Activity Report 2019

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, end of the Project-Team: 2019 November 30

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, Researcher]
Anthony Leverrier [Inria, Researcher, HDR]
María Naya Plasencia [Inria, Senior Researcher, HDR]
Léo Perrin [Inria, Researcher, from Sep 2019]
Nicolas Sendrier [Inria, Senior Researcher, HDR]
Jean-Pierre Tillich [Inria, Senior Researcher, HDR]

Faculty Members

Magali Bardet [Univ de Rouen, Associate Professor, from Sept 2019]
Christina Boura [Univ de Versailles Saint-Quentin-en-Yvelines, Associate Professor, from Sept 2019]

Post-Doctoral Fellows

Christophe Vuillot [Inria, Post-Doctoral Fellow, from Nov 2019]
Simon Apers [Inria, Post-Doctoral Fellow]
Ivan Bardet [Inria, Post-Doctoral Fellow, from Mar 2019]
Léo Perrin [Inria, Post-Doctoral Fellow, until Aug 2019]

PhD Students

Xavier Bonnetain [Sorbonne Université, PhD Student]
Rémi Bricout [Sorbonne Université, PhD Student]
Kevin Carrier [Ministère de la Défense, PhD Student9]
Daniel Coggia [DGA, PhD Student]
Thomas Debris [Sorbonne Université PhD Student, until Sep 2019]
Simona Etinski [Univ Denis Diderot, PhD Student, from Oct 2019]
Antonio Florez Gutierrez [Inria, PhD Student, from Sep 2019]
Shouvik Ghorai [Sorbonne Université]
Antoine Grospellier [Sorbonne Université, PhD Student, until Aug 2019]
Lucien Grouès [Sorbonne Université, PhD Student, from Oct 2019]
Matthieu Lequesne [Univ Pierre et Marie Curie, PhD Student]
Vivien Londe [Univ de Bordeaux, PhD Student, until Aug 2019]
Rocco Mora [Sorbonne Université, PhD Student, from Oct 2019]
Andrea Olivo [Inria, PhD Student]
André Schrottenloher [Inria, PhD Student]
Ferdinand Sibleyras [Inria, PhD Student]
Valentin Vasseur [Univ René Descartes, PhD Student]

Interns and Apprentices

Augustin Bariant [Inria, from Apr 2019 until Aug 2019]
Nicolas David [École Normale Supérieure de Cachan, from Mar 2019 until Aug 2019]
Rachelle Heim [Sorbonne Université, Jul 2019]
Sohaib Ouzineb [Inria, from Jul 2019 until Aug 2019]
Elodie Rohart-Barbey [Inria, from Jun 2019 until Aug 2019]
Pierre Briaud [Inria, from Mar 2019 until Aug 2019]
Antonio Florez Gutierrez [Inria, from Mar 2019 until Aug 2019]
Lucien Grouès [Inria, from Mar 2019 until Sep 2019]

Administrative Assistant

Christelle Guiziou [Inria, Administrative Assistant]

Visiting Scientists

Akinori Hosoyamada [NTT Secure Platform Labaratories, Japan, Mar 2019 and Nov 2019]
Mustafa Mahmoud Mohammed Kairallah [NTU, Singapore, Jul 2019]
Thomas Peyrin [NTU, Singapore, Jan and June 2019]
Yu Sasaki [NTT Secure Platform Labaratories, Japan, Nov 2019]
Shizhu Tian [Chinese Academy of Sciences, until Sep 2019]

2. Overall Objectives

2.1. Presentation and scientific foundations

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

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

2.2. Main topics

Our domain in cryptology includes the analysis and the design of

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

3. Research Program

3.1. Scientific foundations

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

3.2. Symmetric cryptology

Symmetric techniques are widely used because they are the only ones that can achieve some major features such as high-speed or low-cost encryption, fast authentication, and efficient hashing. It is a very active research area which is stimulated by a pressing industrial demand. The process which has led to the new block cipher standard AES in 2001 was the outcome of a decade of research in symmetric cryptography, where new attacks have been proposed, analyzed and then thwarted by some appropriate designs. However, even if its security has not been challenged so far, it clearly appears that the AES cannot serve as a Swiss knife in all environments. In particular an important challenge raised by several new applications is the design of symmetric encryption schemes with some additional properties compared to the AES, either in terms of implementation performance (low-cost hardware implementation, low latency, resistance against side-channel attacks...) or in terms of functionalities (like authenticated encryption). The past decade has then been characterized by a multiplicity of new proposals. This proliferation of symmetric primitives has been amplified by several public competitions (eSTREAM, SHA-3, CAESAR...) which have encouraged innovative constructions and promising but unconventional designs. We are then facing up to a very new situation where implementers need to make informed choices among more than 40 lightweight block ciphers [1] or 57 new authenticated-encryption schemes [2]. Evaluating the security of all these proposals has then become a primordial task which requires the attention of the community.

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

[1] 35 are described on https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers.
[2] see http://competitions.cr.yp.to/caesar-submissions.html

3.3. Code-based cryptography

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

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

3.4. Quantum information

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

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

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

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

4. Application Domains

4.1. Cryptographic primitives

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

4.2. Code Reconstruction

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

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

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

5. Highlights of the Year

5.1. Highlights of the Year

- **Keynote at FSE 2019:** María Naya Plasencia bas been an invited keynote speaker at FSE 2019 in Paris.
- **NIST competition on post-quantum cryptography:** The members of the project-team have submitted 5 candidates to the NIST competition on post-quantum cryptography. After a first selection, three of our candidates have been moved to the second round of the competition, which includes a total of 26 candidates.
- **NIST competition on lightweight cryptography:** The members of the project-team are involved in the design of 3 authenticated encryption schemes submitted to the NIST lightweight competition. These three ciphers are among the 32 candidates which have been move to the second round of the competition.

