Orlandi, Aarhus University, Denmark

Other partners: see http://www.cost.eu/domains_actions/ict/Actions/IC1306

Abstract: The aim of this COST action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments.

Anne Canteaut is co-leader of the working group on cryptographic primitives. She co-organized a 2-day workshop for PhD students and early-career researchers in symmetric cryptography, DISC 2016 (Bochum, Germany, March 23-24 2016) and a winter school dedicated to Symmetric Cryptography and Blockchain (Torremolinos, Spain, February 19-23, 2018). She also serves on the program committee of the CryptoAction Symposium organized every year.

9.2.2.2. QCDA

Program: QuantERA ERA-NET Cofund in Quantum Technologies

Project acronym: QCDA

Project title: Quantum Code Design and Architecture

Duration: February 2018 - January 2021

Coordinator: Earl Campbell, University of Sheffield, UK

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

Abstract: 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.

9.3. International Initiatives

9.3.1. Inria Associate Teams Not Involved in an Inria International Labs

9.3.1.1. CHOCOLAT

Title: Chosen-prefix Collision Attack on SHA-1 with ASICs Cluster

International Partner (Institution - Laboratory - Researcher):

NTU (Singapore) - SYLLAB - Peyrin Thomas

Start year: 2017

See also: https://team.inria.fr/chocolat/

The hash function SHA-1 is one of the most widely used hash functions in the industry, but it has been shown to not be collision-resistant by a team of Chinese researchers led by Prof. Wang in 2005. However, a real pair of colliding messages was only published recently by a team from CWI and Google, because the estimated attack complexity is around 2^{63} SHA-1 computations (this represents about 70000 years of computation on a normal PC).

While this SHA-1 collision clearly demonstrates the weakness of the algorithm, a much more powerful attack would be to find a collision such that the prefix of the colliding messages is chosen by some challenger beforehand. In particular, this would allow creating a rogue certificate authority certificate that would be accepted by browsers. Such an attack has already been deployed for certificates using the MD5 hash function, but MD5 is much weaker than SHA-1 and it has already been removed from most security applications. SHA-1 is still widely used and performing such an attack for certificates using SHA-1 would have a very big impact.

The objective of the project is to design a chosen-prefix collision attack against the SHA-1 hash function, and to implement the attack in practice. We estimate this will require 2^{70} computations.

9.3.2. Inria International Partners

9.3.2.1. Declared Inria International Partners

Title: Discrete Mathematics, Codes and Cryptography

International Partner (Institution - Laboratory - Researcher):

Indian Statistical Institute (India) - Cryptology Research Group - Bimal Roy

Duration: 2014 - 2018

Start year: 2014

Today's cryptology offers important challenges. Some are well-known: Can we understand existing cryptanalysis techniques well enough to devise criterion for the design of efficient and secure symmetric cryptographic primitives? Can we propose cryptographic protocols which offer provable security features under some reasonable algorithmic assumptions? Some are newer: How could we overcome the possible apparition of a quantum computer with its devastating consequences on public key cryptography as it is used today? Those challenges must be addressed, and some of the answers will involve tools borrowed to discrete mathematics, combinatorics, algebraic coding theory, algorithmic. The guideline of this proposal is to explore further and enrich the already well established connections between those scientific domains and their applications to cryptography and its challenges.

9.3.2.2. Informal International Partners

- Nanyang Technological University (Singapore): cryptanalysis of symmetric primitives.
- Ruhr-Universität Bochum (Germany): design and cryptanalysis of symmetric primitives.

9.3.3. Participation in Other International Programs

Anirudh Krishna, PhD student at Sherbroke University (Canada) spends six months in our team within the MITACS program.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Giannicola Scarpa, Universidad Complutense de Madrid, Spain, April 2017.
- Thomas Peyrin, NTU Singapore, May 2017, July 2017 and January 2018.
- Kaisa Nyberg, University of Helsinki, Finlande, May 2017.
- Adi Shamir, The Weizmann Institute of Science, Rehovot, Israel, May 2017.
- Christof Beierle, Bochum University, Germany, visiting PhD student, April-June 2017.
- Özgül Küçük, Bilgi University, Turkey, July-August 2017 (Bourse SSHN du Gouvernement Français).

9.4.1.1. Internships

- Sristy Agrawal, Kolkata, India, June-Aug. 2017
- Tim Beyne, Univ. Leuven, Belgium, Aug.-Sept. 2017
- Mathilde De La Morinerie, École Polytechnique, April-July 2017
- Matthieu Lequesne, MPRI, March-Aug. 2017
- André Schrottenloher, MPRI and Telecom ParisTech, March-Aug. 2017
- Ferdinand Sibleyras, MPRI, March-Aug. 2017
- Valentin Vasseur, Univ. Grenoble, March-Aug. 2017
- Matthieu Vieira, ENS Lyon, May-July 2017

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

- NTU, Singapore, October 16 - November 3, joint work within the CHOCOLAT Associate Team (G. Leurent).

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

- EuroS&P 2017: April 26-28, 2015, Paris (France): G. Leurent (poster chair);
- TQC 2017 (Theory of Quantum Computation, Communication and Cryptography): June 20-22, 2017, Paris (France): A. Chailloux, A. Leverrier.
- Dagstuhl Seminar 17401, "Quantum Cryptanalysis": October 1-6, 2017, Dagstuhl (Germany): N. Sendrier (co-organizer)
- Training School on Symmetric Cryptography and Blockchain: February 19-23, 2018, Torremolinos (Spain): A. Canteaut (co-organizer).

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

As a co-editor-in-chief of the journal *IACR Transactions on Symmetric Cryptology*, María Naya-Plasencia serves as a program chair of the conference *Fast Software Encryption (FSE)*, hold in Tokyo March 2017, and to be held in Bruges March 2018.

