Activity Report 2018

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
B9.5.1. - Computer science
B9.5.2. - Mathematics
B9.10. - Privacy

1. Team, Visitors, External Collaborators

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 until Feb. 2018, Researcher from March 2018]
Anthony Leverrier [Inria, Researcher, HDR]
María Naya Plasencia [Inria, Senior 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, en délégation until Oct. 2018]

Post-Doctoral Fellow

Léo Perrin [Inria from Sept 2018, Fondation Sciences Mathématiques de Paris until Aug 2018]

PhD Students

Xavier Bonnetain [Sorbonne Université]
Rémi Bricout [Sorbonne Université]
Rodolfo Canto Torres [Inria, until Oct 2018]

Kevin Carrier [Ministère de la Défense]
Daniel Coggia [DGA, from Sep 2018]
Thomas Debris [Sorbonne Université]
Sébastien Duval [Sorbonne Université, until Sep 2018]
Shouvik Ghorai [Sorbonne Université]
Antoine Grospellier [Sorbonne Université]
Matthieu Lequesne [Sorbonne Université]
Vivien Londe [Univ de Bordeaux]
Andrea Olivo [Inria]
Yann Rotella [Inria, until Sep 2018]
André Schrottenloher [Inria, from Feb 2018]
Ferdinand Sibleyras [Inria]
Valentin Vasseur [Univ René Descartes]

Interns

Daniel Coggia [DGA, from Mar 2018 until Aug 2018]
Mariem Hammami [Inria, from Jul 2018 until Oct 2018]
Anirudh Krishna [Univ. Sherbroke, Canada, until Mar 2018, MITACS]
Anais Querol Cruz [Inria, from Mar 2018 until Aug 2018]
Florian Wartelle [Inria, from Mar 2018 until Sep 2018]

Administrative Assistant

Christelle Guiziou [Inria]

Visiting Scientists

Thomas Peyrin [NTU, Singapore, January and July 2018]
Shizhu Tian [Univ. Chinese Academy of Sciences, from Sep 2018]

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.

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.

[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] P. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, FOCS 1994.
[4] http://csrc.nist.gov/groups/ST/post-quantum-crypto/

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:

- 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;
- 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 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

- **Keynote at Eurocrypt:** A. Canteaut bas been an invited keynote speaker at Eurocrypt 2018 in Tel-Aviv.

- **Cryptanalysis of candidates to the NIST post-quantum competition:** The members of the project-team are involved in the design of several attacks against submissions to the NIST standardization effort for post-quantum cryptography. This work has led to the break of `EDON-K` key encapsulation mechanism, of `RLCE` encryption scheme, of `RankSign`, and of a recently proposed IBE scheme.
- **Quantum fault-tolerance with constant overhead:** In a couple of papers published at STOC 2018 and FOCS 2018, A. Grospellier and A. Leverrier together with O. Fawzi (from ENS Lyon) proved that quantum expander codes can be combined with quantum fault-tolerance techniques to achieve constant overhead: the ratio between the total number of physical qubits required for a quantum computation with faulty hardware and the number of logical qubits involved in the ideal computation is asymptotically constant, and can even be taken arbitrarily close to 1 in the limit of small physical error rate. This improves on the polylogarithmic overhead promised by the celebrated threshold theorem.

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, Daniel Coggia, Sébastien Duval, Gaëtan Leurent, María Naya Plasencia, Léo Perrin, Yann Rotella, André Schrottenloher, Ferdinand Sibleyras.

7.1.1. Block ciphers

Our recent results mainly concern either the analysis or the design of lightweight block ciphers.
Recent results:

- Nonlinear approximations of block ciphers: A. Canteaut, together with C. Beierle and G. Leander have exhibited the relationship between nonlinear invariants for block ciphers and nonlinear approximations. They have shown that, in some cases, the linear hull effect may be formalized in terms of nonlinear invariants. They have also introduced a new framework to study the probability of nonlinear approximations over iterated block ciphers [13], [26]
- Impossible differential cryptanalysis: C. Boura, V. Lallemand and M. Naya-Plasencia have introduced new techniques and complexity analyses for impossible differential cryptanalysis. They also showed that the technique of multiple differentials can be applied to impossible differential attacks [16]
- Construction of lightweight MDS matrices: S. Duval and G. Leurent have exhibited MDS matrices with the lowest known implementation cost. They have been constructed by a search through a space of circuits yielding MDS matrices [20], [11]

7.1.2. Stream ciphers

Stream ciphers provide an alternative to block-cipher-based encryption schemes. They are especially well-suited in applications which require either extremely fast encryption or a very low-cost hardware implementation.
Recent results:

- 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].
- Cryptanalysis of Goldreich pseudo-random generator: Goldreich's PRG is a theoretical construction which expands a short random string into a long pseudo-random string by applying a simple d-ary predicate to public random sized subsets of the bits of the seed. While the security of Goldreich's PRG has been thoroughly investigated, with a variety of results deriving provable security guarantees against classes of attacks in some parameter regimes and necessary criteria to be satisfied by the underlying predicate, little was known about its concrete security and efficiency. Motivated by the hope of getting practical instantiations of this construction, Y. Rotella and his co-authors initiated a study of the concrete security of Goldreich's PRG, and evaluated its resistance to cryptanalytic attacks. They developped a new guess-and-determine-style attack, and identified new criteria which captured the security guarantees [44].

7.1.3. Authenticated encryption

A limitation of all classical block ciphers is that they aim at protecting confidentiality only, while most applications need both encryption and authentication. These two functionalities are provided by using a block cipher like the AES together with an appropriate mode of operation. However, it appears that the most widely-used mode of operation for authenticated encryption, AES-GCM, is not very efficient for high-speed networks. Also, the security of the GCM mode completely collapses when an IV is reused. These severe drawbacks have then motivated an international competition named CAESAR, partly supported by the NIST, which has been launched in order to define some new authenticated encryption schemes [5]. The project-team is involved in a national cryptanalytic effort in this area led by the BRUTUS project funded by the ANR. In this context, the members of the project-team have obtained some cryptanalytic results on several candidates to the CAESAR competition.

Recent results:

- State-recovery attack on a simplified version of Ketje Jr. [21], [34]
- Cryptanalysis of Morus, one of the finalists of the CAESAR competition [42]

7.1.4. 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:

- 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 [15], [25]. 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.
- Boomerang Uniformity of Sboxes: The boomerang attack is a cryptanalysis technique against block ciphers which combines two differentials for the upper part and the lower part of the cipher. The Boomerang Connectivity Table (BCT) is a tool introduced by Cid *et al.* at Eurocrypt 2018 for analysing the dependency between these two differentials. C. Boura and A. Canteaut [14] have provided an in-depth analysis of BCT, by studying more closely differentially 4-uniform Sboxes. They have completely characterized the BCT of all differentially 4-uniform permutations of 4 bits and then study these objects for some cryptographically relevant families of Sboxes, as the inverse function and quadratic permutations. These two families are the first examples of differentially 4-uniform Sboxes optimal against boomerang attacks for an even number of variables, answering an open question raised by Cid *et al.*.
- CCZ equivalence of Sboxes: A. Canteaut and L. Perrin have characterized CCZ-equivalence as a property of the zeroes in the Walsh spectrum of an Sbox (or equivalently in their DDT). They used this framework to show how to efficiently upper bound the number of distinct EA-equivalence classes in a given CCZ-equivalence class. More importantly, they proved that CCZ-equivalence can be reduced to the association of EA-equivalence and an operation called twisting. They then revisited several results from the literature on CCZ-equivalence and showed how they can be interpreted in light of this new framework [18], [29]

[5] http://competitions.cr.yp.to/caesar.html

- Links between linear and differential properties of Sboxes: P. Charpin together with J. Peng has established new links between the differential uniformity and the nonlinearity of some Sboxes in the case of two-valued functions and quadratic functions. More precisely, they have exhibited a lower bound on the nonlinearity of monomial permutations depending on their differential uniformity, as well as an upper bound in the case of differentially two-valued functions [19], [55]
- Construction of building-blocks with resistance against fault-attacks at a low implementation overhead [50].

