Activity Report 2016

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:

4. - Security and privacy
4.2. - Correcting codes
4.3. - Cryptography
4.3.1. - Public key cryptography
4.3.2. - Secret key cryptography
7.2. - Discrete mathematics, combinatorics
7.8. - Information theory
7.13. - Quantum algorithms

Other Research Topics and Application Domains:

6.4. - Internet of things
6.5. - Information systems
9.8. - Privacy

1. Members

Research Scientists

Anne Canteaut [Team leader, Inria, Senior Researcher, HDR]
André Chailloux [Inria, Researcher]
Pascale Charpin [Inria, Senior Researcher, Emeritus, HDR]
Gaëtan Leurent [Inria, Starting Research position]
Anthony Leverrier [Inria, Researcher on leave from Corps des Mines]
María Naya Plasencia [Inria, Researcher]
Nicolas Sendrier [Inria, Senior Researcher, HDR]
Jean-Pierre Tillich [Inria, Senior Researcher, HDR]

PhD Students

Xavier Bonnetain [Univ. Paris VI, from Sept 2016]
Rodolfo Canto Torres [Inria]
Kevin Carrier [Min. de la Défense, from Oct 2016]
Kaushik Chakraborty [Inria]
Julia Chaulet [Thales, granted by CIFRE]
Thomas Debris [Univ. Paris VI, from Aug 2016]
Sébastien Duval [Univ. Paris VI]
Antoine Grospellier [ENS Lyon, from Sep 2016]
Adrien Hauteville [Univ. Limoges]
Virginie Lallemand [Inria, until Oct 2016]
Vivien Londe [Univ. Bordeaux, from Sep 2016]
Yann Rotella [Inria]

Post-Doctoral Fellows

Irene Márquez Corbella [Inria, until Apr 2016]
Nicky Mouha [FWO grant (Belgium), until Jun 2016]

Visiting Scientist

Thomas Peyrin [NTU Singapore, from Feb 2016 until Mar 2016, and June 2016]

Administrative Assistant

Christelle Guiziou [Inria]

Others

Xavier Bonnetain [Inria, internship, from Mar 2016 until Aug 2016]
Rémi Bricout [ENS Paris, internship, from Mar 2016 until Aug 2016]
Vivien Londe [Inria, internship, from Apr 2016 until July 2016]
Thomas Debris [ENS Cachan, internship, from Mar 2016 until Aug 2016]
Ghazal Kachigar [Inria, internship, from Mar 2016 until Sep 2016]

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 very recently, 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:

[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/

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

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

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

4. Application Domains

4.1. Cryptographic primitives

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

4.2. Code Reconstruction

To evaluate the quality of a cryptographic algorithm, it is usually assumed that its specifications are public, as, in accordance with Kerckhoffs principle, it would be dangerous to rely, even partially, on the fact that the adversary does not know those specifications. However, this fundamental rule does not mean that the specifications are known to the attacker. In practice, before mounting a cryptanalysis, it is necessary to strip off the data. This reverse-engineering process is often subtle, even when the data formatting is not concealed on purpose. A typical case is interception: some raw data, not necessarily encrypted, is observed out of a noisy channel. To access the information, the whole communication system has first to be disassembled and every constituent reconstructed. A transmission system actually corresponds to a succession of elements (symbol mapping, scrambler, channel encoder, interleaver...), and there exist many possibilities for each of them. In addition to the "preliminary to cryptanalysis" aspect, there are other links between those problems and cryptology. They share some scientific tools (algorithmics, discrete mathematics, probability...), but beyond that, there are some very strong similarities in the techniques.

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Post-quantum symmetric cryptanalysis

We have been considering the problem of symmetric cryptography in the future environment that will see the arrival of quantum computers. Indeed, this environment will pose a real problem for the majority of asymmetric primitives, but little is known about the implications for the security of symmetric primitives. Confidence in our symmetric primitives is entirely based on our knowledge within the field of cryptanalysis, but in reality, we do not know much about the symmetric post-quantum attacks. If we want post-quantum systems to be reliable and efficient, we need to understand how adversaries might exploit this new computing power. This year, two preliminary results have been obtained within the team and published at CRYPTO 2016 [51] and in the *IACR Transactions on Symmetric Cryptology* [23]. They include surprising results demonstrating that, in some scenarios, some symmetric systems can also become vulnerable to the quantum computer. Recently María Naya-Plasencia has been awarded an ERC starting grant, QUASYModo, to work on this subject. This grant will enable us to continue this work in more depth.