10.1.2.2. Member of the Conference Program Committees

- QIP 2017: January 16-20 2017, Seattle, USA (A. Chailloux, A. Leverrier);
- CT-RSA 2017: February 14-17, 2017, San Francisco, US (M. Naya-Plasencia);
- FSE 2017: March 5-8, 2017, Tokyo, Japan (A. Canteaut, G. Leurent, M. Naya-Plasencia);
- CryptoAction Symposium 2017: March 27-28, Amsterdam, the Netherlands (A. Canteaut);
- Financial Crypto 2017: April 3-7, 2017, Sliema, Malta (G. Leurent);
- Journées Codage et Cryptographie - C2 2017: April 23-28, La Bresse, France (G. Leurent);
- Eurocrypt 2017: 30 April- 4 May, 2017, Paris, France (M. Naya-Plasencia);
- Fq13: June 4-9, 2017, Gaeta, Italy (A. Canteaut);
- CEWQO 2017: June 26-30 2017, Lyngby, Denmark (A. Leverrier);
- PQCrypto 2017: 26-28 June, 2017, Utrecht, the Netherlands (M. Naya-Plasencia, N. Sendrier, J.P. Tillich)
- SAC 2017: August 16-18, 2017, Ottawa, Canada (G. Leurent, M. Naya-Plasencia);
- Crypto 2017: August 20-24, 2017, Santa Barbara, CA, USA (G. Leurent);
- AQIS 2017: September 4-8, 2017, Singapore (A. Chailloux);
- SCN 2018: September 5-7, 2018, Amalfi, Italy (G. Leurent);
- QCrypt 2017: 2017, September 18-22 2017, Cambridge, UK (A. Leverrier);
- WCC 2017: September 18-22, Saint-Petersburg, Russia (P. Charpin, J.-P. Tillich);
- FSE 2018: March 5-7, 2018, Bruges, Belgium (C. Boura, A. Canteaut, G. Leurent, M. Naya-Plasencia, L. Perrin);
- CryptoAction Symposium 2018: April 4-5, Sutomore, Montenegro (A. Canteaut);
- PQCrypto 2018: April 9-11, 2018, Fort Lauderdale, USA, (N. Sendrier, J.P. Tillich);

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- *Designs, Codes and Cryptography*, associate editor: P. Charpin.
- *Finite Fields and Applications*, associate editors: A. Canteaut, P. Charpin.
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut.
- *IACR Transactions on Symmetric Cryptology*, associate editors: C. Boura, A. Canteaut, G. Leurent, L. Perrin, co-editor-in-chief: M. Naya-Plasencia.
- *Annals of telecommunications*, associate editor: J.P. Tillich.
- *Advances in Mathematics for Communications*, associated editor : J.P. Tillich

10.1.3.2. Editor for books or special issues

- Special Issue on Coding and Cryptography, *Designs, Codes and Cryptography* : P. Charpin, T. Johansson, G. Kyureghyan, N. Sendrier and J.-P. Tillich, Eds., Volume 82, Issue 1-2, January 2017

10.1.3.3. Reviewer - Reviewing Activities

- Reviewer for Mathematical Reviews: P. Charpin.
- Reviewer for ERC proposals: G. Leurent

10.1.4. Invited Talks

- A. Leverrier, *Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction*, Trustworthy Quantum Information TyQi 2017, Paris, France, 19-21 June 2017.
- A. Leverrier, *Challenges in continuous-variable quantum cryptography*, QCRYPT 2017, Cambridge, UK, 18-22 September 2017.
- N. Sendrier, *Quantum Safe Cryptography from Codes: Present and Future*, 16th IMA International Conference on Cryptography and Coding, Oxford, UK, December 13, 2017.

The members of the project-team have also been invited to give talks to some workshops or international seminars, including:

- A. Canteaut, *Proving Resistance against Invariant Attacks: Properties of the Linear Layer* , Early Symmetric Crypto - ESC 2017, Canach, Luxembourg, January 2017
- A. Canteaut, *Proving resistance of a block cipher against invariant attacks*, BFA 2017 - Boolean Functions and their Applications, Os, Norway, July 2017.
- A. Chailloux, *A tight security reduction in the quantum random oracle model for code-based signature schemes*, IRIF Algocomp seminar, Paris, France, November 2017
- G. Leurent, *On the Practical (In-)Security of 64-bit Block Ciphers*, Early Symmetric Crypto - ESC 2017, Canach, Luxembourg, January 2017
- G. Leurent, *Breaking Symmetric Cryptosystems Using Quantum Algorithms*, Frontiers of Quantum Safe Cryptography - FOQUS, April 2017, Paris, France.
- G. Leurent, *Bad Symmetric Crypto in the Real World*, Journées Nationales 2017 Pré-GDR Sécurité Informatique, Paris, France, May 2017.
- A. Leverrier, *A Gaussian de Finetti theorem and application to truncations of random Haar matrices*, Workshop on "Probabilistic techniques and Quantum Information Theory", IHP, Paris, France, 23-27 October 2017.
- A. Leverrier, *Efficient decoding of random errors for quantum expander codes*, Conference on "Quantum Information Theory", IHP, Paris, France, 11-15 December 2017.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis* Dagstuhl seminar "Quantum Cryptanalysis", Dagstuhl, Germany, October 2017.
- N. Sendrier,*Code-based Cryptography*, PQCRYPTO Summer School on Post-Quantum Cryptography 2017, TU Eindhoven, June 2017. 5 hours.
- N. Sendrier,*Code-based Cryptography*, Executive School on Post-Quantum Cryptography 2017, TU Eindhoven, June 2017. 1 1/2 hours.
- J.P. Tillich *Décodage de codes LDPC quantiques*, Journées C2 La Bresse, April 27, 2017.
- J.P. Tillich *Code based cryptography and quantum attacks*, Dagstuhl seminar "Quantum Cryptanalysis", Dagstuhl, Germany, October 2017.
- J.P. Tillich *Recent advances in decoding quantum LDPC codes*, Recent advances in Quantum Computing, CEA Saclay, December 13, 2017.