5.1.1. Awards

- María Naya Plasencia was awarded the Inria - Académie des Sciences prize for young researchers https://www.academie-sciences.fr/fr/Laureats/prix-inria-academie-des-sciences-2019-vincent-hayward-equipe-scikit-learn-et-maria-naya-plasencia.html
- Anne Canteaut has been made doctor honoris causa of the University of Bergen (Norway), October 2019 https://www.uib.no/en/news/129910/ten-new-honorary-doctorates

BEST PAPERS AWARDS:

[31]
L. PERRIN. *Partitions in the S-Box of Streebog and Kuznyechik*, in "IACR Transactions on Symmetric Cryptology", March 2019, vol. 2019, n^{o} 1, pp. 302-329 [*DOI :* 10.13154/TOSC.V2019.I1.302-329], https://hal.inria.fr/hal-02396814

[49]
T. DEBRIS-ALAZARD, N. SENDRIER, J.-P. TILLICH. *Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes*, in "ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, LNCS, Springer, November 2019, vol. 11921, pp. 21-51 [*DOI :* 10.1007/978-3-030-34578-5_2], https://hal.inria.fr/hal-02424057

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 variant 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, Daniel Coggia, Pascale Charpin, Daniel Coggia, Gaëtan Leurent, María Naya Plasencia, Léo Perrin, 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:

- Design of SATURNIN a new lightweight block cipher for authenticated encryption [74], which is resistant to quantum cryptanalysis. SATURNIN has been submitted to the NIST competition for lightweight cryptography, and has been selected for the 2nd round of the competition [5].
- Mixture-differential distinguishers on AES-like ciphers [18].
- Cryptanalysis of the Sbox of the Russian standards, Streebog and Kuznyechik [31], [56]. This work by L. Perrin received the best paper award at *FSE 2019*. Moreover, L. Perrin has been invited to present his results to AFNOR. He is involved in the international standardization processes in symmetric cryptography [50], [86] and has been invited to ISO meetings on this topic.
- The work on the Streebog Sbox has led to a more general study on tools for quantifying anomalies in Sboxes [44].
- Design of BISON, the first concrete block cipher following the whitened swap-or-not construction [46].

7.1.2. MACs and hash functions

The international research effort related to the selection of the new hash function standard SHA-3 has led to many important results and to a better understanding of the security offered by hash functions. However, hash functions are used in a huge number of applications with different security requirements, and also form the building-blocks of some other primitives, like MACs.

[5] https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/saturnin-spec-round2.pdf

Recent results:

- Chosen-prefix collision attack on SHA-1 [52]: A chosen-prefix collision attack is a stronger variant of a collision attack, where an arbitrary pair of challenge prefixes are turned into a collision. Chosen-prefix collisions are usually significantly harder to produce than (identical-prefix) collisions, but the practical impact of such an attack is much larger. G. Leurent and T. Peyrin proposed new techniques to turn collision attacks into chosen-prefix collision attacks, and present such an attack against SHA-1 with complexity between $2^{66.9}$ and $2^{69.4}$ (depending on assumptions about the cost of finding near-collision blocks).
- Design of lighweight MACs from universal hash functions [51]. Many constructions of MACs used in practice (such as GMAC or Poly1305-AES) follow the Wegman-Carter-Shoup construction, which is only secure up to 2^{64} queries with a 128-bit state. S. Duval and G. Leurent proposed new constructions to reach security beyond the birthday bound, and proposed a concrete instantiation, with very good performances on ARM micro-controllers.

7.1.3. 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 [19]. 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 have provided an in-depth analysis of BCT, by studying more closely differentially 4-uniform Sboxes. More recently, C. Boura, L. Perrin and S. Tian have obtained new results on the boomerang uniformity of several constructions of Sboxes [57].
- 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 [21], [58].
- 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 [27]

- Study of the properties of the error-correcting codes associated to differentially 4-uniform Sboxes [26]. Most notably, this work analyzes the relationship between the number of low-weight codewords and the nonlinearity of the corresponding Sbox.
- Study of crooked and weakly-crooked functions [35]: Crooked functions form a family of APN functions whose derivaties take they values in an (affine) hyperplane.
- APN functions with the butterfly construction [22], [34]: the butterfly construction, originally introduced by Perrin et al., is a general construction which includes the only known example of APN permutation operating on an even number of variables. A. Canteaut, L. Perrin and S. Tian have proved that the most recent generalization of this construction does not include any other APN function when the number of variables exceeds six.

7.1.4. Modes of operation and generic attacks

In order to use a block cipher in practice, and to achieve a given security notion, a mode of operation must be used on top of the block cipher. Modes of operation are usually studied through 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:

- Low-memory attacks against the 2-round Even-Mansour construction, using the 3-xor problem [41]: G. Leurent and F. Sibleyras proved that attacking the 2-round Even-Mansour construction with blocksize n is related to the 3-XOR problem with elements on size $2n$. Then, they exhibited the first generic attacks on this construction where both the data and the memory complexity are significantly lower than 2^n.
- Generic attacks against the tweakable FX-construction [55]: F. Sibleyras exhibited a generic attack on the general tweakable iterated FX-construction, which provides an upper-bound on its security. Most notably, for two rounds, this upper bound matches the proof of the particular case of XHX2 by Lee and Lee at Asiacrypt 2018, thus proving for the first time its tightness.
- Modes for authenticated encryption: Besides the design of new lightweight authenticated encryption schemes, we also analyzed some modes of operation in case of release of unverified plaintext (RUP). Indeed, in this setting, an adversary gets separated access to the decryption and verification functionality, and has more power in breaking the scheme. Our results include a forgery attack against the GCM-RUP mode of operation [54], and the design of a new lightweight deterministic scheme, named ANYDAE, which is particularly efficient for short messages, and achieves both conventional security and RUP security [24].
- Generic attacks on hash combiners [15]: G. Leurent and his co-authors analyzed the security of hash combiners, i.e. of procedures that combine two or more hash functions in a way that is hopefully more secure than each of the underlying hash functions, or at least remains secure as long as one of them is secure. They found generic attacks on the XOR combiner, on the concatenation of two Merkle-Damgård hash functions and on the Zipper hash and on the Hash-Twice combiners when they both use Merkle-Damgård hash constructions.

7.2. Code-based cryptography

Participants: Magali Bardet, Kevin Carrier, André Chailloux, Thomas Debris, Matthieu Lequesne, Rocco Mora, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur.

In recent years, there has been a substantial amount of research on quantum computers. Such computers would be a major threat for all the public-key cryptosystems used in practice, since all these systems rely on the hardness of integer factoring or discrete logarithms, and these problems are easy on a quantum computer. This has prompted NIST to launch a standardization process in 2017 for quantum-safe alternatives to those cryptosystems. This concerns all three major asymmetric primitives, namely public-key encryption schemes, key-exchange protocols and digital signatures. There were 69 valid submissions to this call in November 2017, with numerous lattice-based, code-based and multivariate-cryptography submissions and some submission based either on hashing or on supersingular elliptic curve isogenies. NIST expects to perform multiple rounds of evaluation, over a period of three to five years. The goal of this process is to select a number of acceptable candidate cryptosystems for standardization. The second round of evaluation started in February 2019.

The research of the project-team in this field is focused on the design and cryptanalysis of cryptosystems making use of coding theory. 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). Our recent work on code-based cryptography has to be seen in the context of the recently launched NIST competition for quantum-safe primitives. We have proposed five code-based candidates to the NIST call for the first two primitives, namely public key encryption and key exchange protocols. 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.

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

7.2.1. Design of new code-based solutions

The members of the project-team have submitted several candidates to the NIST competition and have designed new code-based primitives.