7.1.5. 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 provable security, and we know that their use is secure as long as the underlying primitive is secure, and we respect some limits on the amount of data processed. The analysis of generic attack helps us understand what happens when the hypotheses of the security proofs do not hold, or the corresponding limits are not respected. Comparing proofs and attacks also shows gaps where our analysis is incomplete, and when improved proof or attacks are required.
Recent results:

- Use of block ciphers operating on small blocks with the CTR mode [53]: the security proof of the CTR mode 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 less problematic than on CBC. However, G. Leurent and F. Sibleyras have exhibited concrete attacks against the CTR mode when processing close to $2^{n/2}$ blocks of data, and have shown that an attacker can actually extract as much information as in the case of CBC encryption.
- Generic attacks against some MAC constructions based on block ciphers [52]: G. Leurent and F. Sibleyras, together with M. Nandi, have studied the security of several recent MAC constructions with provable security beyond the birthday bound, namely `SUM-ECBC`, `PMAC+`, `3kf9`, `GCM-SIV2`, and some variants. They described a new cryptanalysis technique for double-block MACs and they showed how to build a forgery attack with query complexity $\mathcal{O}(2^{3n/4})$, proving that these schemes do not reach full security in the information-theoretic model. Surprisingly, their attack on `LightMAC+` invalidates a recent security proof by Naito. Moreover, they gave the first attack against `SUM-ECBC` and `GCM-SIV2`, with complexity below 2^n.

7.2. Code-based cryptography

Participants: Rodolfo Canto Torres, Thomas Debris, Matthieu Lequesne, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur.

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.

Our recent work on code-based cryptography has to be seen in the context of the recently launched NIST competition 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.

Our contributions in this area are two-fold and consist in:

- designing and analysis new code-based solutions;
- cryptanalyzing code-based schemes, especially candidates to the NIST competition.

7.2.1. Design of new code-based solutions

The members of the project-team have submitted several candidates to the NIST competition, including a key-exchange protocol based on quasi-cyclic MDPC codes [41]. Their recent work on MDPC codes is important in this context in order to carefully analyze the properties of this candidate.

Recent results:

- Thwarting the GJS attack: the decryption algorithm of the QC-MDPC cryptosystem is based on an iterative bit-flipping algorithm, which fails with a small probability. These failures have been exploited in 2016 by Guo, Johansson and Stankovski to perform a key-recovery attack. JP Tillich recently analyzed how this attack can be avoided by increasing the key size of the scheme. Most notably, he proved that, under a very reasonable assumption, the error probability after decoding decays almost exponentially with the code-length with just two iterations of bit-flipping. With an additional assumption, it even decays exponentially with an unbounded number of iterations, implying that in this case the increase of the key size equired for resisting to the GJS attack is only moderate [54].
- Design of a new KEM with IND-CCA2 security in a model considering decoding failures [46]: M. Lequesne, N. Sendrier and their co-authors explored the underlying causes of the GJS attack, how it can be improved and how it can be mitigated. They derived a new timing attack performing well even in cases which were more challenging to the GJS attack. They also showed how to construct a new KEM, called ParQ that can reduce the decryption failure rate to a level negligible in the security parameter. They formally proved the IND-CCA2 security of ParQ, in a model that considers decoding failures.
- Design of a new code-based signature scheme [81]: T. Debris, N. Sendrier and JP Tillich recently proposed a "hash-and-sign" code-based signature scheme called `Wave`, which uses a family of ternary generalized (U, U + V) codes. `Wave` achieves existential unforgeability under adaptive-chosen-message attacks in the random oracle model with a tight reduction to two assumptions from coding theory: one is a distinguishing problem that is related to the trapdoor inserted in the scheme, the other one is a multiple-target version of syndrome decoding. This scheme enjoys efficient signature and verification algorithms. For 128-bit security, signature are 8000-bit long and the public-key size is slightly smaller than one megabyte.

7.2.2. Cryptanalysis of code-based schemes

Recent results:

- Cryptanalysis of two public-key cryptosystems based on the rank syndrome decoding problem [41]: JP Tillich and his co-authors proposed an attack on the Rank Syndrome Decoding problem which improves the previously best known algorithm for solving this problem. This attack breaks for some parameters some recently proposed cryptosystems based on LRPC codes or Gabidulin codes, including Loidreau's cryptosystem and the LRPC cryptosystem.
- Cryptanalysis of the NIST submission `RankSign` and of a recently proposed IBE scheme: T. Debris and JP Tillich have presented an algebraic attack against `RankSign` that exploits the fact that the augmented LRPC codes used in this scheme have codewords with a very low weight. This attack shows that all the parameters proposed for this candidate can be broken. They also proved that, for the IBE scheme based on `RankSign`, the problem is deeper than finding a new signature in rank-based cryptography, since they found an attack on the generic problem upon which the security reduction relies [45].

- Cryptanalysis of the EDON-K key encapsulation mechanism submitted to the NIST competition: EDON-K is a candidate to the NIST competition which is inspired by the McEliece scheme but uses another family of codes defined over $\mathbb{F}_{2^{128}}$ instead of $\mathbb{F}_2$ and is not based on the Hamming metric. M. Lequesne and JP Tillich presented an attack making the scheme insecure for the intended use. Indeed, recovering the error in the McEliece scheme corresponding to EDON-K can be viewed as a decoding problem for the rank-metric with a super-code of an LRPC code of very small rank A suitable parity-check matrix for this super-code can then be easily derived from the public key and used to recover the error [51].
- Attack against RLCE [80]: M. Lequesne and JP Tillich, together with A. Couvreur, recently presented a key-recovery attack against the Random Linear Code Encryption (RLCE) scheme recently submitted by Y. Wang to the NIST competition. This attack recovers the secret-key for all the short key-parameters proposed by the author. It uses a polynomial-time algorithm based on a square code distinguisher.