10.1.5. Leadership within the Scientific Community

- A. Canteaut serves as a chair of the steering committee of *Fast Software Encryption (FSE)*.
- A. Canteaut serves on the steering committee of the international competition CAESAR for authenticated encryption [6].
- N. Sendrier serves on the steering committee of *Post-quantum cryptography (PQCrypto)*.
- N. Sendrier serves on the steering committee of the WCC conference series.
- N. Sendrier is a member of the "Comité de pilotage" of the ANR (défi 9).
- A. Leverrier serves on the steering committee of *DIM SIRTEQ* (réseau francilien pour les technologies quantiques).

10.1.6. Research Administration

- A. Canteaut serves as Head of Science of the Inria Paris research center since September 2017. She was deputy Head of Science from January to August 2017.
- A. Canteaut serves on the *Evaluation Committee* since September 2017.
- A. Canteaut was a member of the steering committee of the Fondation Sciences Mathématiques de Paris until June 2017.
- P. Charpin serves on the *Comité Parité* at Inria.
- M. Naya-Plasencia is a member of *Inria Paris CES Committee* (Comité de suivi doctoral).
- M. Naya-Plasencia is a member of *Inria Paris Scientific Hiring Committee* (Assignement of PhD, post-doctoral and delegation Inria fundings).
- M. Naya-Plasencia serves on the jury for PhD scholarships from EDITE.
- M. Naya-Plasencia serves on the *Comité des usagers du projet "rue Barrault"*.
- M. Naya-Plasencia serves on the *commission bureaux*.

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

- Inria Paris Chargés de recherche: M. Naya-Plasencia
- Inria Directeurs de recherche: A. Canteaut
- Université Pierre-et-Marie-Curie, professor: A. Canteaut
- Université de Rouen, assistant professor: C. Boura, M. Naya-Plasencia
- Université de Limoges, assistant professor: C. Boura, M. Naya-Plasencia
- ENSEA, assistant Professor: M. Naya-Plasencia
- DTU Denmark, associate professor: A. Canteaut.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: A. Canteaut, *Error-correcting codes and applications to cryptology*, 12 hours, M2, University Paris-Diderot (MPRI), France;

Master: A. Canteaut, *Symmetric crypography*, 6 hours M2, Ecole des Mines de Saint-Etienne, campus de Gardanne (ingénieurs Spécialité Microélectronique et Informatique), France, 2017.

Master: A. Chailloux, *Quantum Computing*, 9 hours, M2, University Paris-Diderot (MPRI), France;

Master: G. Leurent *Algorithmique et programmation*, 25 hours, M1, UVSQ, France;

Corps des Mines: G. Leurent *Cryptographie symétrique*, 9 hours, Telecom ParisTech, France;

Master: J.-P. Tillich, *Introduction to Information Theory*, 32 hours, M2, Ecole Polytechnique, France;

[6] https://competitions.cr.yp.to/caesar.html

10.2.2. Supervision

HdR : María Naya Plasencia, *Symmetric Cryptography for Long-Term Security*, University Pierre-et-Marie-Curie, May 5, 2017.

HdR : Anthony Leverrier, *Protecting information in a quantum world: from cryptography to error correction*, University Pierre-et-Marie-Curie, September 27, 2017.

PhD : Julia Chaulet, *Study of public-key cryptosystems based on MDPC quasi-cyclic codes*, University Pierre-et-Marie-Curie, March 20, 2017.

PhD : Kaushik Chakraborty, *Cryptography with spacetime constraints*, Université Pierre-et-Marie Curie, October 12, 2017.

PhD : Adrien Hauteville, *Nouveaux protocoles et nouvelles attaques pour la cryptologie basée sur les codes en métrique rang* , University of Limoges, December 4, 2017.

PhD in progress: Rodolfo Canto Torres, *Analysis of generic decoding algorithms for the Hamming metric and study of cryptosystems based on the rank metric*, since September 2015, supervisor: N. Sendrier

PhD in progress: Sébastien Duval, *Constructions for lightweight cryptography*, since October 2015, supervisor: A. Canteaut and G. Leurent

PhD in progress: Yann Rotella, *Finite fields and symmetric cryptography*, since October 2015, supervisor: A. Canteaut

PhD in progress: Xavier Bonnetain, *Cryptanalysis of symmetric primitives in the post-quantum world*, since September 2016, supervisor: M. Naya Plasencia

PhD in progress: Thomas Debris, *Quantum algorithms for decoding linear codes*, since September 2016, supervisor: J.-P. Tillich

PhD in progress: Antoine Grospellier, *LDPC codes: constructions and decoding*, since October 2016, supervisor: J.-P. Tillich

PhD in progress: Vivien Londe, *Study of quantum LDPC codes*, since September 2016, supervisors: G. Zémor and A. Leverrier

PhD in progress: Kevin Carrier, *Reconstruction of error-correcting codes*, since October 2016, supervisor: N. Sendrier

PhD in progress: Matthieu Lequesne, *Attaques par canaux cachés sur les cryptosystèmes à base de codes MDPC quasi-cycliques*, since September 2017, supervisor: N. Sendrier

PhD in progress: Ferdinand Sibleyras, *Security of modes of operation*, since October 2017, supervisor: G. Leurent and A. Canteaut

PhD in progress: Valentin Vasseur, *Etude du décodage des codes QC-MDPC*, since October 2017, supervisor: N. Sendrier

PhD in progress: Rémi Bricout, *Etude de scénarios non-locaux quantiques à l'aide d'outils de la théorie de l'information quantique*, since September 2017, supervisor: A. Chailloux and A. Leverrier

PhD in progress: Shouvik Ghorai, *Beyond-QKD continuous-variable quantum cryptographic protocols*, since October 2017, supervisors: E. Diamanti (UPMC), A. Leverrier

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

10.2.3. Juries

- C. Mavromati, *Cryptanalyse des algorithmes de type Even-Mansour*, University Paris-Saclay, January 24, 2017, committee: A. Canteaut (reviewer).