Recent results:

- Design of a new code-based signature scheme [49]: 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.
- Analysis of the ternary Syndrome Decoding problem [45]: R. Bricout, A. Chailloux, T. Debris and M. Lequesne have performed an algorithmic study of this decoding problem in large weight, which corresponds to the underlying problem in the WAVE signature scheme. Most notably, their study results in an update of the Wave parameters. It also shows that ternary Syndrome Decoding with large weight is a really harder problem than the binary Syndrome Decoding problem, and could have several applications for the design of code-based cryptosystems.

7.2.2. Cryptanalysis of code-based schemes

Recent results:

- Attack against RLCE [48]: 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.
- Analysis of an encryption scheme based on the rank syndrome decoding problem [61]: D. Coggia and A. Couvreur presented an attack against a cryptosystem proposed proposed by Loidreau, which used an intermediary version between Gabidulin codes and LRPC codes. This attack has polynomial time for some parameters of the scheme.
- Decoding algorithm for codes with a non-trivial automorphism group [47]: R. Canto-Torres and JP Tillich presented an algorithm which is able to speed up the decoding of a code with a non-trivial automorphism group. For a certain range of parameters, this results in a decoding that is faster by an exponential factor in the code length when compared to the best algorithms for decoding generic linear codes. This algorithm was then used to break several proposals of public-key cryptosystems based on codes with a non-trivial automorphism group.

7.3. Quantum Information

Participants: Simon Apers, Ivan Bardet, Xavier Bonnetain, Rémi Bricout, André Chailloux, Simona Etinski, Antonio Florez Gutierrez, Shouvik Ghorai, Antoine Grospellier, Lucien Grouès, Anthony Leverrier, Vivien Londe, María Naya Plasencia, Andrea Olivo, Jean-Pierre Tillich, André Schrottenloher, Christophe Vuillot.

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 theses have been defended this year within the project-team on this topic. First, Antoine Grospellier, co-advised by A. Leverrier and O. Fawzi (Ens Lyon), studied efficient decoding algorithms for quantum LDPC codes [13]. 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, co-advised by A. Leverrier and G. Zémor (IMB), worked on the design of better quantum LDPC codes [14]: the main idea is to generalize the celebrated toric code of Kitaev by considering cellulations of manifolds in higher dimensions. A 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.

Lucien Grouès, who did an internship this summer in the project-team, has recently started a PhD with A. Leverrier and O. Fawzi on decoding quantum LDPC codes, and preliminary numerical results have already appeared in [62].

Ivan Bardet joined the project-team as a postdoc in March 2019, and will start a starting research position in 2020. His research focusses on the study of open-system dynamics as well as mixing times of Markovian dissipative evolutions with the goal of better understanding the lifetime of quantum memories.

Recent results:

- Decoding algorithms for Hypergraph Product Codes [62]: this work deals with numerical simulation of several variants of the SMALL-SET-FLIP decoder for hypergraph product codes. While this decoder had already been studied analytically in previous work in the regime of extremely low noise, we are focussing here on understanding its performance for a realistic noise model.
- Towards Low Overhead Magic State Distillation [30]: the major source of overhead in quantum fault-tolerance usually lies in the primitive called magic state distillation which takes a number of noisy versions of a specific quantum state and prepares a new state with less noise. An important question is to understand how efficient this procedure can be. In this work, we prove that magic state distillation can perform much more efficiently than expected when working with quantum systems of large dimension instead of qubits.

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 contributes to this project by studying the security of new key distribution protocols.

Recent results:

- Security proof for two-way continuous-variable quantum key distribution [28]: 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, 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.
- Asymptotic security of continuous-variable quantum key distribution with a discrete modulation [29]: in this work, we establish a lower bound on the secret key rate of a practical quantum key distribution protocol that will be implemented in the context of the H2020 project CiViQ.

7.3.3. Quantum cryptanalysis of symmetric primitives and quantum algorithms

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 been awarded an ERC Starting grant for her project named QUASYModo on this topic.

In parallel to this work, S. Apers is developing generic quantum algorithms solving combinatorial problems, notably in graphs. He also recently proposed a unified framework of quantum walk search, that will likely find applications in the context of quantum cryptanalysis.

Recent results:

- Quantum algorithm for the k-XOR problem and for list merging: 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. A. Chailloux, 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 [38], [39].

- Quantum security of AES [17]: In order to determine the post-quantum secuirty margin of AES-256, X. Bonnetain and M. Naya-Plasencia have proposed generalized and quantized versions of the best known cryptanalysis on reduced-round versions of AES-256, including a quantum Demirci-Selçuk meet-in-the-middle attack.
- Quantum attacks without superposition queries : In symmetric cryptanalysis, the model of superposition queries has led to surprising results, but the practical implications of these attacks remain blurry. In contrast, the results obtained so far for a quantum adversary making classical queries only were less impressive. For the first time, M. Naya-Plasencia and A. Schrottenloher, together with A. Hosoyamada and Y. Sasaki, managed to leverage the algebraic structure of some cryptosystems in the context of a quantum attacker limited to classical queries and offline quantum computations. Most notably, they are able to break the Even-Mansour construction in quantum time $\widetilde{\mathcal{O}}(2n/3)$ with $\mathcal{O}(2n/3)$ classical queries and $\mathcal{O}(n^2)$ qubits only.
- Quantum cryptanalysis of CSIDH and Ordinary Isogeny-based Schemes [16]: 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.
- New graph-related quantum algorithms. A first paper presents an approach to improve expansion testing using quantum Fast-Forwarding and growing seed sets [64]. A second paper introduces a graph sparsification algorithm [65], which when combined with existing classical algorithms yields the first quantum speedup for approximating the max cut, min cut, min st-cut, sparsest cut and balanced separator of a graph. Moreover, combining it with a classical Laplacian solver yields a similar speedup for Laplacian solving, for approximating effective resistances, cover times and eigenvalues of the Laplacian, and for spectral clustering.
- Quantum walks: in a first work, S. Apers describes a new quantum algorithm for quantum walk sampling using growing seed sets [42] with applications for st-connectivity and problems related to graph isomorphism. A second work [66] introduces a new quantum walk search framework that unifies and strengthens the existing ones.
- Quantum query lower bounds [59], [60]: Many computational problems, such as finding collisions in a function, are symmetric in their inputs. A. Chailloux showed that for this class of problems, any quantum algorithm can have at most a cubic advantage over the best classical algorithm in the query model, while the previously known bound gave up to 7th root advantage. This result enhances our understanding on the limitations of quantum algorithms.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **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. 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.

8.2.1.2. 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.