7.3. Quantum Information

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

Two PhD students within the project-team work on this topic. First, Antoine Grospellier, co-advised by A. Leverrier and O. Fawzi (Ens Lyon), studies efficient decoding algorithms for quantum LDPC codes. Beyond their intrinsic interest for channel-coding problems, such algorithms would be particularly relevant in the context of quantum fault-tolerance, since they would allow to considerably reduce the required overhead to obtain fault-tolerance in quantum computation. Vivien Londe is co-advised by A. Leverrier and G. Zémor (IMB) and his thesis is devoted to the design of better quantum LDPC codes: the main idea is to generalize the celebrated toric code of Kitaev by considering cellulations of manifolds in higher dimensions. A recent surprising result was that this approach leads to a much better behaviour than naively expected and a major challenge is to explore the mathematics behind this phenomenon in order to find even better constructions, or to uncover potential obstructions.

Recent results:

- Decoding algorithm for quantum expander codes [48], [47], [56] In this work, A. Grospellier, A. Leverrier and O. Fawzi analyze an efficient decoding algorithm for quantum expander codes and prove that it can correct a linear number of random errors with a negligible failure probability. 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.

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. The interest of continuous variables for quantum cryptography was recently recognized by being awarded a 10 M€ funding from the Quantum Flagship and SECRET will contribute to this project by studying the security of new key distribution protocols [88].

Recent results:

- Security proof for two-way continuous-variable quantum key distribution [22]: while many quantum key distribution protocols are one-way in the sense that quantum information is sent from one party to the other, it can be beneficial in terms of performance to consider two-way protocols where the quantum states perform a round-trip between the two parties. In this paper (to appear in *Physical Review A*), we show how to exploit the symmetries of the protocols in phase-space to establish their security against the most general attacks allowed by quantum theory.
- Investigating the optimality of ancilla-assisted linear optical Bell measurements [24]: Due to its experimental and theoretical simplicity, linear quantum optics has proved to be a promising route for the early implementation of important quantum communication protocols. A. Olivo and F. Grosshans study the efficiency of non ambiguous Bell measurements in this model and show both theoretical and numerical bounds depending on the number of ancilla qubits. This is important for understanding what resources are needed for building quantum repeaters, the last missing building block for secure long distance quantum key distribution networks.

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 commitment and zero-knowledge proofs [30]: A. Chailloux and A. Leverrier constructed 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. R. Bricout and A. Chailloux also studied relativistic multi-round bit commitment schemes. They showed optimal classical cheating strategies for the canonical F_Q commitment scheme.

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.

Recent results:

- Hidden-shift quantum cryptanalysis [43]: X. Bonnetain and M. Naya-Plasencia have obtained new results that consider the tweak proposed at Eurocrypt 2017 of using modular additions to counter Simon's attacks. They have developed new algorithms that improve and generalize Kuperberg's algorithm for the hidden shift problem. Thanks to their improved algorithm, they have been able to build a quantum attack in the superposition model on Poly1305, proposed at FSE 2005, largely used and claimed to be quantumly secure. They also analyzed the security of some classical symmetric constructions with concrete parameters, to evaluate the impact and practicality of the proposed tweak, concluding that it does not seem to be efficient
- Quantum algorithm for the k-XOR problem [49]: The k-XOR (or generalized birthday) problem aims at finding k elements of n-bits, drawn at random, such that the XOR of all of them is 0. The algorithms proposed by Wagner more than 15 years ago remain the best known classical algorithms for solving it, when disregarding logarithmic factors. M. Naya-Plasencia and A. Schrottenloher, together with L. Grassi, studied this problem in the quantum setting and provided algorithms with the best known quantum time-complexities. In particular, they were able to considerably improve the 3-XOR algorithm.
- Quantum cryptanalysis of CSIDH and Ordinary Isogeny-based Schemes [68]: CSIDH is a recent proposal by Castryck et al. for post-quantum non-interactive key-exchange. It is similar in design to a scheme by Couveignes, Rostovtsev and Stolbunov, but it replaces ordinary elliptic curves by supersingular elliptic curves. Although CSIDH uses supersingular curves, it can attacked by a quantum subexponential hidden shift algorithm due to Childs et al. While the designers of CSIDH claimed that the parameters they suggested ensures security against this algorithm, X. Bonnetain and A. Schrottenloher showed that these security parameters were too optimistic: they improved the hidden shift algorithm and gave a precise complexity analysis in this context, which greatly reduced the complexity. For example, they showed that only 2^{35} quantum equivalents of a key-exchange are sufficient to break the 128-bit classical, 64-bit quantum security parameters proposed, instead of 2^{62}. They also extended their analysis to ordinary isogeny computations, and showed that an instance proposed by De Feo, Kieffer and Smith and expected to offer 56 bits of quantum security can be broken in 2^{38} quantum evaluations of a key exchange.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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** ($10/17 \rightarrow 09/21$)
  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** ($10/17 \rightarrow 09/21$)
  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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. 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.

8.2.1.2. 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.

8.2.1.3. 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.

8.2.2. Collaborations in European Programs, Except FP7 & H2020

8.2.2.1. 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)

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.

8.3. International Initiatives

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

8.3.1.1. 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, nobody has publicly produced a real pair of colliding messages so far, because the estimated attack complexity is around 2^{63} SHA-1 computations (this represents about 70000 years of computation on a normal PC).

While a collision of SHA-1 would clearly demonstrate 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, and we will use an ASIC cluster to perform such a computation.

8.3.2. Inria International Partners

8.3.2.1. 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.

8.3.2.2. Informal International Partners

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

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Thomas Peyrin, NTU Singapore, January 2018 and July 2018.
- Sristy Agrawal, Indian Institute of Science Education and Research, Kolkata, India, January 2018.
- Anastasiya Gorodilova, Sobolev Institute of Mathematics, Novosibirsk, Russia, September 2018.
- Lorenzo Grassi, IAIK, Graz University of Technology, Austria, September 2018.

8.4.1.1. Internships

- Daniel Coggia, MPRI, March-Aug. 2018
- Anaïs Querol Cruz, MPRI, March-Aug. 2018
- Florian Wartelle, UVSQ, March-Sept. 2018

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

- NTU, Singapore, joint work within the CHOCOLAT Associate Team: S. Duval (April 8-19), G. Leurent (October 29 - November 10).
- University of Sherbrooke, Sherbrooke, Canada, June 11-15, 2018 (J.P. Tillich)
- Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, September 30-October 9, 2018 (P. Charpin).

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- WCC 2019, March 31 - April 5, 2019, St Jacut-de-la-Mer, France: A. Canteaut, program co-chair
- Eurocrypt 2020, Zagreb, Croatia: A. Canteaut, program co-chair
- Workshop on quantum code design and architectures (kick-off meeting of the European project QCDA), November 5-6, 2018, Paris (France): A. Leverrier.

9.1.1.2. Member of the Organizing Committees

- Training School on Symmetric Cryptography and Blockchain: February 19-23, 2018, Torremolinos (Spain): A. Canteaut.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

As a co-editor-in-chief of the journal *IACR Transactions on Symmetric Cryptology*, María Naya-Plasencia served as a program chair of the conference *Fast Software Encryption (FSE)*, held in Bruges March 2018. Gaëtan Leurent will serve as a co-editor-in-chief of *IACR Transactions on Symmetric Cryptology* starting from 2019.