- J. Chaulet, *Study of public-key cryptosystems based on MDPC quasi-cyclic codes*, University Pierre-et-Marie-Curie, March 20, 2017, committee: N. Sendrier (supervisor), JP Tillich.
- R. do Canto de Loura, *Quantum measures, noise and measurement errors in a quantum bit commitment protocol*, Universidade de Lisboa, Instituto Superior Tecnico, March 31, 2017, committee: A. Leverrier (reviewer).
- M. Naya-Plasencia, *Symmetric Cryptography for Long-Term Security*, Habilitation, University Pierre-et-Marie-Curie, May 5, 2017, committee: A. Canteaut.
- H. Kalachi, *Sécurité de Protocoles Cryptographiques Fondés sur la Théorie des Codes Correcteurs d'Erreurs*, July 5, 2017, University of Rouen, committee: J.P. Tillich;
- B. Dravie, *Synchronisation et systèmes dynamiques, application à la cryptographie*, University of Lorraine, July 6, 2017, committee: A. Canteaut (reviewer).
- V. Dragoi, *Approche algébrique pour l'étude et la résolution de problèmes algorithmiques issus de la cryptographie et de la théorie des codes*, July 6, 2017, University of Rouen, committee: N. Sendrier (reviewer), J.P. Tillich;
- V. Migliore, *Cybersécurité matérielle et conception de composants dédiés au calcul homomorphe*, Université de Bretagne Sud, September 26, 2017. committee: N. Sendrier (reviewer);
- A. Leverrier, *Protecting information in a quantum world: from cryptography to error correction*, Habilitation, University Pierre-et-Marie-Curie, September 27, 2017, committee: J.P. Tillich;
- A. Bannier, *Combinatorial analysis of block ciphers with trapdoor*, Arts et Métiers ParisTech, September 29, 2017, committee: A. Canteaut;
- K. Chakraborty, *Cryptography with spacetime constraints*, Université Pierre-et-Marie Curie, October 12, 2017, committee: A. Leverrier (supervisor), J.P. Tillich (supervisor);
- A. Hauteville, *Nouveaux protocoles et nouvelles attaques pour la cryptologie basée sur les codes en métrique rang* , University of Limoges, December 4, 2017, committee: N. Sendrier, J.P. Tillich (supervisor);
- D. Mirandola, *On products of linear error correcting codes*, Leiden University, the Netherlands, and Univ. de Bordeaux, December 6, 2017, committee: A. Canteaut (reviewer, chair).
- G. Spini, *Unconditionally secure cryptographic protocols from coding-theoretic primitives*, Leiden University, the Netherlands, and Univ. de Bordeaux, December 6, 2017, committee: A. Canteaut (chair).
- P. Méaux, *Chiffrement complètement homomorphe hybride*, Research University PSL, December 8, 2017, committee: A. Canteaut (reviewer);
- M. Saad Taha. *Algebraic Approach for Code Equivalence*, Université de Rouen, December 18, 2017. committee: N. Sendrier (reviewer), J.P. Tillich;

10.3. Popularization

- **Alkindi cipher challenge:** Several members of the project-team are involved in the cipher challenge for high-school students "concours Alkindi" http://www.concours-alkindi.fr/. Matthieu Lequesne organized the challenge and created the scientific content of the competition. He also gave a talk during the final of the cipher challege Alkindi on May 17 at the "Cité des Sciences" in Paris. The 2018 edition of the competition has been launched in December 2017 at Lycée de la Vallée de Chevreuse, Gif-sur-Yvette. Matthieu Lequesne, Sébastien Duval and Yann Rotella gave talks on cryptography during the opening ceremony. The best teams from Académies de Dijon and Orléans-Tours have been visiting the SECRET project-team in June 2017 https://www.youtube.com/watch?v=EVLHEOWAORc.
- N. Sendrier, *Code-Based Cryptography: State of the Art and Perspectives*, IEEE Security & Privacy, Special Issue on Post-quantum Cryptography. July/August 2017.

- A. Chailloux *Cryptographie Quantique en théorie* - Journée Maths en Mouvement sur l'ordinateur quantique organized by the FSMP, Paris, France, May 2017
- Matthieu Lequesne co-organized the final of the French Tournament of Young Mathematicians at École polytechnique on May 26-28 and was chaired the jury sessions. He also participated to the elaboration of the problems for the 8th French Tournament of Young Mathematicians (TFJM^2) in December 2017.
- Matthieu Lequesne co-organized the International Tournament of Young Mathematicians (ITYM) in Iasi, Romania in July 2017 and was part of the international jury.
- Matthieu Lequesne taught for one week during a mathematical summer camp for high school students in Bethlehem, Palestine, organized by the Al Khwarizmi Noether Institute in August 2017.
- Matthieu Lequesne co-organized a weekend for female high-school students interested in mathematics (Rendez-vous des Jeunes Mathématiciennes) at ENS Ulm, November 25-26.
- Yann Rotella gave a talk on cryptography at Lycée Théophile Gautier, Tarbes, January 31, 2017.
- Yann Rotella gave a presentation for *Raconte-moi ta thèse !* during Fete de la Science, at IHP, Paris, October 2017.
- Several members of the team (C. Boura, A. Canteaut, M. Lequesne, A. Leverrier, Y. Rotella) have been involved in the *Cinquante ans d'Inria*, November 2017. They hold a stand to present a serious game on cryptography. A. Canteaut has participated on a panel on Cyber-security. A. Leverrier gave a short talk (pitch de science) on quantum computing.
- Matthieu Lequesne was auditioned by the committee in charge of proposing a reform of mathematical education (Mission Maths Villani-Torossian) on November 29.