8.2.1.3. H2020 FET Flagship on Quantum Technologies - CiViQ

Title: CiViQ *Continuous Variable Quantum Communications*

Program: H2020 FET Flagship on Quantum Technologies

Duration: October 2018 - September 2021

PI: Anthony Leverrier

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

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 - 2019

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.
- NTT Secure Platforms Laboratories (Japan): quantum cryptanalysis, symmetric cryptography.
- University of Sherbrooke (Canada): quantum codes.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Thomas Peyrin, NTU Singapore, January 2019 and July 2019
- Mustafa Mahmoud Mohammed Kairallah, NTU Singapore, July 2019
- Léo Ducas, CWI Amsterdam, NL, March 2019
- Akinori Hosoyamada, NTT Secure Platform Labaratories, Tokyo, Japan, March 2019 and November 2019
- Yu Sasaki, NTT Secure Platform Labaratories, Tokyo, Japan, November 2019
- Gregor Leander, Ruhr Université Bochum, Germany, November 2019

8.4.1.1. Internships

- Pierre Briaud, MPRI, March-Aug. 2019
- Lucien Grouès, Telecom ParisTech, March-Sept. 2019
- Antonio Florez Gutierrez, Université Paris Saclay, March-Aug. 2019

- Sohaïb Ouzineb, Telecom ParisTech, July-Aug. 2019
- Elodie Rohart-Barbey, INSA Rouen, June-Aug. 2019
- Augustin Bariant, Ecole Polytechnique, April-Aug. 2019

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

- Bar-Ilan Unversity, Israel, June 16-18, invitation by Nathan Keller (A. Canteaut and G. Leurent)
- Rostock University, Rostock, Germany, June 23-28, invitation to the Institut für Mathematik by Gohar Kyureghyan, (L. Perrin).
- NTT, Tokyo, Japan, August 27-September 27, invitation by Yu Sasaki (F. Sibleyras)

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events: Organisation

9.1.1.1. General Chair, Scientific Chair

- FSE 2020, March 2020, Athens, Greece: C. Boura, general chair ; G. Leurent, program co-chair
- PQCrypto 2020, April 15 - April 17, 2020, Paris, France: N. Sendrier, general co-chair ; J.P. Tillich, program co-chair
- Dagstuhl seminar on Quantum Cryptanalysis 2019, October 13-18, 2019, Dagstuhl, Germany: M. Naya-Plasencia co-organizer.

9.1.1.2. Member of the Organizing Committees

- FSE 2019: March 25-28, 2019, Paris, France: Gaëtan Leurent.

9.1.2. Scientific Events: Selection

9.1.2.1. Chair of Conference Program Committees

- Co-editor-in-chief of *IACR Transactions on Symmetric Cryptology* starting from 2019: Gaëtan Leurent.
- Co-chair of the Program Committee of *Eurocrypt 2020*, Zagreb, Croatia, May 2020: Anne Canteaut
- Co-chair of the Program Committee of *FSE 2020*, Athens, Greece, March 2020: Gaëtan Leurent.
- Co-chair of the Program Committee of *WCC 2019*, March-April 2019, St Jacut-de-la-Mer, France: A. Canteaut
- Chair of the Program Committee of *QCrypt 2019*, August 26-30 2019, Montreal, Canada: A. Leverrier

9.1.2.2. Member of the Conference Program Committees

- 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, (M. Naya-Plasencia, N. Sendrier, J.P. Tillich);
- CBC 2019: May 18-19, 2019, Darmstadt, Germany, (J.-P. Tillich);
- TQC 2019: June 3-9, 2019, University of Maryland, USA, (A. Chailloux);
- ISIT 2019: July 7-12, 2019, Paris, France, (A. Leverrier, J.-P. Tillich);

- CHES 2019: August 25-28, 2019, Atlanta, USA, (G. Leurent);
- PQC: Perspectives on Quantum Computing, NISQ and beyond: November 20, 2019, Paris, France (A. Leverrier);
- SPACE 2019: December 3-7, 2019, Gandhinagar, India (L. Perrin);
- FSE 2020: March 22-26, 2020, Athens, Greece, (C. Boura, A. Canteaut, G. Leurent co-chair, L. Perrin)
- PQCrypto 2020: April 15-17, 2020, Paris, France (A. Chailloux, M. Naya-Plasencia, N. Sendrier, J.P. Tillich);
- CBCrypto 2020: May 9-10, 2020, Zagreb, Croatia, (J.-P. Tillich);
- Eurocrypt 2020: May 10-14, 2020, Zagreb, Croatia, (A. Canteaut co-chair, M. Naya-Plasencia);
- ISIT 2020: June 21-26, 2020, Los Angeles, USA, (J.-P. Tillich).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- *Advances in Mathematics of Communications*, associate editors: N. Sendrier and J.P. Tillich
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut.
- *Designs, Codes and Cryptography*, associate editor: P. Charpin.
- *Finite Fields and Applications*, associate editors: A. Canteaut, P. Charpin.
- *IACR Transactions on Symmetric Cryptology*, associate editors: C. Boura, A. Canteaut, G. Leurent (co-editor in chief), M. Naya-Plasencia, L. Perrin.
- *IACR Transactions on Cryptographic Hardware and Embedded Systems*, associate editor: G. Leurent.
- *Quantum (the open journal for quantum science)*, associate editor: A. Leverrier.
- *IEEE Transactions on Information Theory*, associate editor: A. Canteaut.

9.1.4. Invited Talks

- P. Charpin, *Crooked and weakly crooked functions*, Finite Fields and Applications - Fq14, Vancouver, Canada, June 3-7, 2019.
- M. Naya-Plasencia, *Preparing Symmetric Cryptography for the Quantum World*, FSE 2019, Paris, France, 24-28 March, 2019.

9.1.5. Leadership within the Scientific Community

- A. Canteaut serves as a chair of the steering committee of *Fast Software Encryption (FSE)*, M. Naya-Plasencia and G. Leurent also serve on the committee.
- N. Sendrier serves on the steering committee of *Post-quantum cryptography (PQCrypto)*.
- P. Charpin, N. Sendrier and JP Tillich serve on the steering committee of the WCC conference series.

9.1.6. Research Administration

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

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

- 2019 Jury Inria Research Positions (ARP/SRP) (M. Naya-Plasencia);
- 2019 Jury d'admission Inria DR2, (M. Naya-Plasencia);
- 2019 Jury d'admissibilité Inria DR2, (A. Canteaut);
- 2019 Jury d'admissibilité Inria CRCN national (A. Canteaut);
- Committee for the nomination to a permanent position, Radboud University Nijmegen, Netherlands (M. Naya-Plasencia).
- Committee for a professorship in cryptography, TU Graz, Austria (A. Canteaut)
- Reviewer for a promotion to professorhip, ISI Kolkata, India (A. Canteaut)
- Committee for 3 assistant professor positions in computer science at Université de Paris: A. Leverrier

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*, 12 hours, M2, University Paris-Diderot (MPRI), France;

Master: A. Chailloux, *Quantum algorithms*, 4 hours, M2, Ecole Normale Supérieure de Lyon, France;

Master: A. Leverrier, *Quantum information and quantum cryptography*, 12 hours, M2, University Paris-Diderot (MPRI), France;

Master: L. Perrin, *Application Web et Sécurité*, 24 hours, M1, UVSQ, France;

Bachelor: L. Perrin, *Cryptographie*, 29 hours, L3, UVSQ, France;

Master: J.-P. Tillich, *Introduction to Information Theory*, 36 hours, M2, Ecole Polytechnique, France;

Master: J.-P. Tillich, *Quantum Information and Applications*, 36 hours, M2, Ecole Polytechnique, France.