5.1.2. Real-word impact of some theoretical cryptanalytic works

Weak cryptography can be used long after weaknesses have been found by the academic community. For instance, Rogaway warned that the predictable IV used in TLS was a problem in 2002, but it took a public demonstration with a practical exploit in 2011 (the BEAST attack) for servers and clients to implement countermeasures. The same happened with the use of compression (CRIME), unsecure version fallback (POODLE), and known biases in RC4 (RC4NOMORE), to name a few examples. In joint works at NDSS and ACM CCS, K. Bhargavan from the PROSECCO project-team and G. Leurent showed two almost practical attacks against deprecated cryptographic primitives that are still used in real-world applications. The SLOTH attack targeted the use of MD5 in TLS for in-protocol signatures, and the Sweet32 attack targeted the use of 64-bit block ciphers: Blowfish in OpenVPN, and 3DES in TLS. Moreover, the SLOTH attack received a distinguished paper award at NDSS.

5.1.3. Symmetric ciphers for homomorphic encryption schemes

In order to avoid the (extremely) high expansion rate of homomorphic encryption, a solution consists in transmitting to the server the ciphertext c obtained by encrypting m with a symmetric scheme (the corresponding secret key encrypted by the homomorphic cipher is also transmitted). The server then needs to compute m encrypted with the homomorphic scheme from c, i.e. the server needs to homomorphically evaluate the decryption circuit of the symmetric cipher. Hybrid encryption schemes dedicated to this application then require the use of symmetric ciphers with very specific features. Our team has two important contributions on this topic: the design of new appropriate solutions based on stream ciphers [44], and the attack of a cipher proposed by Méaux et al. in this context [48], [32].

5.1.4. Awards

BEST PAPERS AWARDS:

[58]

A. PHESSO, J.-P. TILLICH. *An Efficient Attack on a Code-Based Signature Scheme*, in "Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016", Fukuoka, Japan, T. TAKAGI (editor), Lecture Notes in Computer Science, Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Springer, February 2016, vol. 9606, pp. 86-103 [*DOI :* 10.1007/978-3-319-29360-8_7], https://hal.inria.fr/hal-01289044

[41]

K. BHARGAVAN, G. LEURENT. *Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH*, in "Network and Distributed System Security Symposium – NDSS 2016", San Diego, United States, February 2016 [*DOI :* 10.14722/NDSS.2016.23418], https://hal.inria.fr/hal-01244855

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

7. New Results

7.1. Symmetric cryptology

Participants: Xavier Bonnetain, Anne Canteaut, Pascale Charpin, Sébastien Duval, Virginie Lallemand, Gaëtan Leurent, Nicky Mouha, María Naya Plasencia, Yann Rotella.

7.1.1. Block ciphers

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

- Design and study of a new construction for low-latency block ciphers, named *reflection ciphers*, which generalizes the so-called α-reflection property exploited in PRINCE. This construction aims at reducing the implementation overhead of decryption on top of encryption [13].
- Design of a new permutation for wide-block block ciphers: N. Mouha and S. Gueron have proposed a family of cryptographic permutations, named Simpira, that supports inputs of $128b$ bits, where b is a positive integer [50]. This wide-block permutation is mainly based on the AES round-function. It then achieves a very high throughput on virtually all modern 64-bit processors that have native instructions for AES.
- Analysis of the division property against block ciphers [42], [26]: A. Canteaut, together with C. Boura, gave a new approach to the division property, which has been recently introduced as a distinguishing property on block ciphers. This work provides a simpler and more general view of the division property which allows the attacker to take into account the characteristics of the building-blocks of the cipher. As an illustration, this new approach provides low-data distinguishers against reduced-round Present, which reach a much higher number of rounds than previously known distinguishers of the same type.
- Modes of operation for full disk encryption [52]: L. Khati, N. Mouha and D. Vergnaud have classified various FDE modes of operation according to their security in a setting where there is no space to store additional data, like an IV or a MAC value. They also introduce the notion of a diversifier, which does not require additional storage, but allows the plaintext of a particular sector to be encrypted into different ciphertexts.

7.1.2. Authenticated encryption and MACs

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 recently 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.

Recent results:

- Attack against π-Cipher : G. Leurent and his coauthors have presented a guess-and-determine attack against some variants of the π-Cipher family, which is a second-round candidate to the Caesar competition. More precisely, they showed a key recovery attack with time complexity little higher than $2^{4\omega}$, and low data complexity, against variants of the cipher with ω-bit words, when the internal permutation is reduced to 2.5 rounds out of 3.
- Improved generic attacks against hash-based MAC [20]
- Cryptanalysis of 7 (out of 8) rounds of the Chaskey MAC [54]. This work has led the designers of Chaskey to increase the number of rounds.