11. Bibliography

Major publications by the team in recent years

[1] K. Bhargavan, G. Leurent. *On the Practical (In-)Security of 64-bit Block Ciphers*, in "ACM CCS 2016 - 23rd ACM Conference on Computer and Communications Security", Vienna, Austria, ACM, October 2016 [*DOI :* 10.1145/2976749.2978423], https://hal.inria.fr/hal-01404208

[2] A. Canteaut, B. Chevallier-Mames, A. Gouget, P. Paillier, T. Pornin, E. Bresson, C. Clavier, T. Fuhr, T. Icart, J.-F. Misarsky, M. Naya-Plasencia, J.-R. Reinhard, C. Thuillet, M. Videau. *Shabal, a Submission to NIST's Cryptographic Hash Algorithm Competition*, October 2008, Submission to NIST

[3] A. Canteaut, M. Naya-Plasencia, B. Vayssière. *Sieve-in-the-Middle: Improved MITM Attacks*, in "Advances in Cryptology - CRYPTO 2013, Part I", Lecture Notes in Computer Science, Springer, 2013, vol. 8042, pp. 222–240

[4] A. Canteaut, J. Roué. *On the behaviors of affine equivalent Sboxes regarding differential and linear attacks*, in "Advances in Cryptology - Eurocrypt 2015", Sofia, Bulgaria, Lecture Notes in Computer Science, Springer, April 2015, https://hal.inria.fr/hal-01104051

[5] K. Chakraborty, A. Chailloux, A. Leverrier. *Arbitrarily long relativistic bit commitment* , in "Physical Review Letters", 2015 [*DOI :* 10.1103/PhysRevLett.115.250501], https://hal.inria.fr/hal-01237241

[6] P. Charpin, G. M. Kyureghyan, V. Suder. *Sparse Permutations with Low Differential Uniformity*, in "Finite Fields and Their Applications", March 2014, vol. 28, pp. 214-243 [*DOI :* 10.1016/j.ffa.2014.02.003], https://hal.archives-ouvertes.fr/hal-01068860

[7] N. Courtois, M. Finiasz, N. Sendrier. *How to achieve a McEliece-based Digital Signature Scheme*, in "Advances in Cryptology - Asiacrypt 2001", LNCS, Springer-Verlag, 2001, n^{o} 2248, pp. 157–174

[8] J.-C. Faugère, A. Otmani, L. Perret, J.-P. Tillich. *Algebraic Cryptanalysis of McEliece Variants with Compact Keys*, in "Advances in Cryptology - EUROCRYPT 2010", LNCS, Springer, 2010, n^{o} 6110, pp. 279-298, http://dx.doi.org/10.1007/978-3-642-13190-5_14

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

[10] R. Misoczki, J.-P. Tillich, N. Sendrier, 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, https://hal.inria.fr/hal-00870929

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] K. Chakraborty. *Cryptography with Spacetime Constraints*, Université Pierre et Marie Curie - Paris VI, October 2017, https://hal.inria.fr/tel-01637818

[12] J. Chaulet. *Study of public key cryptosystems based on quasi-cyclic MDPC codes*, Université Pierre et Marie Curie - Paris VI, March 2017, https://tel.archives-ouvertes.fr/tel-01599347

[13] A. Leverrier. *Protecting information in a quantum world: from cryptography to error correction*, Université Pierre et Marie Curie - Paris VI, September 2017, Habilitation à diriger des recherches, https://hal.inria.fr/tel-01636624

[14] M. Naya-Plasencia. *Symmetric Cryptography for Long-Term Security*, Université Pierre et Marie Curie - Paris VI, May 2017, Habilitation à diriger des recherches, https://hal.inria.fr/tel-01656036

Articles in International Peer-Reviewed Journals

[15] C. Boura, A. Canteaut, L. R. Knudsen, G. Leander. *Reflection ciphers*, in "Designs, Codes and Cryptography", January 2017, vol. 82, n^{o} 1–2, pp. 3–25 [*DOI :* 10.1007/s10623-015-0143-x], https://hal.inria.fr/hal-01237135

[16] R. Bricout, A. Chailloux. *Recursive cheating strategies for the relativistic $\mathbb{F}_Q$ bit commitment protocol*, in "MDPI - Cryptography", August 2017, https://arxiv.org/abs/1608.03820 [*DOI :* 10.3390/cryptography1020014], https://hal.inria.fr/hal-01409563

[17] A. CANTEAUT, S. CARPOV, C. FONTAINE, T. LEPOINT, M. NAYA-PLASENCIA, P. PAILLIER, R. SIRDEY. *Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression*, in "Journal of Cryptology", 2017, forthcoming, https://hal.inria.fr/hal-01650012

[18] A. CANTEAUT, S. DUVAL, L. PERRIN. *A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size* 2^{4k+2}, in "IEEE Transactions on Information Theory", 2017, vol. 63, n^{o} 11, pp. 7575–7591 [*DOI :* 10.1109/TIT.2017.2676807], https://hal.inria.fr/hal-01589131

[19] A. CANTEAUT, E. LAMBOOIJ, S. NEVES, S. RASOOLZADEH, Y. SASAKI, M. STEVENS. *Refined Probability of Differential Characteristics Including Dependency Between Multiple Rounds*, in "IACR Transactions on Symmetric Cryptology", May 2017, vol. 2017, n^{o} 2, pp. 203–227 [*DOI :* 10.13154/TOSC.V2017.I2.203-227], https://hal.inria.fr/hal-01649954

[20] C. CARLET, P. MÉAUX, Y. ROTELLA. *Boolean functions with restricted input and their robustness; application to the FLIP cipher*, in "IACR Transactions on Symmetric Cryptology", 2017, vol. 2017, n^{o} 3, pp. 192–227 [*DOI :* 10.13154/TOSC.V2017.I3.192-227], https://hal.inria.fr/hal-01633506

[21] N. CEPAK, P. CHARPIN, E. PASALIC. *Permutations via linear translators*, in "Finite Fields and Their Applications", 2017, vol. 45, pp. 19–42, https://arxiv.org/abs/1609.09291 [*DOI :* 10.1016/J.FFA.2016.11.009], https://hal.inria.fr/hal-01412487