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

- N. Sendrier, *Code-Based Cryptography*, PQCrypto 2019 Summer School, Chongqing, China, May 6, 2019.

9.2.2. Supervision

PhD: Xavier Bonnetain, *Cryptanalysis of symmetric primitives in the post-quantum world*, Sorbonne Université, November 15, 2019, supervisor: M. Naya Plasencia.

PhD: Thomas Debris, *Quantum algorithms for decoding linear codes*, Sorbonne Université, December 17, 2019, supervisor: JP Tillich.

PhD: Antoine Grospellier, *LDPC codes: constructions and decoding*, Sorbonne Université, November 8, 2019, supervisors: A. Leverrier and O. Fawzi (ENS Lyon)

PhD: Vivien Londe, *Study of quantum LDPC codes*, University of Bordeaux, December 6, 2019, supervisors: G. Zémor (Univ. Bordeaux) and A. Leverrier

PhD in progress: Kevin Carrier, *Presque-collisions et applications au décodage générique et à la reconnaissance de codes correcteurs d'erreurs*, since October 2016, supervisor: N. Sendrier and JP Tillich.

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: André Schrottenloher, *Long-term security of symmetric primitives*, since February 2018 supervisor: M. Naya-Plasencia

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.

PhD in progress: Simona Etinski, *Quantum algorithms and protocols*, since October 2019, supervisors: A. Chailloux, A. Leverrier and F. Magniez (Université de Paris)

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

PhD in progress: Lucien Grouès, *Decoding algorithms for quantum LDPC codes*, since October 2019, supervisors: A. Leverrier, O. Fawzi

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

9.2.3. Juries

- Lorenzo Grassi, *Cryptanalysis of AES-like ciphers and reviving old design ideas for new constructions*, TU Graz, Austria, April 26, 2019, committe: A. Canteaut (reviewer).
- Louiza Khati, *Full Disk Encryption and Beyond*, Université Paris PSL, July 15, 2019, committee: M. Naya-Plasencia (chair).
- T. van Himbeeck, *Quantum Cryptography with Partially Trusted Devices*, Université Libre de Bruxelles, October 18, 2019, committee: A. Leverrier
- A. Aloshious, *Higher dimensional topological codes : structural properties and decoders*, Indian Institute of Technology Madras, November, 2019, committee: J.-P. Tillich (reviewer).
- A. Grospellier, *Décodage des codes expanseurs quantiques et application au calcul quantique tolérant aux fautes*, Sorbonne University, November 8, 2019, committee: A. Leverrier (supervisor), J.-P. Tillich.
- Xavier Bonnetain, *Hidden structures and quantum cryptanalysis*, Sorbonne Université, November 15, 2019, committee: A. Chailloux, M. Naya-Plasencia (Supervisor).
- Loïc Ferreira, *Secure Tunnels for Constrained Environments*, Université Bretagme Loire, November 18, 2019, committee: M. Naya-Plasencia.
- O. Fawzi, HdR, *Contributions to quantum information theory*, École Normale Supérieure de Lyon, December 2, committee: J.-P. Tillich (reviewer).
- V. Londe, *Topological Quantum Error-Correcting Codes beyond dimension 2*, Bordeaux University, December 6, 2019, committee: A. Leverrier (supervisor), JP Tillich

- M. Bozzio, *Security and implementation of advanced quantum cryptography: Quantum money - Quantum weak coin flipping*, Université Paris-Saclay, December 10, 2019, committee: A. Leverrier (reviewer)
- Alain Couvreur, HdR, *Codes algébriques et géométriques, applications à la cryptographie et à l'information quantique*; Université Paris-Diderot, December 16, 2020, committee: N. Sendrier (reviewer), J.P. Tillich
- Patrick Lacharme, HdR, *Études en Securité Informatique*, Université de Normandie, February 6, 2020, committee: M. Naya-Plasencia (reviewer).
- Thomas Debris, *Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves ; contribution en cryptanalyse*; Sorbonne Université, December 17, 2019, committee: N. Sendrier, J.P. Tillich (supervisor)

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

- *La fragilité inattendue du chiffrement symétrique dans le monde post-quantique*, Gaëtan Leurent and Maria Naya-Plasencia, María, Interstices [63]

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, he was also involved in the redaction of the exercises.
- Organization of the event “Rendez-vous des Jeunes Mathématiciennes et Informaticiennes” at Inria Paris (October 28-29) by M. Lequesne, a 2-day camp for 20 high-school girls interested in mathematics and computer science. C. Boura, A. Canteaut and L. Perrin gave talks at this event.
- **Project Algo’scape with a high school (Lycée Anna Judic, Semur en Auxois):** design of an escape game on cryptography (L. Perrin), visit of 15 students at Inria, May 2019 (A. Canteaut and L. Perrin).

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^{o} 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] X. BONNETAIN. *Hidden Structures and Quantum Cryptanalysis*, Sorbonne Université, November 2019, https://tel.archives-ouvertes.fr/tel-02400328

[12] T. DEBRIS-ALAZARD. *Code-based Cryptography: New Approaches for Design and Proof ; Contribution to Cryptanalysis*, Sorbonne Universites, UPMC University of Paris 6, December 2019, https://hal.inria.fr/tel-02424234

[13] A. GROSPELLIER. *Constant Time Decoding of Quantum Expander Codes and Application to Fault-Tolerant Quantum Computation*, Sorbonne universités, November 2019, https://hal.inria.fr/tel-02422585

[14] V. LONDE. *Topological Quantum Error-Correcting Codes beyond dimension 2*, Inria Paris ; Université de bordeaux, December 2019, https://hal.inria.fr/tel-02429868

Articles in International Peer-Reviewed Journals

[15] Z. BAO, I. DINUR, J. GUO, G. LEURENT, L. WANG. *Generic Attacks on Hash Combiners*, in "Journal of Cryptology", 2020, 82 p. , forthcoming [*DOI :* 10.1007/S00145-019-09328-W], https://hal.inria.fr/hal-02424905

[16] J.-F. BIASSE, X. BONNETAIN, B. PRING, A. SCHROTTENLOHER, W. YOUMANS. *A trade-off between classical and quantum circuit size for an attack against CSIDH*, in "Journal of Mathematical Cryptology", August 2019, pp. 1-16, https://hal.inria.fr/hal-02423394