9.1.2.2. Member of the Conference Program Committees

- 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, (M. Naya-Plasencia, N. Sendrier, J.P. Tillich);
- CT-RSA 2018: April 16-20, 2018, San Francisco, USA (M. Naya-Plasencia);
- Eurocrypt 2018: April 29- May 3, 2018, Tel Aviv, Israel (M. Naya-Plasencia);
- WAIFI 2018: June 14-16, 2018, Bergen, Norway, (L. Perrin)
- SAC 2018: August 13-14, 2018, Calgary, Canada, (G. Leurent);
- Crypto 2018: August 17-19, 2018, Santa Barbara, USA, (M. Naya-Plasencia);
- QCrypt 2018: August 27-31, 2018, Shanghai, China, (A. Leverrier);
- TQC 2018: July 16-18, 2018, Sydney, Australia, (A. Leverrier);
- QTech 2018: September 5-7, 2018, Paris, France, (A. Leverrier);
- SCN 2018: September 5-7, 2018, Amalfi, Italy, (G. Leurent);
- AQIS 2018: September 8-12, 2018, Nagoya, Japan, (A. Leverrier);
- SETA 2018: October 1-6, 2018, Hong-Kong, China, (P. Charpin);
- Asiacrypt 2018: December 02-06, 2018, Brisbane, Australia, (G. Leurent);
- CT-RSA 2019: March 4-8, 2019, San Francisco, USA, (L. Perrin)
- FSE 2019: March 25-28, 2019, Paris, France (C. Boura, A. Canteaut, G. Leurent, M. Naya-Plasencia)
- WCC 2019: March 31 - April 5, 2019, St Jacut-de-la-Mer, France, (A. Canteaut chair, P. Charpin, N. Sendrier, J.P. Tillich);
- PQCrypto 2019: May 8-10, 2019, Chongqing, China, (J.P. Tillich);
- CBC 2019: May 18-19, Darmstadt, Germany, (J.P. Tillich);
- Eurocrypt 2019: May 19-23, 2019, Darmstadt, Germany (C. Boura)
- ISIT 2019: July 7-12, 2019, Paris, France, (J.P. Tillich);
- CHES 2019: August 25-28, 2019, Atlanta, USA, (G. Leurent);
- Eurocrypt 2020: Zagreb, Croatia (A. Canteaut, PC co-chair).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- *Designs, Codes and Cryptography*, associate editor: P. Charpin.
- *Finite Fields and Applications*, associate editor: 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, M. Naya-Plasencia.
- *IACR Transactions on Cryptographic Hardware and Embedded Systems*, associate editors: G. Leurent.
- *Advances in Mathematics of Communications*, associate editors: N. Sendrier and J.P. Tillich

9.1.3.2. Reviewer - Reviewing Activities

- Remote Referee - step 2- ERC-2018-CoG (A. Canteaut)
- Remote Referee - step 2- ERC-2018-STG (M. Naya-Plasencia)

9.1.4. Invited Talks

- A. Canteaut, *Desperately Seeking Sboxes*, Eurocrypt 2018, Tel Aviv, Israel, April 29 - May 3 2018.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis*, QUANTALGO Quantum Algorithms and Applications Workshop, 2018, Paris, France, September 25 - 28, 2018.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis*, CrossFYRE Workshop, 2018, Surrey, UK, September 13 - 14, 2018.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis*, Journées Nationales 2018 du GDR Informatique Mathématique, Apr 2018, Palaiseau, France
- J.P. Tillich *Schémas cryptographiques à clé publique à base de codes correcteurs proposés à la compétition du NIST*, Journées Nationales 2018 du Pré-GDR Sécurité Informatique, June 1, 2018.

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

- C. Boura, A. Canteaut, J. Jean and V. Suder, *On Sboxes sharing the same DDT*, Dagstuhl Seminar 18021 Symmetric Cryptography, Jan 2018, Dagstuhl, Germany
- A. Canteaut *L'insoutenable légèreté du chiffrement*, Journées Scientifiques Inria 2018, June 2018, Bordeaux, France
- A. Canteaut and L. Perrin *On CCZ-Equivalence, Extended-Affine Equivalence and Function Twisting*, BFA 2018 - 3rd International Workshop on Boolean Functions and their Applications, Jun 2018, Loen, Norway
- A. Chailloux, *Relativistic commitment and zero-knowledge proofs*, 17th Bellairs Crypto-Workshop 2018, Mar 2018, Holetown, Barbados.
- T. Fuhr, M. Naya-Plasencia and Y. Rotella, *New Results on Modified Versions of Ketje Jr*, Dagstuhl Seminar 18021 Symmetric Cryptography, Jan 2018, Dagstuhl, Germany
- G. Leurent, *MDS Matrices with Lightweight Circuits*, The Challenges of Lightweight Cryptanalysis, April 2018, Tel Aviv, Israel.
- G. Leurent, *Security Issues with Small Block Sizes*, Lightweight Crypto Day, April 2018, Tel Aviv, Israel.
- G. Leurent *The Missing Difference Problem*, Flexible Symmetric Cryptography, March 2018, Leiden, Netherlands.
- M. Naya-Plasencia, *Quantum Safe Symmetric Cryptography*, Flexible Symmetric Cryptography Lorentz Center Workshop, 2018, Leiden, Netherlands, March 19 - 23, 2018.
- M. Naya-Plasencia, *Symmetric lightweight primitives: (Design and) Cryptanalysis*, Lightweight Crypto Day, April 2018, Tel Aviv, Israel.
- L. Perrin, *Generalized Feistel Networks with Optimal Diffusion*, Dagstuhl Seminar 18021 Symmetric Cryptography, Jan 2018, Dagstuhl, Germany
- L. Perrin, *S-Box Reverse-Engineering: Boolean Functions, American/Russian Standards, and Butterflies*, CECC 2018 - Central European Conference on Cryptology, Jun 2018, Smolenice, Slovakia.

9.1.5. 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)*.
- P. Charpin, N. Sendrier and JP Tillich serve on the steering committee of the WCC conference series.
- A. Leverrier serves on the steering committee of *DIM SIRTEQ* (réseau francilien pour les technologies quantiques).

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

9.1.6. Research Administration

- A. Canteaut serves as Head of Science of the Inria Paris research center since September 2017.
- A. Canteaut serves on the *Inria Evaluation Committee* since September 2017.
- M. Naya-Plasencia and G. Leurent are members of *Inria Paris CSD 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 as head of the jury for PhD scholarships from EDITE.
- M. Naya-Plasencia serves on the *Comité des usagers du projet "rue Barrault"*.