[22] A. CHAILLOUX, I. KERENIDIS. *Physical Limitations of Quantum Cryptographic Primitives or Optimal Bounds for Quantum Coin Flipping and Bit Commitment*, in "SIAM Journal on Computing", January 2017, vol. 46, n^{o} 5, pp. 1647–1677 [*DOI :* 10.1137/15M1010853], https://hal.inria.fr/hal-01650970

[23] P. CHARPIN, G. M. KYUREGHYAN. *On sets determining the differential spectrum of mappings*, in "International journal of information and Coding Theory", 2017, vol. 4, n^{o} 2/3, pp. 170–184, Special issue on the honor of Gerard Cohen [*DOI :* 10.1504/IJICOT.2017.083844], https://hal.inria.fr/hal-01406589

[24] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions*, in "IEEE Transactions on Information Theory", January 2017, vol. 63, n^{o} 1, pp. 404–427 [*DOI :* 10.1109/TIT.2016.2574841], https://hal.inria.fr/hal-01661935

[25] I. DINUR, G. LEURENT. *Improved Generic Attacks Against Hash-Based MACs and HAIFA*, in "Algorithmica", December 2017, vol. 79, n^{o} 4, pp. 1161–1195 [*DOI :* 10.1007/S00453-016-0236-6], https://hal.inria.fr/hal-01407953

[26] A. LEVERRIER. *Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction*, in "Physical Review Letters", May 2017, vol. 118, n^{o} 20, pp. 1–24, https://arxiv.org/abs/1701.03393 [*DOI :* 10.1103/PHYSREVLETT.118.200501], https://hal.inria.fr/hal-01652082

[27] M. TOMAMICHEL, A. LEVERRIER. *A largely self-contained and complete security proof for quantum key distribution*, in "Quantum", 2017, vol. 1, 14 p. , https://arxiv.org/abs/1506.08458 [*DOI :* 10.22331/Q-2017-07-14-14], https://hal.inria.fr/hal-01237240

Invited Conferences

[28] C. Beierle, A. Canteaut, G. Leander, Y. Rotella. *Proving Resistance against Invariant Attacks: Properties of the Linear Layer* , in "ESC 2017 - Early Symmetric Crypto", Canach, Luxembourg, January 2017, https://hal.inria.fr/hal-01649994

[29] C. Beierle, A. Canteaut, G. Leander, Y. Rotella. *Proving resistance of a block cipher against invariant attacks*, in "BFA 2017 - Boolean Functions and their Applications", Os, Norway, July 2017, https://hal.inria.fr/hal-01649990

[30] A. Chailloux. *A tight security reduction in the quantum random oracle model for code-based signature schemes*, in "2017 - IRIF Algocomp seminar", Paris, France, November 2017, https://hal.inria.fr/hal-01660701

[31] G. Leurent, K. Bhargavan. *On the Practical (In-)Security of 64-bit Block Ciphers*, in "ESC 2017 - Early Symmetric Crypto", Canach, Luxembourg, January 2017, https://hal.inria.fr/hal-01105128

[32] G. Leurent. *Bad Symmetric Crypto in the Real World*, in "Journées Nationales 2017 Pré-GDR Sécurité Informatique", Paris, France, May 2017, https://hal.inria.fr/hal-01652853

[33] G. Leurent. *Breaking Symmetric Cryptosystems Using Quantum Algorithms*, in "FOQUS - Frontiers of Quantum Safe Cryptography", Paris, France, April 2017, https://hal.inria.fr/hal-01652852

[34] A. Leverrier. *A Gaussian de Finetti theorem and application to truncations of random Haar matrices*, in "Workshop on ”Probabilistic techniques and Quantum Information Theory”", Paris, France, October 2017, pp. 1-60, https://hal.inria.fr/hal-01656425

[35] A. Leverrier. *Efficient decoding of random errors for quantum expander codes*, in "Conference on ”Quantum Information Theory”", Paris, France, December 2017, pp. 1-33, https://hal.inria.fr/hal-01656427

[36] A. Leverrier. *Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction*, in "TyQi 2017 - Trustworthy Quantum Information", Paris, France, June 2017, https://hal.inria.fr/hal-01656418

[37] A. Leverrier. *Theoretical challenges in continuous-variable quantum cryptography*, in "QCrypt 2017 - 7th International Conference on Quantum Cryptography", Cambridge, United Kingdom, September 2017, pp. 1-26, https://hal.inria.fr/hal-01656419

[38] M. Naya-Plasencia. *New results on symmetric quantum cryptanalysis*, in "Dagstuhl Seminar 17401 - Quantum Cryptanalysis", Dagstuhl, Germany, October 2017, https://hal.inria.fr/hal-01671913

[39] J.-P. Tillich. *Code based cryptography and quantum attacks*, in "Dagstuhl Seminar 17401 - Quantum cryptanalysis", Dagstuhl, Germany, October 2017, https://hal.archives-ouvertes.fr/hal-01671921

International Conferences with Proceedings

[40] P. S. L. M. Barreto, S. Gueron, T. Guneysu, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich. *CAKE: Code-based Algorithm for Key Encapsulation*, in "IMACC 2017 - 16th IMA International Conference on Cryptography and Coding", Oxford, United Kingdom, M. O'Neill (editor), LNCS - Lecture Notes in Computer Science, Springer, December 2017, vol. 10655, pp. 207–226 [*DOI :* 10.1007/978-3-319-71045-7_11], https://hal.inria.fr/hal-01661949

[41] C. BEIERLE, A. CANTEAUT, G. LEANDER, Y. ROTELLA. *Proving Resistance Against Invariant Attacks: How to Choose the Round Constants*, in "Crypto 2017 - Advances in Cryptology", Santa Barbara, United States, J. KATZ, H. SHACHAM (editors), LNCS - Lecture Notes in Computer Science, Springer, August 2017, vol. 10402, pp. 647–678 [*DOI :* 10.1007/978-3-319-63715-0_22], https://hal.inria.fr/hal-01631130