[17] X. BONNETAIN, M. NAYA-PLASENCIA, A. SCHROTTENLOHER. *Quantum Security Analysis of AES*, in "IACR Transactions on Symmetric Cryptology", June 2019, vol. 2019, n^{o} 2, pp. 55-93 [*DOI :* 10.13154/TOSC.V2019.I2.55-93], https://hal.inria.fr/hal-02397049

[18] C. BOURA, A. CANTEAUT, D. COGGIA. *A General Proof Framework for Recent AES Distinguishers*, in "IACR Transactions on Symmetric Cryptology", March 2019, vol. 2019, n^{o} 1, pp. 170-191 [*DOI :* 10.13154/TOSC.V2019.I1.170-191], https://hal.inria.fr/hal-02431695

[19] C. BOURA, A. CANTEAUT, J. JEAN, V. SUDER. *Two Notions of Differential Equivalence on Sboxes*, in "Designs, Codes and Cryptography", 2019, vol. 87, n^{o} 2-3, pp. 185-202, forthcoming [*DOI :* 10.1007/S10623-018-0496-Z], https://hal.inria.fr/hal-01944565

[20] C. BOURA, E. CHAVLI, M. CHLOUVERAKI, K. KARVOUNIS. *The BMM symmetrising trace conjecture for groups G, G, G, G, G*, in "Journal of Symbolic Computation", 2020, vol. 96, pp. 62-84, https://arxiv.org/abs/1802.07482 [*DOI :* 10.1016/J.JSC.2019.02.012], https://hal.archives-ouvertes.fr/hal-02147376

[21] 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

[22] A. CANTEAUT, L. PERRIN, S. TIAN. *If a generalised butterfly is APN then it operates on 6 bits*, in "Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences ", November 2019, vol. 11, n^{o} 6, pp. 1147-1164 [*DOI :* 10.1007/S12095-019-00361-X], https://hal.inria.fr/hal-02420992

[23] K. CARRIER, J.-P. TILLICH. *Identifying an unknown code by partial Gaussian elimination*, in "Designs, Codes and Cryptography", March 2019, vol. 87, n^{o} 2-3, pp. 685-713 [*DOI :* 10.1007/S10623-018-00593-7], https://hal.inria.fr/hal-02424098

[24] D. CHANG, N. DATTA, A. DUTTA, B. MENNINK, M. NANDI, S. SANADHYA, F. SIBLEYRAS. *Release of Unverified Plaintext: Tight Unified Model and Application to ANYDAE*, in "IACR Transactions on Symmetric Cryptology", 2019, forthcoming, https://hal.inria.fr/hal-02424957

[25] P. CHARPIN, P. LANGEVIN. *Obituary of Jacques Wolfmann (1932–2018)*, in "Designs, Codes and Cryptography", May 2019, vol. 87, n^{o} 5, pp. 955-956 [*DOI :* 10.1007/S10623-019-00631-Y], https://hal-univ-tln.archives-ouvertes.fr/hal-02168222

[26] P. CHARPIN, J. PENG. *Differential uniformity and the associated codes of cryptographic functions*, in "Advances in Mathematics of Communications", November 2019, vol. 13, n° 4, pp. 579-600 [*DOI :* 10.3934/AMC.2019036], https://hal.inria.fr/hal-01908336

[27] 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

[28] S. GHORAI, E. DIAMANTI, A. LEVERRIER. *Composable security of two-way continuous-variable quantum key distribution without active symmetrization*, in "Physical Review A", January 2019, vol. 99, n° 1, 11 p. , https://arxiv.org/abs/1806.11356 [*DOI :* 10.1103/PHYSREVA.99.012311], https://hal.archives-ouvertes.fr/hal-02096575

[29] S. GHORAI, P. GRANGIER, E. DIAMANTI, A. LEVERRIER. *Asymptotic security of continuous-variable quantum key distribution with a discrete modulation*, in "Physical Review X", June 2019, vol. 9, n° 2, 11 p. , https://arxiv.org/abs/1902.01317 [*DOI :* 10.1103/PHYSREVX.9.021059], https://hal.archives-ouvertes.fr/hal-02163714

[30] A. KRISHNA, J.-P. TILLICH. *Towards Low Overhead Magic State Distillation*, in "Physical Review Letters", August 2019, vol. 123, n° 7, 4 p. [*DOI :* 10.1103/PHYSREVLETT.123.070507], https://hal.inria.fr/hal-02424053

[31] *Best Paper*
L. PERRIN. *Partitions in the S-Box of Streebog and Kuznyechik*, in "IACR Transactions on Symmetric Cryptology", March 2019, vol. 2019, n° 1, pp. 302-329 [*DOI :* 10.13154/TOSC.V2019.I1.302-329], https://hal.inria.fr/hal-02396814.

Invited Conferences

[32] A. CANTEAUT. *Algebraic attacks on symmetric primitives for advanced protocols*, in "Frisiacrypt 2019 - Workshop on Symmetric Cryptography", Borkum, Germany, September 2019, https://hal.inria.fr/hal-02431723

[33] A. CANTEAUT. *Cryptanalysis – a Never-Ending Story*, in "Guest lecture for Honorary Doctorate", Bergen, Norway, October 2019, https://hal.inria.fr/hal-02431731

[34] A. CANTEAUT. *Searching for APN permutations with the butterfly construction*, in "CANADAM 2019 - minisymposium on "Finite Fields in Discrete Mathematics"", Vancouver, Canada, May 2019, https://hal.inria.fr/hal-02431757

[35] P. CHARPIN. *Crooked and weakly crooked functions*, in "Fq14 - 14th international conference on Finite Fields and Applications -", Vancouver, Canada, June 2019, https://hal.inria.fr/hal-02431744

[36] A. LEVERRIER, V. LONDE, G. ZÉMOR. *Quantum local testability*, in "Symmetry, Phases of Matter, and Resources in Quantum Computing", Waterloo, Canada, November 2019, https://hal.inria.fr/hal-02432364

[37] M. NAYA-PLASENCIA. *Preparing Symmetric Crypto for the Quantum World*, in "FSE 2019 - 26th Annual Fast Software Encryption Conference", Paris, France, March 2019, https://hal.inria.fr/hal-02424409

[38] M. NAYA-PLASENCIA, A. SCHROTTENLOHER, A. CHAILLOUX, L. GRASSI. *New algorithms for quantum (symmetric) cryptanalysis*, in "QuAC: Quantum Algorithms for Cryptanalysis", Darmstadt, Germany, May 2019, https://hal.inria.fr/hal-02423376