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

- Inria Paris Chargés de recherche: A. Canteaut (vice-chair)
- Inria Chargés de recherche (national selection): A. Canteaut
- ISTIC, Rennes, maître de conférence: M. Naya-Plasencia

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

Master: A. Chailloux, *Quantum Information*, 18 hours, M2, University Paris-Diderot (MPRI), France;

Master: A. Leverrier, *Quantum information and cryptography*, 18 hours, M2, University Paris-Diderot (MPRI), France;

Master: N. Sendrier, Information theory, 40 hours, M1, UVSQ, MINT, France;

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

Corps des Mines: G. Leurent *Cryptographie symétrique*, 7 hours, Telecom ParisTech, France;

The members of the project-team were also invited to give courses at training schools for PhD students and young researchers:

- A. Canteaut, *Secure building-blocks against differential and linear attacks*, Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, February 2018. 3 hours.
- A. Canteaut, *Exploiting algebraic properties of block ciphers*, Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, February 2018. 1.5 hours.
- G. Leurent *How Not to Use a Blockcipher*, Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, February 2018. 2.5 hours.
- A. Leverrier, *Security of continuous-variable quantum key distribution*, Secure Quantum Communications School, Baiona, Spain, May 2018.
- M. Naya-Plasencia, *Introduction to Symmetric Cryptography*, Summer School on real-world crypto and privacy, Sibenik, Croatia, June 2018.
- M. Naya-Plasencia, *Lightweight Cryptography*, Summer School on real-world crypto and privacy, Sibenik, Croatia, June 2018.

9.2.2. Supervision

PhD: Sébastien Duval, *Constructions for lightweight cryptography*, Sorbonne Université, October 3, 2018.

PhDs: Yann Rotella, *Finite fields and symmetric cryptography*, Sorbonne Université, September 19, 2018.

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: 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).

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

9.2.3. Juries

- Alex Bredariol Grilo, *Quantum proofs, the Local Hamiltonian problem and applications*; Université Sorbonne Paris Cité, Paris, April 27, 2018, committee: A. Leverrier.
- Vincent Zucca, *Towards efficient arithmetic for Ring-LWE based homomorphic encryption*, Sorbonne Université, June 25, 2018, committee: A. Canteaut (chair);
- Yann Rotella, *Mathématiques discrètes appliquées à la cryptographie symétrique*, Sorbonne Université, September 19, 2018, committee: A. Canteaut (supervisor), M. Naya-Plasencia
- Dahmun Goudarzi, *Secure implementation of block ciphers against physical attacks*, PSL, September 21, 2018, committee: A. Canteaut
- Sébastien Duval, *Constructions pour la cryptographie à bas coût*, Sorbonne Université, October 3, committee: C. Boura, A. Canteaut (supervisor), G. Leurent (supervisor)

- Benjamin Lac, *Cryptographie légère intrinsèquement résistante aux attaques physiques pour l'Internet des objets*, Ecole des Mines de St-Etienne, October 18, 2018, committee: A. Canteaut
- Michele Minelli, *Chiffrement Totalement Homomorphe pour l'Apprentissage Automatique*, Université Paris Sciences et Lettres, October 26, 2018, committee: M. Naya-Plasencia (chair)
- Claire Delaplace, *Algorithmes d'algèbre linéaire pour la cryptographie*, Université de Rennes, November 21, 2018, committee: M. Naya-Plasencia.
- David Gérault, *Security Analysis of Contactless Communication Protocols*, Université Clermont Auvergne, November 27, 2018, committee: M. Naya-Plasencia (reviewer).
- Colin Chaigneau, *Cryptanalyse des Algorithmes de Chiffrement Symétrique*, Université de Versailles, November 28, 2018, committee: M. Naya-Plasencia (reviewer).
- Victor Cauchois, *Couches de Diffusion Lineaires à Partir de Matrices MDS*, Université de Rennes, December 13, 2018, committee: M. Naya-Plasencia.
- Eloi de Chérisey, *Towards a better formalisation of the side-channel threat*, Telecom Paris, December 18, 2018, committee: A. Canteaut (chair).

9.3. Popularization

9.3.1. Internal or external Inria responsibilities

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

9.3.2. Articles and contents

- A.Chailloux, *L'algorithme de Shor*, Interstices, Inria, March 2018.
- G. Leurent and M. Naya-Plasencia, *La fragilité inattendue du chiffrement symétrique*, "La Recherche", November 2018.
- JP Tillich, *Les codes correcteurs*, "La Recherche", November 2018, p. 45-46.
- A. Canteaut, *La meilleure garantie de sécurité est l'épreuve du temps*, interview to the journal "La Recherche", November 2018.
- M. Naya-Plasencia, *Symmetric Cryptanalysis: The Foundation of Trust*, Lorentz Center Highlights, 2018, Leiden, Netherlands, Mars 20, 2018.

9.3.3. Education

- **Alkindi cipher challenge:** Several members of the project-team are involved in the cipher challenge for high-school students "concours Alkindi" http://www.concours-alkindi.fr/. Mathieu Lequesne serves as a co-organizer of the challenge, preparing the three rounds and the final. Together with C. Boura and A. Canteaut, he was also involved in the redaction of the exercises, and in videos for Inria channel on different aspects of cryptography and how to solve problems from the Alkindi challenge: https://www.youtube.com/watch?v=Y-VQBzwEaqQ&t=17s, https://www.youtube.com/watch?v=Mv415zfUFNs&t=3s and https://www.youtube.com/watch?v=8ohEeTPKBwA&t=21s. The best teams from Académie de Paris have been visiting the SECRET project-team in June 2018 https://www.youtube.com/watch?v=EVLHEOWAORc.
- Organization of the event "Rendez-vous des Jeunes Mathématiciennes et Informaticiennes" at Inria Paris (October 22-23) by M. Lequesne, a 2-days camp for 20 high-school girls interested in mathematics and computer science.

- Organization of the International Tournament of Young Mathematicians in Paris, a one-week competition (July 5-12) for 120 high-school students. M. Lequesne served as vice-president of the local organizing committee.

9.3.4. Interventions

- A. Canteaut gave a talk to high-school students at Palais de la Découverte, during the "Semaine des maths" (March 2018) [61];
- A. Canteaut gave the talk during the closing ceremony of "Olympiades nationales de mathématiques" (June 2018) [62];
- A. Canteaut gave a presentation on research in computer science to 10-year children in a school in Paris (Jan. 2018);
- M. Lequesne gave a presentation on code-based cryptography to high-school interns (stagiaires de 3e) (Dec. 2018).

10. Bibliography

Major publications by the team in recent years

[1] 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

[2] 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

[3] 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

[4] 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

[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] 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° 1, pp. 404–427 [*DOI :* 10.1109/TIT.2016.2574841], https://hal.inria.fr/hal-01661935

[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] S. DUVAL. *Constructions for Lightweight Cryptography*, Sorbonne Université , UPMC, October 2018, https://hal.inria.fr/tel-01900290

[12] Y. ROTELLA. *Discrete Mathematics for symmetric cryptography*, Sorbonne Université, September 2018, https://hal.inria.fr/tel-01944827

Articles in International Peer-Reviewed Journals

[13] C. BEIERLE, A. CANTEAUT, G. LEANDER. *Nonlinear Approximations in Cryptanalysis Revisited*, in "IACR Transactions on Symmetric Cryptology", December 2018, vol. 2018, n° 4, pp. 80-101 [*DOI :* 10.13154/TOSC.V2018.I4.80-101], https://hal.inria.fr/hal-01944995

[14] C. BOURA, A. CANTEAUT. *On the Boomerang Uniformity of Cryptographic Sboxes*, in "IACR Transactions on Symmetric Cryptology", September 2018, vol. 2018, n° 3, pp. 290-310 [*DOI :* 10.13154/TOSC.V2018.I3.290-310], https://hal.inria.fr/hal-01944598