[42] A. BIRYUKOV, L. PERRIN. *Symmetrically and Asymmetrically Hard Cryptography*, in "Asiacrypt 2017 - Advances in Cryptology", Hong Kong, China, T. TAKAGI, T. PEYRIN (editors), LNCS - Lecture Notes in Computer Science, Springer, December 2017, vol. 10626, pp. 417–445 [*DOI :* 10.1007/978-3-319-70700-6_15], https://hal.inria.fr/hal-01650044

[43] O. BLAZY, P. GABORIT, J. SCHREK, N. SENDRIER. *A code-based blind signature*, in "ISIT 2017 - IEEE International Symposium on Information Theory", Aachen, Germany, IEEE, June 2017, pp. 2718–2722 [*DOI :* 10.1109/ISIT.2017.8007023], https://hal.archives-ouvertes.fr/hal-01610410

[44] X. BONNETAIN. *Quantum Key-Recovery on full AEZ*, in "SAC 2017 - Selected Areas in Cryptography", Ottawa, Canada, August 2017, https://hal.inria.fr/hal-01650026

[45] C. BOURA, A. CANTEAUT, J. JEAN, V. SUDER. *Two Notions of Differential Equivalence on Sboxes*, in "WCC 2017 - Workshop on Coding and Cryptography", Saint Petersburg, Russia, September 2017, https://hal.inria.fr/hal-01650010

[46] A. CHAILLOUX, A. LEVERRIER. *Relativistic (or 2-Prover 1-Round) Zero-Knowledge Protocol for NP Secure Against Quantum Adversaries*, in "Eurocrypt 2017 - Advances in Cryptology", Paris, France, J.-S. CORON, J. B. NIELSEN (editors), LNCS - Lecture Notes in Computer Science, Springer, April 2017, vol. 10212, pp. 369–396 [*DOI :* 10.1007/978-3-319-56617-7_13], https://hal.inria.fr/hal-01650985

[47] A. CHAILLOUX, M. NAYA-PLASENCIA, A. SCHROTTENLOHER. *An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography*, in "Asiacrypt 2017 - Advances in Cryptology", Hong Kong, China, T. TAKAGI, T. PEYRIN (editors), LNCS - Lecture Notes in Computer Science, Springer, December 2017, vol. 10625, pp. 211–240 [*DOI :* 10.1007/978-3-319-70697-9_8], https://hal.inria.fr/hal-01651007

[48] T. DEBRIS-ALAZARD, J.-P. TILLICH. *Statistical Decoding*, in "ISIT 2017 - IEEE International Symposium on Information Theory", Aachen, Germany, IEEE, June 2017, pp. 1789–1802 [*DOI :* 10.1109/ISIT.2017.8006839], https://hal.inria.fr/hal-01661749

[49] P. GABORIT, A. HAUTEVILLE, D. H. PHAN, J.-P. TILLICH. *Identity-based Encryption from Codes with Rank Metric*, in "Crypto 2017 - Advances in Cryptology", Santa-Barbara, United States, J. KATZ, H. SHACHAM (editors), LNCS - Lecture Notes in Computer Science, Springer, August 2017, vol. 10403, pp. 194–224 [*DOI :* 10.1007/978-3-319-63697-9_7], https://hal.inria.fr/hal-01589463

[50] G. KACHIGAR, J.-P. TILLICH. *Quantum Information Set Decoding Algorithms*, in "PQCrypto 2017 - The Eighth International Conference on Post-Quantum Cryptography", Utrecht, Netherlands, T. LANGE, T. TAKAGI (editors), LNCS - Lecture Notes in Computer Science, Springer, June 2017, vol. 10346, pp. 69-89 [*DOI :* 10.1007/978-3-319-59879-6_5], https://hal.inria.fr/hal-01661905

[51] L. KHATI, N. MOUHA, D. VERGNAUD. *Full Disk Encryption: Bridging Theory and Practice*, in "CT-RSA 2017 - RSA Conference Cryptographers' Track", San Francisco, United States, H. HANDSCHUH (editor),

Lecture Notes in Computer Science, Springer, February 2017, vol. 10159, pp. 241–257 [*DOI :* 10.1007/978-3-319-52153-4_14], https://hal.inria.fr/hal-01403418

[52] B. LAC, A. CANTEAUT, J. J. A. FOURNIER, R. SIRDEY. *DFA on LS-Designs with a Practical Implementation on SCREAM*, in "COSADE 2017 - Constructive Side-Channel Analysis and Secure Design", Paris, France, S. GUILLEY (editor), LNCS - Lecture Notes in Computer Science, Springer, April 2017, vol. 10348, pp. 223–247 [*DOI :* 10.1007/978-3-319-64647-3_14], https://hal.inria.fr/hal-01649974

[53] I. MARQUEZ-CORBELLA, J.-P. TILLICH. *Attaining Capacity with iterated* $(U|U+V)$ *codes based on AG codes and Koetter-Vardy soft decoding*, in "ISIT 2017 - IEEE International Symposium on Information Theory", Aachen, Germany, IEEE, June 2017, pp. 6–10 [*DOI :* 10.1109/ISIT.2017.8006479], https://hal.inria.fr/hal-01661977

Conferences without Proceedings

[54] C. BEIERLE, A. CANTEAUT, G. LEANDER, Y. ROTELLA. *Attaques par invariant : comment s'en protéger?*, in "Journées codage et cryptographie 2017", La Bresse, France, April 2017, 1 p. , https://hal.inria.fr/hal-01633519

[55] A. CANTEAUT, S. DUVAL, L. PERRIN. *On a generalisation of Dillon's APN permutation*, in "Fq13 - Finite Fields and Applications", Gaeta, Italy, June 2017, https://hal.inria.fr/hal-01650001

[56] A. CHAILLOUX. *A tight security reduction in the quantum random oracle model for code-based signature schemes*, in "Code based crypto seminar", Paris, France, October 2017, pp. 1-22, https://hal.inria.fr/hal-01660693