[39] M. NAYA-PLASENCIA, A. SCHROTTENLOHER, A. CHAILLOUX, L. GRASSI. *Quantum Merging Algorithms*, in "Dagstuhl Seminar 19421 Quantum Cryptanalysis", Dagstuhl, Germany, October 2019, https://hal.inria.fr/hal-02423380

[40] F. SIBLEYRAS. *The Missing Difference Problem, and its Applications to Counter Mode Encryption*, in "Invited talk at NTT Secure Platform Laboratories", Musashino, Japan, September 2019, https://hal.inria.fr/hal-02424996

[41] F. SIBLEYRAS. *Low-Memory Attacks Against Two-Round Even-Mansour Using the 3-XOR Problem*, in "Invited talk at NTT Secure Platform Laboratories", Musashino, Japan, September 2020, https://hal.inria.fr/hal-02425000

International Conferences with Proceedings

[42] S. APERS. *Quantum Walk Sampling by Growing Seed Sets*, in "ESA 2019 - 27th Annual European Symposium on Algorithms", Munich/Garching, Germany, September 2019, https://arxiv.org/abs/1904.11446 [*DOI :* 10.4230/LIPICS.ESA.2019.9], https://hal.inria.fr/hal-02436629

[43] X. BONNETAIN, A. HOSOYAMADA, M. NAYA-PLASENCIA, Y. SASAKI, A. SCHROTTENLOHER. *Quantum Attacks without Superposition Queries: the Offline Simon's Algorithm*, in "ASIACRYPT 2019 - 25th Annual International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, LNCS, Springer, December 2019, vol. 11921, pp. 552-583 [*DOI :* 10.1007/978-3-030-34578-5_20], https://hal.inria.fr/hal-02397056

[44] X. BONNETAIN, L. PERRIN, S. TIAN. *Anomalies and Vector Space Search: Tools for S-Box Analysis*, in "ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, LNCS, Springer, November 2019, vol. 11921, pp. 196-223 [*DOI :* 10.1007/978-3-030-34578-5_8], https://hal.inria.fr/hal-02396738

[45] R. BRICOUT, A. CHAILLOUX, T. DEBRIS-ALAZARD, M. LEQUESNE. *Ternary Syndrome Decoding with Large Weight*, in "SAC 2019 - 26th International Conference Selected Areas in Cryptography", Waterloo, Canada, August 2019, https://hal.inria.fr/hal-02420997

[46] A. CANTEAUT, V. LALLEMAND, G. LEANDER, P. NEUMANN, F. WIEMER. *Bison: Instantiating the Whitened Swap-Or-Not Construction*, in "Eurocrypt 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Darmstadt, Germany, LNCS, Springer, May 2019, vol. 11478 [*DOI :* 10.1007/978-3-030-17659-4_20], https://hal.inria.fr/hal-02431714

[47] R. CANTO-TORRES, J.-P. TILLICH. *Speeding up decoding a code with a non-trivial automorphism group up to an exponential factor*, in "ISIT 2019 - IEEE International Symposium on Information Theory", Paris, France, IEEE, July 2019, pp. 1927-1931 [*DOI :* 10.1109/ISIT.2019.8849628], https://hal.inria.fr/hal-02424101

[48] A. COUVREUR, M. LEQUESNE, J.-P. TILLICH. *Recovering short secret keys of RLCE encryption scheme in polynomial time*, in "PQCrypto 2019 - International Conference on Post-Quantum Cryptography", Chongqing,

China, May 2019, https://arxiv.org/abs/1805.11489 [*DOI :* 10.1007/978-3-030-25510-7_8], https://hal.inria.fr/hal-01959617

[49] *Best Paper*
T. DEBRIS-ALAZARD, N. SENDRIER, J.-P. TILLICH. *Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes*, in "ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, LNCS, Springer, November 2019, vol. 11921, pp. 21-51 [*DOI :* 10.1007/978-3-030-34578-5_2], https://hal.inria.fr/hal-02424057.

[50] O. DUNKELMAN, L. PERRIN. *Adapting Rigidity to Symmetric Cryptography: Towards "Unswerving" Designs*, in "SSR 2019 - Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop", London, Royaume-Uni, ACM Press, November 2019, pp. 69-80 [*DOI :* 10.1145/3338500.3360335], https://hal.inria.fr/hal-02396695

[51] S. DUVAL, G. LEURENT. *Lightweight MACs from Universal Hash Functions*, in "CARDIS 2019 - 18th Smart Card Research and Advanced Application Conference", Prague, Czech Republic, November 2019, https://hal.inria.fr/hal-02424904

[52] G. LEURENT, T. PEYRIN. *From Collisions to Chosen-Prefix Collisions : Application to Full SHA-1*, in "Eurocrypt 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Darmstadt, Germany, LNCS, Springer, April 2019, vol. 11478, pp. 527-555 [*DOI :* 10.1007/978-3-030-17659-4_18], https://hal.inria.fr/hal-02424900

[53] G. LEURENT, F. SIBLEYRAS. *Low-Memory Attacks against Two-Round Even-Mansour using the 3-XOR Problem*, in "CRYPTO 2019 - 39th Annual International Cryptology Conference", Santa Barbara, United States, A. BOLDYREVA, D. MICCIANCIO (editors), LNCS, Springer, August 2019, vol. 11693, pp. 210-235 [*DOI :* 10.1007/978-3-030-26951-7_8], https://hal.inria.fr/hal-02424902

[54] Y. LI, G. LEURENT, M. WANG, W. WANG, G. ZHANG, Y. LIU. *Universal Forgery Attack against GCM-RUP*, in "CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020", San Francisco, United States, February 2020, https://hal.inria.fr/hal-02424899

[55] F. SIBLEYRAS. *Generic Attack on Iterated Tweakable FX Constructions*, in "CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020", San Francisco, United States, February 2020, https://hal.inria.fr/hal-02424953

National Conferences with Proceedings

[56] L. PERRIN, X. BONNETAIN. *Russian Style (Lack of) Randomness*, in "Symposium sur la sécurité des technologies de l'information et des communications", Rennes, France, June 2019, https://hal.inria.fr/hal-02396792

Conferences without Proceedings

[57] C. BOURA, L. PERRIN, S. TIAN. *Boomerang Uniformity of Popular S-box Constructions*, in "WCC 2019 - The Eleventh International Workshop on Coding and Cryptography", Saint-Jacut-de-la-Mer, France, March 2019, https://hal.inria.fr/hal-02420970

[58] A. CANTEAUT, L. PERRIN. *On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting*, in "Fq14 - 14th international conference on Finite Fields and Applications", Vancouver, Canada, June 2019, https://hal.inria.fr/hal-02431739

[59] A. CHAILLOUX. *A note on the Quantum Query Complexity of Permutation Symmetric Functions*, in "QIP 2019 - 22nd Annual Conference on Quantum Information Processing", Boulder, United States, January 2019, https://hal.inria.fr/hal-02427235