[15] C. BOURA, A. CANTEAUT, J. JEAN, V. SUDER. *Two Notions of Differential Equivalence on Sboxes*, in "Designs, Codes and Cryptography", 2018 [*DOI :* 10.1007/S10623-018-0496-Z], https://hal.inria.fr/hal-01944565

[16] C. BOURA, V. LALLEMAND, V. SUDER, M. NAYA-PLASENCIA. *Making the Impossible Possible*, in "Journal of Cryptology", January 2018, vol. 31, n° 1, pp. 101-133 [*DOI :* 10.1007/S00145-016-9251-7], https://hal.inria.fr/hal-01953916

[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", July 2018, vol. 31, n° 3, pp. 885-916 [*DOI :* 10.1007/S00145-017-9273-9], https://hal.inria.fr/hal-01650012

[18] A. CANTEAUT, L. PERRIN. *On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting*, in "Finite Fields and Their Applications", March 2019, vol. 56, pp. 209-246 [*DOI :* 10.1016/J.FFA.2018.11.008], https://hal.inria.fr/hal-01953353

[19] P. CHARPIN, J. PENG. *New links between nonlinearity and differential uniformity*, in "Finite Fields and Their Applications", March 2019, vol. 56, pp. 188-208 [*DOI :* 10.1016/J.FFA.2018.12.001], https://hal.inria.fr/hal-01907499

[20] S. DUVAL, G. LEURENT. *MDS Matrices with Lightweight Circuits*, in "IACR Transactions on Symmetric Cryptology", June 2018 [*DOI :* 10.13154/TOSC.V2018.I2.48-78], https://hal.inria.fr/hal-01944495

[21] T. FUHR, M. NAYA-PLASENCIA, Y. ROTELLA. *State-Recovery Attacks on modified Ketje Jr*, in "IACR Transactions on Symmetric Cryptology", March 2018, vol. 2018, n^{o} 1, pp. 29-56 [*DOI :* 10.13154/TOSC.V2018.I1.29-56], https://hal.inria.fr/hal-01944785

[22] S. GHORAI, E. DIAMANTI, A. LEVERRIER. *Composable security of two-way continuous-variable quantum key distribution without active symmetrization*, in "Physical Review A", 2019, https://arxiv.org/abs/1806.11356 [*DOI :* 10.1103/PHYSREVA.99.012311], https://hal.inria.fr/hal-01951932

[23] A. LEVERRIER. *$SU(p,q)$ coherent states and a Gaussian de Finetti theorem*, in "Journal of Mathematical Physics", 2018, vol. 59, 042202 p. , https://arxiv.org/abs/1612.05080 [*DOI :* 10.1063/1.5007334], https://hal.inria.fr/hal-01652084

[24] A. OLIVO, F. GROSSHANS. *Ancilla-assisted linear optical Bell measurements and their optimality*, in "Physical Review A", October 2018, vol. 98, n^{o} 4, 042323 p. [*DOI :* 10.1103/PHYSREVA.98.042323], https://hal.inria.fr/hal-01951361

Invited Conferences

[25] C. BOURA, A. CANTEAUT, J. JEAN, V. SUDER. *On Sboxes sharing the same DDT*, in "Dagstuhl Seminar 18021 Symmetric Cryptography", Dagstuhl, Germany, January 2018 [*DOI :* 10.4230/DAGREP.8.1.1], https://hal.inria.fr/hal-01955256

[26] A. CANTEAUT, C. BEIERLE, G. LEANDER. *On nonlinear approximations and the linear hull effect*, in "ASK 2018 - 8th Asian Workshop on Symmetric Key Cryptography", Kolkata, India, November 2018, https://hal.inria.fr/hal-01955286

[27] A. CANTEAUT. *Desperately Seeking Sboxes*, in "Eurocrypt 2018", Tel Aviv, Israel, April 2018, https://hal.inria.fr/hal-01944401

[28] A. CANTEAUT. *L'insoutenable légèreté du chiffrement*, in "Journées Scientifiques Inria 2018", Bordeaux, France, June 2018, https://hal.inria.fr/hal-01955337

[29] A. CANTEAUT, L. PERRIN. *On CCZ-Equivalence, Extended-Affine Equivalence and Function Twisting*, in "BFA 2018 - 3rd International Workshop on Boolean Functions and their Applications", Loen, Norway, June 2018, https://hal.inria.fr/hal-01953349

[30] A. CHAILLOUX. *Relativistic commitment and zero-knowledge proofs*, in "Seventeenth Bellairs Crypto-Workshop 2018", Holetown, Barbados, March 2018, https://hal.inria.fr/hal-01950643

[31] G. LEURENT. *MDS Matrices with Lightweight Circuits*, in "The Challenges of Lightweight Cryptanalysis", Tel Aviv, Israel, April 2018, https://hal.inria.fr/hal-01953383

[32] G. LEURENT. *Security Issues with Small Block Sizes*, in "Lightweight Crypto Day 2018", Tel Aviv, Israel, April 2018, https://hal.inria.fr/hal-01966550

[33] A. LEVERRIER. *Introduction to quantum computing*, in "Lecture series on Quantum Engineering at University Paris-Saclay", Palaiseau, France, May 2018, https://hal.inria.fr/hal-01955373

[34] M. NAYA-PLASENCIA, T. FUHR, Y. ROTELLA. *New Results on Modified Versions of Ketje Jr*, in "Dagstuhl Seminar 18021 Symmetric Cryptography", Dagstuhl, Germany, January 2018 [*DOI :* 10.4230/DAGREP.8.1.1], https://hal.archives-ouvertes.fr/hal-01953975

[35] M. NAYA-PLASENCIA. *New Results on Quantum Symmetric Cryptanalysis*, in "Journées Nationales 2018 du GDR Informatique Mathématique", Palaiseau, France, April 2018, https://hal.inria.fr/hal-01954618

[36] M. NAYA-PLASENCIA. *New results on symmetric quantum cryptanalysis (Keynote speaker)*, in "QUANTALGO Quantum Algorithms and Applications", Paris, France, September 2018, https://hal.inria.fr/hal-01953994

[37] M. NAYA-PLASENCIA. *New results on symmetric quantum cryptanalysis*, in "Crossfyre 2018 - 8th international workshop on cryptography, robustness, and provably secure schemes for female young researchers", Surrey, United Kingdom, September 2018, Keynote speaker at Crossfyre 2018, https://hal.inria.fr/hal-01953997

[38] M. NAYA-PLASENCIA. *Symmetric lightweight primitives: (Design and) Cryptanalysis*, in "Lightweight Crypto Day 2018", Tel Aviv, Israel, April 2018, https://hal.inria.fr/hal-01953947

[39] L. PERRIN. *Generalized Feistel Networks with Optimal Diffusion*, in "Dagstuhl Seminar 18021 Symmetric Cryptography", Dagstuhl, Germany, January 2018 [*DOI :* 10.4230/DAGREP.8.1.1], https://hal.inria.fr/hal-01953351