7.1.3. 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 (see Section 5.1.3): 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 [44], [30].
- Cryptanalysis of the FLIP family of stream ciphers: S. Duval, V. Lallemand and Y. Rotella have exhibited an attack against a new family of stream ciphers intended for use in Fully Homomorphic Encryption systems, and proposed by Méaux et al. at Eurocrypt 2016 [48], [32]. More precisely, their attack applies to the early version of FLIP. It exploits the structure of the filter function and the constant internal state of the cipher. The proposed algorithm then recovers the secret key for the two instantiations originally proposed by Méaux et al.
- New types of correlation attacks against filter generators: A. Canteaut and Y. Rotella presented a new family of attacks against filter generators, which exploit a change of the primitive root defining the LFSR [45]. Most notably, an attack can often be mounted by considering non-bijective monomial mappings. In this setting, a divide-and-conquer strategy applies, based on a search within a multiplicative subgroup of $\mathbb{F}_{2^n}$ where n is the LFSR length. If the LFSR length is not a prime, a fast correlation involving a shorter LFSR can then be performed.

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

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

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:

- Cryptographic properties of involutions: P. Charpin, together with S. Mesnager and S. Sarkar, has provided a rigorous study of involutions over the finite field of order 2^n which are relevant primitives for cryptographic designs [19]. Most notably, they have focused on the class of involutions defined by Dickson polynomials [61].
- Construction of a new family of permutations over binary fields of dimension $(4k + 2)$ with good cryptographic properties. An interesting property is that this family includes as a specific case the only known APN permutation of an even number of variables [64].
- Construction of cryptographic permutations over finite fields with a sparse representation: P. Charpin, together with N. Cepak and E. Pasalic, exhibited permutations which are derived from sparse functions via linear translators [14].
- New methods for determining the differential spectrum of an Sbox: P. Charpin and G. Kyureghyan have proved that the whole differential spectrum of an Sbox can be determined without examining all derivatives of the mapping, but only the derivatives with respect to an element within a hyperplane [18]. Also, they have proved that, for mappings of a special shape, it is enough to consider the derivatives with respect to all elements within a suitable multiplicative subgroup of $\mathbb{F}_{2^n}$.

7.1.5. Side-channel attacks

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

Recent results:

- Differential fault attack against the block cipher PRIDE [53]: the efficiency of this attack mainly originate from the design of the linear layer of the cipher which relies on the interleaved construction.
- Study of the criteria to quantify the resistance offered by an Sbox to differential power analysis [17]. This work by K. Chakraborty and his coauthors shows that the classical criterion, called transparency order, has many limitations; an alternative definition is then proposed.

7.1.6. Security of Internet protocols

Cryptographic primitives are used to in key-exchange protocols such as TLS, IKE and SSH, to verify the integrity of the exchange. The recent works by K. Bhargavan and G. Leurent show the real-word impact of some recent theoretical cryptanalytic works.

Recent results:

- Impact of hash function collisions on the security of TLS: most practitioners believe that the hash function only need to resist preimage attacks for this use. However, K. Bhargavan and G. Leurent have shown that collisions in the hash function are sufficient to break the integrity of these protocols, and to impersonate some of the parties [41], [34]. Since many protocols still allow the use of MD5 or SHA-1 (for which collision attacks are known), this results in some practical attacks, and extends the real-world impact of the collision attacks against MD5 and SHA-1. This work has already influenced the latest TLS 1.3 draft, and the main TLS libraries are removing support of MD5 signatures.
- Use of block ciphers operating on small blocks: It is well-known that most modes of operation, like CBC, are not secure if the same key is used for encrypting $2^{n/2}$ blocks of plaintext, where n is the block size. But this threat has traditionally been dismissed as impractical, even for 64-bit blocks, since it requires some prior knowledge of the plaintext and even then, it only leaks a few secret bits per gigabyte. In this context, K. Bhargavan and G. Leurent demonstrated two concrete attacks that exploit such short block ciphers [40]. First, they presented an attack on the use of 3DES in HTTPS that can be used to recover a secret session cookie. Second, they showed how a similar attack on Blowfish can be used to recover HTTP BasicAuth credentials sent over OpenVPN connections.

7.2. Code-based cryptography

Participants: Rodolfo Canto Torres, Julia Chaulet, Thomas Debris, Adrien Hauteville, Ghazal Kachigar, Irene Márquez Corbella, Nicolas Sendrier, Jean-Pierre Tillich.