[60] A. CHAILLOUX. *A note on the quantum query complexity of permutation symmetric functions*, in "ITCS 2019 - 10th Annual Innovations in Theoretical Computer Science", San Diego, United States, 2019, https://arxiv.org/abs/1810.01790 [*DOI :* 10.4230/LIPICS.ITCS.2019.19], https://hal.inria.fr/hal-01950650

[61] D. COGGIA, A. COUVREUR. *On the security of a Loidreau's rank metric code based encryption scheme*, in "WCC 2019 - The Eleventh International Workshop on Coding and Cryptography", Saint Jacut de la mer, France, March 2019, https://hal.archives-ouvertes.fr/hal-02064465

[62] A. GROSPELLIER, L. GROUÈS, A. KRISHNA, A. LEVERRIER. *Combining Hard and Soft Decoders for Hypergraph Product Codes*, in "QEC19 - 5th International Conference on Quantum Error Correction", London, United Kingdom, July 2019, https://hal.inria.fr/hal-02429542

Scientific Popularization

[63] G. LEURENT, M. NAYA-PLASENCIA. *La fragilité inattendue du chiffrement symétrique dans le monde post-quantique*, in "Interstices", December 2019, https://hal.inria.fr/hal-02425716

Other Publications

[64] S. APERS. *Expansion Testing using Quantum Fast-Forwarding and Seed Sets*, January 2020, https://arxiv.org/abs/1907.02369 - 17 pages, 2 figures; v2: fixed error in Lemma 3, with corresponding modifications, https://hal.inria.fr/hal-02436647

[65] S. APERS, R. DE WOLF. *Quantum Speedup for Graph Sparsification, Cut Approximation and Laplacian Solving*, January 2020, https://arxiv.org/abs/1911.07306 - working paper or preprint, https://hal.inria.fr/hal-02436651

[66] S. APERS, A. GILYÉN, S. JEFFERY. *A Unified Framework of Quantum Walk Search*, January 2020, https://arxiv.org/abs/1912.04233 - working paper or preprint, https://hal.inria.fr/hal-02436653

[67] M. BARDET, P. BRIAUD, M. BROS, P. GABORIT, V. NEIGER, O. RUATTA, J.-P. TILLICH. *An Algebraic Attack on Rank Metric Code-Based Cryptosystems*, October 2019, working paper or preprint, https://hal-unilim.archives-ouvertes.fr/hal-02303015

[68] I. BARDET, A. CAPEL, A. LUCIA, D. PÉREZ-GARCÍA, C. ROUZÉ. *On the modified logarithmic Sobolev inequality for the heat-bath dynamics for 1D systems*, January 2020, https://arxiv.org/abs/1908.09004 - 26 pages, 4 figures, https://hal.archives-ouvertes.fr/hal-02436766

[69] I. BARDET, M. JUNGE, N. LARACUENTE, C. ROUZÉ, D. S. FRANÇA. *Group transference techniques for the estimation of the decoherence times and capacities of quantum Markov semigroups*, January 2020, https://arxiv.org/abs/1904.11043 - 39 pages, 2 figures, https://hal.archives-ouvertes.fr/hal-02436767

[70] A. BARIANT. *Cryptanalysis of Tweakable Block Ciphers and Forkciphers*, École Polytechnique, July 2019, INTERNSHIP REPORT, https://hal.inria.fr/hal-02426441

[71] X. BONNETAIN. *Collisions on Feistel-MiMC and univariate GMiMC*, December 2019, working paper or preprint, https://hal.inria.fr/hal-02400343

[72] X. BONNETAIN. *Improved Low-qubit Hidden Shift Algorithms*, December 2019, https://arxiv.org/abs/1901.11428 - working paper or preprint, https://hal.inria.fr/hal-02400414

[73] R. BRICOUT, A. CHAILLOUX, T. DEBRIS-ALAZARD, M. LEQUESNE. *Ternary Syndrome Decoding with Large Weight*, July 2019, Munich Workshop on Coding and Cryptography (MWCC), Poster, https://hal.inria.fr/hal-02421017

[74] A. CANTEAUT, S. DUVAL, G. LEURENT, M. NAYA-PLASENCIA, L. PERRIN, T. PORNIN, A. SCHROTTENLOHER. *Saturnin: a suite of lightweight symmetric algorithms for post-quantum security*, March 2019, Soumission à la compétition "Lightweight Cryptography" du NIST, https://hal.inria.fr/hal-02436763

[75] A. CHAILLOUX. *DEREC - Développement de la cryptographie relativiste*, October 2019, WISG 2019 - 13ème Workshop Interdisciplinaire sur la Sécurité Globale, Poster, https://hal.inria.fr/hal-02427236

[76] A. CHAILLOUX. *Quantum security of the Fiat-Shamir transform of commit and open protocols*, 2019, https://arxiv.org/abs/1906.05415 - working paper or preprint, https://hal.inria.fr/hal-02427223

[77] P. CHARPIN. *Crooked functions*, October 2019, working paper or preprint, https://hal.inria.fr/hal-02337711

[78] N. DAVID. *Quantum impossible differential attack. Applications to CLEFIA, AES and SKINNY*, MPRI, September 2019, https://hal.inria.fr/hal-02424410

[79] T. DEBRIS-ALAZARD, N. SENDRIER, J.-P. TILLICH. *About Wave Implementation and its Leakage Immunity*, December 2019, working paper or preprint, https://hal.inria.fr/hal-02424231

[80] A. FLOREZ GUTIERREZ. *Improving the key recovery in Linear Cryptanalysis: An application to PRESENT*, UVSQ, September 2019, https://hal.inria.fr/hal-02424413

[81] A. KRISHNA, J.-P. TILLICH. *Magic state distillation with punctured polar codes*, May 2019, https://arxiv.org/abs/1811.03112 - working paper or preprint, https://hal.inria.fr/hal-02120563

[82] A. KRISHNA, J.-P. TILLICH. *Towards low overhead magic state distillation*, May 2019, https://arxiv.org/abs/1811.08461 - working paper or preprint, https://hal.inria.fr/hal-02120564

[83] A. LEVERRIER, V. LONDE, G. ZÉMOR. *Towards local testability for quantum coding*, January 2020, https://arxiv.org/abs/1911.03069 - 38 pages, https://hal.inria.fr/hal-02432360

[84] S. OUZINEB. *Towards the Reverse-Engineering of the CaveTable*, Télécom ParisTech, August 2019, https://hal.inria.fr/hal-02275389

[85] L. PERRIN. *Russian Style (Lack of) Randomness*, December 2019, working paper or preprint, https://hal.inria.fr/hal-02396756

[86] L. PERRIN. *Streebog and Kuznyechik: Inconsistencies in the Claims of their Designers*, July 2019, IETF 105, https://hal.inria.fr/hal-02396671