[40] L. PERRIN. *S-Box Reverse-Engineering: Boolean Functions, American/Russian Standards, and Butterflies*, in "CECC 2018 - Central European Conference on Cryptology", Smolenice, Slovakia, June 2018, pp. 1-99, https://hal.inria.fr/hal-01953348

International Conferences with Proceedings

[41] N. ARAGON, P. GABORIT, A. HAUTEVILLE, J.-P. TILLICH. *A New Algorithm for Solving the Rank Syndrome Decoding Problem*, in "ISIT 2018 - IEEE International Symposium on Information Theory", Vail, United States, June 2018, pp. 2421-2425 [*DOI :* 10.1109/ISIT.2018.8437464], https://hal.inria.fr/hal-01957179

[42] T. ASHUR, M. EICHLSEDER, M. M. LAURIDSEN, G. LEURENT, B. MINAUD, Y. ROTELLA, Y. SASAKI, B. VIGUIER. *Cryptanalysis of MORUS*, in "ASIACRYPT 2018 - 24th Annual International Conference on the Theory and Application of Cryptology and Information Security", Brisbane, Australia, LNCS - Lecture Notes in Computer Science, Springer, December 2018, vol. 11273, pp. 35-64 [*DOI :* 10.1007/978-3-030-03329-3_2], https://hal.inria.fr/hal-01944776

[43] X. BONNETAIN, M. NAYA-PLASENCIA. *Hidden Shift Quantum Cryptanalysis and Implications*, in "ASIACRYPT 2018 - 24th Annual International Conference on the Theory and Application of Cryptology and Information Security", Brisbane, Australia, LNCS - Lecture Notes in Computer Science, Springer, December 2018, vol. 11272, pp. 560-592 [*DOI :* 10.1007/978-3-030-03326-2_19], https://hal.inria.fr/hal-01953914

[44] G. COUTEAU, A. DUPIN, P. MÉAUX, M. ROSSI, Y. ROTELLA. *On the Concrete Security of Goldreich's Pseudorandom Generator*, in "ASIACRYPT 2018 - 24th Annual International Conference on the Theory and Application of Cryptology and Information Security", Brisbane, Australia, LNCS - Lecture Notes in Computer Science, Springer, December 2018, vol. 11273, pp. 96-124 [*DOI :* 10.1007/978-3-030-03329-3_4], https://hal.inria.fr/hal-01944772

[45] T. DEBRIS-ALAZARD, 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", Brisbane, Australia, LNCS - Lecture Notes in Computer Science, Springer, December 2018, vol. 11272, pp. 62-92 [*DOI :* 10.1007/978-3-030-03326-2_3], https://hal.inria.fr/hal-01957207

[46] E. EATON, M. LEQUESNE, A. PARENT, N. SENDRIER. *QC-MDPC: A Timing Attack and a CCA2 KEM*, in "PQCrypto 2018 - Ninth International Conference on Post-Quantum Cryptography", Fort Lauderdale, United States, LNCS - Lecture Notes in Computer Science, Springer, April 2018, vol. 10786 [*DOI :* 10.1007/978-3-319-79063-3_3], https://hal.inria.fr/hal-01949590

[47] O. FAWZI, A. GROSPELLIER, 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, October 2018, pp. 743-754, https://arxiv.org/abs/1808.03821 [*DOI :* 10.1109/FOCS.2018.00076], https://hal.archives-ouvertes.fr/hal-01895430

[48] O. FAWZI, A. GROSPELLIER, A. LEVERRIER. *Efficient decoding of random errors for quantum expander codes*, in "STOC 2018 - 50th Annual ACM Symposium on the Theory of Computing", Los Angeles, United States, June 2018, pp. 521-534, https://arxiv.org/abs/1711.08351 [*DOI :* 10.1145/3188745.3188886], https://hal.archives-ouvertes.fr/hal-01895427

[49] L. GRASSI, M. NAYA-PLASENCIA, A. SCHROTTENLOHER. *Quantum Algorithms for the k-xor Problem*, in "ASIACRYPT 2018 - 24th Annual International Conference on the Theory and Application of Cryptology and Information Security", Brisbane, Australia, LNCS - Lecture Notes in Computer Science, Springer, December 2018, vol. 11272, pp. 527-559 [*DOI :* 10.1007/978-3-030-03326-2_18], https://hal.inria.fr/hal-01896036

[50] B. LAC, A. CANTEAUT, J. J.-A. FOURNIER, R. SIRDEY. *Thwarting Fault Attacks against Lightweight Cryptography using SIMD Instructions*, in "ISCAS 2018 - IEEE International Symposium on Circuits and Systems", Florence, Italy, May 2018, pp. 1-5 [*DOI :* 10.1109/ISCAS.2018.8351693], https://hal-cea.archives-ouvertes.fr/cea-01746138

[51] M. LEQUESNE, 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], https://hal.inria.fr/hal-01949569

[52] G. LEURENT, M. NANDI, F. SIBLEYRAS. *Generic Attacks Against Beyond-Birthday-Bound MACs*, in "Crypto 2018 - 38th International Cryptology Conference", Santa Barbara, United States, LNCS - Lecture Notes in Computer Science, Springer, August 2018, vol. 10991, pp. 306-336 [*DOI :* 10.1007/978-3-319-96884-1_11], https://hal.inria.fr/hal-01944318

[53] G. LEURENT, F. SIBLEYRAS. *The Missing Difference Problem, and Its Applications to Counter Mode Encryption*, in "Eurocrypt 2018 - 37th Annual International Conference on the Theory and Applications of

Cryptographic Techniques", Tel Aviv, Israel, LNCS - Lecture Notes in Computer Science, April 2018, vol. 10821, pp. 745-770 [*DOI :* 10.1007/978-3-319-78375-8_24], https://hal.inria.fr/hal-01944288

[54] J.-P. TILLICH. *The decoding failure probability of MDPC codes*, in "ISIT 2018 - IEEE International Symposium on Information Theory", Vail, United States, June 2018, pp. 941-945 [*DOI :* 10.1109/ISIT.2018.8437843], https://hal.inria.fr/hal-01957037

Conferences without Proceedings

[55] P. CHARPIN, J. PENG. *New links between nonlinearity and differential uniformity*, in "Sequences and Their Applications (SETA) 2018", Hong-Kong, China, October 2018, https://hal.inria.fr/hal-01836184

[56] 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

[57] G. LEURENT. *The Missing Difference Problem: And its Applications to Counter Mode Encryption*, in "Flexible Symmetric Cryptography", Leiden, Netherlands, March 2018, https://hal.inria.fr/hal-01953390

[58] A. OLIVO, F. GROSSHANS. *Optimality of linear optical Bell measurements. How much can ancillae help?*, in "GDR IQFA 9th Colloquium", Montpellier, France, November 2018, https://hal.inria.fr/hal-01951749

[59] A. OLIVO, F. GROSSHANS. *Optimality of linear optical Bell measurements. How much can ancillae help?*, in "ICIQP 2018 - International Conference on Integrated Quantum Photonics", Paris, France, October 2018, https://hal.inria.fr/hal-01951728