[57] O. FAWZI, A. GROSPELLIER, A. LEVERRIER. *Efficient decoding of random errors for quantum expander codes*, in "QIP 2018 - 21th Annual Conference on Quantum Information Processing", Delft, Netherlands, QuTech, January 2018, pp. 1-31, https://arxiv.org/abs/1711.08351 - 31 pages, https://hal.archives-ouvertes.fr/hal-01654670

[58] A. GROSPELLIER, A. LEVERRIER, O. FAWZI. *Efficient decoding of random errors for quantum expander codes*, in "Journées Informatique Quantique 2017", Bordeaux, France, November 2017, https://hal.archives-ouvertes.fr/hal-01671491

[59] A. GROSPELLIER, A. LEVERRIER, O. FAWZI. *Quantum expander codes*, in "Journées codage et cryptographie 2017", La Bresse, France, April 2017, https://hal.archives-ouvertes.fr/hal-01671485

[60] G. LEURENT, M. KAPLAN, A. LEVERRIER, M. NAYA-PLASENCIA. *Quantum differential and linear cryptanalysis*, in "FSE 2017 - Fast Software Encryption", Tokyo, Japan, March 2017, https://hal.inria.fr/hal-01652807

[61] A. LEVERRIER. *SU(p,q) coherent states and Gaussian de Finetti theorems*, in "QIP 2017 - 20th Annual Conference on Quantum Information Processing", Seattle, United States, January 2017, pp. 1-24, https://hal.inria.fr/hal-01656414

[62] V. LONDE. *Golden codes: 4D hyperbolic regular quantum codes*, in "8th colloquium of the GDR IQFA - Ingénierie Quantique, des Aspects Fondamentaux aux Applications", Nice, France, November 2017, https://hal.inria.fr/hal-01671528

[63] V. LONDE. *Homological quantum error correcting codes and real projective space*, in "Journées Codage et Cryptographie 2017", La Bresse, France, April 2017, https://hal.inria.fr/hal-01671444

[64] V. LONDE. *4D hyperbolic regular quantum codes*, in "Journées Informatique Quantique 2017", Bordeaux, France, November 2017, https://hal.inria.fr/hal-01671456

[65] N. SENDRIER. *Quantum Safe Cryptography from Codes: Present and Future*, in "16th IMA International Conference on Cryptography and Coding", Oxford, United Kingdom, December 2017, https://hal.archives-ouvertes.fr/hal-01671452

Scientific Popularization

[66] A. CHAILLOUX. *Cryptographie Quantique en théorie*, in "2017 - 9ème Journée Mathématiques en Mouvement sur l'ordinateur quantique", Paris, France, FSMP, May 2017, https://hal.inria.fr/hal-01660726

Other Publications

[67] N. ARAGON, P. S. L. M. BARRETO, S. BETTAIEB, L. BIDOUX, O. BLAZY, J.-C. DENEUVILLE, P. GABORIT, S. GUERON, T. GUNEYSU, C. AGUILAR MELCHOR, R. MISOCZKI, E. PERSICHETTI, N. SENDRIER, J.-P. TILLICH, G. ZÉMOR. *BIKE: Bit Flipping Key Encapsulation*, December 2017, Submission to the NIST post quantum standardization process, https://hal.archives-ouvertes.fr/hal-01671903

[68] N. ARAGON, P. GABORIT, A. HAUTEVILLE, J.-P. TILLICH. *Improvement of Generic Attacks on the Rank Syndrome Decoding Problem*, October 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01618464

[69] M. BARDET, E. BARELLI, O. BLAZY, R. CANTO TORRES, A. COUVREUR, P. GABORIT, A. OTMANI, N. SENDRIER, J.-P. TILLICH. *BIG QUAKE BInary Goppa QUAsi–cyclic Key Encapsulation*, December 2017, submission to the NIST post quantum cryptography standardization process, https://hal.archives-ouvertes.fr/hal-01671866

[70] A. CHAILLOUX, T. DEBRIS-ALAZARD. *A tight security reduction in the quantum random oracle model for code-based signature schemes* , December 2017, working paper or preprint, https://hal.inria.fr/hal-01671870

[71] T. DEBRIS-ALAZARD, J.-P. TILLICH. *Statistical Decoding*, December 2017, working paper or preprint, https://hal.inria.fr/hal-01661745

[72] O. FAWZI, A. GROSPELLIER, A. LEVERRIER. *Efficient decoding of random errors for quantum expander codes*, December 2017, working paper or preprint, https://hal.inria.fr/hal-01671348

[73] O. FAWZI, A. GROSPELLIER, A. LEVERRIER. *Efficient decoding of random errors for quantum expander codes*, November 2017, 8th colloquium of the GDR IQFA - Ingénierie Quantique, des Aspects Fondamentaux aux Applications, Poster, https://hal.archives-ouvertes.fr/hal-01671496

[74] M. LEQUESNE. *Side Channel Key Recovery Attacks on QC-MDPC Codes*, MPRI, September 2017, pp. 1-22, https://hal.inria.fr/hal-01658381

[75] A. LEVERRIER. *$SU(p,q)$ coherent states and a Gaussian de Finetti theorem*, November 2017, working paper or preprint, https://hal.inria.fr/hal-01652084

[76] A. SCHROTTENLOHER. *Collision search and quantum symmetric cryptanalysis*, Université Paris-Saclay, September 2017, pp. 1-25, https://hal.inria.fr/hal-01654190

[77] F. SIBLEYRAS. *Cryptanalysis of the Counter mode of operation*, Paris 7, September 2017, https://hal.inria.fr/hal-01662040

[78] V. VASSEUR. *Cryptographie post-quantique : étude du décodage des codes QC-MDPC*, Université Grenoble-Alpes, September 2017, https://hal.inria.fr/hal-01664082

[79] M. DE LA MORINERIE. *Implémentation à seuil de boîtes S*, Ecole Polytechnique, July 2017, https://hal.inria.fr/hal-01672270