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 particular families of codes,
- addressing new functionalities, like hashing or symmetric encryption.

Recent results:

- J. Chaulet and N. Sendrier are working on the analysis Gallager's bit flipping algorithm for the decoding of QC-MDPC codes. A first outcome is an improved decoder with an adaptative threshold [47]. The ultimate goal of this work is to avoid side-channel attacks on QC-MDPC-McEliece by designing a failure-free constant-time decoder.
- We have started to explore whether generalized Reed-Solomon codes, and more generally MDS codes, can be used in a McEliece cryptosystem. We have first started by a fundamental work about MDS codes by first characterizing which MDS codes can be efficiently decoded with the rather general technique using error correcting pairs [25] We have also studied whether it is possible, if we know only a random generator matrix of a code admitting an error correcting pair, to recover the pair itself [55]. The latter problem is precisely the problem that an attacker wants to solve when he wants to perform a key attack on a McEliece system based on MDS codes admitting an error correcting pair. Finally, we have come up with what we believe to be a viable McEliece scheme based on Reed-Solomon codes by combining them with a generalized $U|U+V$ construction which hides at the same time the algebraic structure and even improves the decoding capacity of the code [57].
- Design of a new code-based stream cipher, named RankSynd, variant of Synd for the rank metric [49] and of the first Identity based Encryption Scheme relying on error correcting codes (paper currently under submission which is joint work of P. Gaborit, A. Hauteville, H. Phan and J.P. Tillich).
- Structural attacks against some variants of the McEliece cryptosystem based on subclasses of alternant/Goppa codes which admit a very compact public matrix, typically quasi-cyclic, quasi-dyadic, or quasi-monoidic matrices [22]. This result is obtained thanks to a new operation on codes called folding that exploits the knowledge of the automorphism group of the code [21].
- Cryptanalysis of a variant of McEliece cryptosystem based on polar codes [38].
- The previous work has been extended by exploring some structural properties of polar codes in [39]. In particular, we have been able to show that these codes have a very large automorphism group and have found an efficient way of counting the number of codewords of low weight.
- Cryptanalysis of all McEliece cryptosystems relying on algebraic geometry codes [73].
- Cryptanalysis of a code-based signature scheme proposed at PQCrypto 2013 by Baldi at al. [58]. This paper has received the best paper award of PQCrypto 2016.
- R. Canto Torres and N. Sendrier have investigated the information-set decoding algorithms applied to the case where the number of errors is sub-linear in the code length [46]. This situation appears in the analysis of the McEliece scheme based on quasi-cyclic Moderate Density Parity Check (MDPC) codes.
- We have also investigated other decoding techniques such as statistical decoding [74] or quantum algorithms [75]. The last work has led to the best known quantum algorithms for decoding a linear code.

7.3. Quantum Information

Participants: Xavier Bonnetain, Rémi Bricout, Kaushik Chakraborty, André Chailloux, Antoine Grospellier, Gaëtan Leurent, Anthony Leverrier, Vivien Londe, María Naya Plasencia, Jean-Pierre Tillich.

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 started in September 2016 on this topic. First, Antoine Grospellier, co-advised by A. Leverrier and O. Fawzi (Ens Lyon), will study 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:

- Introduction of a new class of quantum LDPC codes, “Quantum expander codes”, featuring a simple and very efficient decoding algorithm which can correct arbitrary patterns of errors of size scaling as the square-root of the length of the code. These are the first codes with constant rate for which such an efficient decoding algorithm is known [36], [59].

7.3.2. Quantum cryptography

A recent approach to cryptography takes into account that all interactions occur in a physical world described by the laws of quantum physics. These laws put severe constraints on what an adversary can achieve, and allow for instance to design provably secure key distribution protocols. We study such protocols as well as more general cryptographic primitives such as coin flipping with security properties based on quantum theory.

Recent results:

- A. Chailloux, together with colleagues from IRIF and Jerusalem, established the existence of quantum weak coin flipping with arbitrarily small bias [12].
- A. Chailloux and international collaborators performed an experimental verification of multipartite entanglement in quantum networks [24].
- A. Chailloux and collaborators established the optimal bounds for quantum weak oblivious transfer [15].
- Security analysis of quantum key distribution with continuous variables [35].

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 recently started investigating such questions through the task of bit commitment. In a paper in *Physical Review Letters* in 2015, K. Chakraborty, A. Chailloux and A. Leverrier developed a security proof for a simple and easily implementable protocol that can achieve arbitrarily long commitment times, thereby establishing that relativistic cryptography is a very practical solution.