[60] A. OLIVO, F. GROSSHANS. *Optimality of linear optical Bell measurements. How much can ancillae help?*, in "Q-Turn: changing paradigms in quantum science", Florianopolis, Brazil, November 2018, https://hal.inria.fr/hal-01951753

Scientific Popularization

[61] A. CANTEAUT. *Chut ! On nous écoute*, in "Semaine des Maths 2018", Paris, France, March 2018, https://hal.inria.fr/hal-01955267

[62] A. CANTEAUT. *Chut ! On nous écoute*, in "Conférence de clôture des Olympiades Nationales de Mathématiques 2018", Paris, France, June 2018, https://hal.inria.fr/hal-01955273

[63] A. CHAILLOUX. *L'algorithme quantique de Shor*, in "Interstices", March 2018, https://hal.inria.fr/hal-01827601

[64] G. LEURENT, M. NAYA-PLASENCIA. *La fragilité inattendue du chiffrement symétrique*, in "La Recherche : l'actualité des sciences", November 2018, vol. Novembre 2018, https://hal.inria.fr/hal-01953448

[65] L. PERRIN. *Building Light but not Weak Protections for the IoT*, in "PhD Graduation Ceremony of the University of Luxembourg (2018)", Belval, Luxembourg, December 2018, https://hal.inria.fr/hal-01959751

Other Publications

[66] X. BONNETAIN, M. NAYA-PLASENCIA, A. SCHROTTENLOHER. *On Quantum Slide Attacks*, December 2018, working paper or preprint, https://hal.inria.fr/hal-01946399

[67] X. BONNETAIN, M. NAYA-PLASENCIA, A. SCHROTTENLOHER. *Quantum Cryptanalysis of AES*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01955534

[68] X. BONNETAIN, A. SCHROTTENLOHER. *Quantum Security Analysis of CSIDH and Ordinary Isogeny-based Schemes*, October 2018, working paper or preprint, https://hal.inria.fr/hal-01896046

[69] X. BONNETAIN, A. SCHROTTENLOHER. *Submerging CSIDH*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01961633

[70] A. CANTEAUT. *Exploiting algebraic properties of block ciphers*, February 2018, COST Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, https://hal.inria.fr/hal-01955320

[71] A. CANTEAUT. *Secure building-blocks against differential and linear attacks*, February 2018, COST Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, https://hal.inria.fr/hal-01955315

[72] A. CANTEAUT, L. PERRIN. *On CCZ-Equivalence, Extended-Affine Equivalence and Function Twisting*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01959749

[73] K. CARRIER, J.-P. TILLICH. *Near collisions search and generic decoding*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01959614

[74] A. CHAILLOUX. *A note on the quantum query complexity of permutation symmetric functions*, December 2018, https://arxiv.org/abs/1810.01790 - 8 pages [*DOI :* 10.01790], https://hal.inria.fr/hal-01950650

[75] A. CHAILLOUX. *DEREC - Développement de la cryptographie relativiste*, October 2018, WISG 2018 - 12ème Workshop Interdisciplinaire sur la Sécurité Globale, Poster, https://hal.inria.fr/hal-01950649

[76] P. CHARPIN, J. PENG. *Differential uniformity and the associated codes of cryptographic functions*, November 2018, working paper or preprint, https://hal.inria.fr/hal-01908336

[77] D. COGGIA. *On subspace trails cryptanalysis*, Université Paris Diderot (Paris 7), September 2018, https://hal.inria.fr/hal-01955305

[78] D. COGGIA. *On subspace trails cryptanalysis*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01960306

[79] A. COUVREUR, M. LEQUESNE, J.-P. TILLICH. *Recovering short secret keys of RLCE encryption scheme in polynomial time*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01959617

[80] A. COUVREUR, M. LEQUESNE, J.-P. TILLICH. *Recovering short secret keys of RLCE in polynomial time*, May 2018, https://arxiv.org/abs/1805.11489 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01803440

[81] T. DEBRIS-ALAZARD, N. SENDRIER, J.-P. TILLICH. *Wave: A New Code-Based Signature Scheme*, December 2018, preprint IACR disponible sur https://eprint.iacr.org/2018/996/20181022:154324, https://hal.inria.fr/hal-01958175

[82] T. DEBRIS-ALAZARD, J.-P. TILLICH. *Deux attaques contre des schémas se fondant sur les codes en métrique rang : Ranksign et un chiffrement basé sur l'identité*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01959613

[83] A. GROSPELLIER, A. KRISHNA. *Numerical estimate of the threshold for quantum expander codes*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.archives-ouvertes.fr/hal-01955453

[84] A. GROSPELLIER, A. KRISHNA. *Numerical study of hypergraph product codes*, October 2018, https://arxiv.org/abs/1810.03681 - 10 pages, 2 figures [*DOI :* 10.03681], https://hal.archives-ouvertes.fr/hal-01895436

[85] M. LEQUESNE, J.-P. TILLICH. *Attack on the EDON-K Key Encapsulation Mechanism*, November 2018, https://arxiv.org/abs/1802.06157 - Submitted to ISIT 2018, https://hal.sorbonne-universite.fr/hal-01925323

[86] G. LEURENT. *How Not to Use a Blockcipher*, February 2018, COST Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, https://hal.inria.fr/hal-01953398

[87] G. LEURENT, F. SIBLEYRAS. *The Missing Difference Problem, and its Applications to Counter Mode Encryption*, October 2018, JC2 2018 - Journées Codage et Cryptographie, https://hal.inria.fr/hal-01961739

[88] A. LEVERRIER. *Security of continuous-variable quantum key distribution*, May 2018, Secure Quantum Communications School, Baiona, Spain, https://hal.inria.fr/hal-01955365

[89] F. MENDEL, M. NAYA-PLASENCIA. *Preface*, March 2018, vol. 2018, n^{o} 1, pp. 1 - 4, IACR Transactions on Symmetric Cryptology (ToSC) [*DOI :* 10.13154/TOSC.V2018.I1.1-4], https://hal.inria.fr/hal-01953923

[90] M. NAYA-PLASENCIA. *Introduction to Symmetric Cryptography*, June 2018, Summer School on real-world crypto and privacy, https://hal.inria.fr/hal-01953897

[91] M. NAYA-PLASENCIA. *Lightweight Cryptography*, June 2018, Summer School on real-world crypto and privacy, https://hal.inria.fr/hal-01953789

[92] M. NAYA-PLASENCIA. *New results on symmetric quantum cryptanalysis*, March 2018, Keynote speaker at Flexible symmetric cryptography -Lorentz Center, https://hal.inria.fr/hal-01954599

[93] M. NAYA-PLASENCIA. *New results on symmetric quantum cryptanalysis*, March 2018, Seminaire CCA, https://hal.inria.fr/hal-01954616

[94] M. NAYA-PLASENCIA. *Symmetric Cryptanalysis: the Foundation of Trust*, March 2018, Lorentz Center Highlights, https://hal.inria.fr/hal-01954612

[95] A. QUEROL CRUZ. *Conditional Differential Cryptanalysis of the Post-Quantum ARX Symmetric Primitive Salsa20*, Univeristé Denis Diderot Paris 7, September 2018, https://hal.inria.fr/hal-01893824