André Chailloux was awarded an ANR “Jeune chercheur” to develop the field of relativistic cryptography [31].

Recent results:

- R. Bricout and A. Chailloux [70] considered explicit attacks against the relativistic protocol for bit commitment mentioned above and proved that the security analysis published in *Physical Review Letters* 2015 is essentially tight.
- A drawback of the relativistic bit commitment protocol is that it requires that all communications remain perfectly synchronized during the entire commitment time, and a single network failure leads to aborting the protocol. K. Chakraborty, A. Chailloux and A. Leverrier proposed a more robust version of the protocol allowing to deal with such network failures, a required feature in order to implement the protocol in realistic conditions [16], [71].

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 is Grover’s algorithm, which allows for an exhaustive key search in the square root of the normal complexity. For this reason, it is 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. M. Naya Plasencia has recently been awarded an ERC Starting grant for her project named QUASYModo on this topic.

Recent results:

- Differential and linear attacks in the quantum setting: G. Leurent, A. Leverrier and M. Naya Plasencia, in collaboration with M. Kaplan, have obtained some results on quantum versions of differential and linear cryptanalysis [23]. They show that it is usually possible to use quantum computations to obtain a quadratic speed-up for these attacks, but not for all variants. Therefore, the best attack in the classical world does not necessarily lead to the best quantum one.
- Application of Simon’s algorithm to symmetric cryptanalysis [51], [33]: Leurent et al. also proved that several attacks can be dramatically sped up using a quantum procedure known as Simon’s algorithm for finding the period of a function. As a first application, the most widely used modes of operation for authentication and authenticated encryption (e.g. CBC-MAC, PMAC, GMAC, GCM, and OCB) are completely broken in this security model. These quantum attacks are also applicable to many CAESAR candidates: CLOC, AEZ, COPA, OTR, POET, OMD, and Minalpher. Second, Simon’s algorithm can also be applied to slide attacks, leading to an exponential speed-up of a classical symmetric cryptanalysis technique in the quantum model.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Grants with Industry

- **Thales** (02/14 → 01/17)
  Funding for the supervision of Julia Chaulet’s PhD.
  30 kEuros.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- **ANR BLOC** (10/11 → 03/16)
  Design and Analysis of block ciphers dedicated to constrained environments
  ANR program: Ingénierie numérique et sécurité
  Partners: INSA Lyon, Inria (project-team SECRET), University of Limoges (XLIM), CryptoExperts
  446 kEuros
  http://bloc.project.citi-lab.fr
  The BLOC project aims at providing strong theoretical and practical results in the domain of cryptanalysis and design of block ciphers.
- **ANR KISS** (12/11 → 02/16)
  Keep your personal Information Safe and Secure
  ANR program: Ingénierie numérique et sécurité
  Partners: Inria (project-teams SMIS and SECRET), LIRIS, Gemalto, University of Versailles-St Quentin, Conseil Général des Yvelines
  64 kEuros
  The KISS project builds upon the emergence of new portable and secure devices known as Secure Portable Tokens (e.g., mass storage SIM cards, secure USB sticks, smart sensors) combining the security of smart cards and the storage capacity of NAND Flash chips. The idea promoted in KISS is to embed, in such devices, software components capable of acquiring, storing and managing securely personal data.
- **ANR BRUTUS** (10/14 → 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 → 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.

9.1.2. Others

- **DGA-MI** (09/15 → 09/16)
  Analysis of binary streams: reconstructing LDPC codes.
  28.6 kEuros.
  The objective of this contract was to examine the code reconstruction problem (from noisy observation) for LDPC codes.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: Technische Universiteit Eindhoven (NL)

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universität Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

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

9.2.1.2. QCALL

Title: Quantum Communications for ALL

Programm: H2020-MSCA-ITN-2015

Duration: December 2016 - November 2020

Coordinator: University of Leeds (UK)

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

Inria contact: Anthony Leverrier

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

9.2.2. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: ICT COST Action IC1306

Project title: Cryptography for Secure Digital Interaction

Duration: January 2014 - November 2017

Coordinator: Claudio Orlandi, Aarhus University, Denmark

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

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

Anne Canteaut is co-leader of the working group on cryptographic primitives. She co-organized a 2-day workshop for PhD students and early-career researchers in symmetric cryptography, DISC 2016 (Bochum, Germany, March 23-24 2016).

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Declared Inria International Partners

Title: Discrete Mathematics, Codes and Cryptography

International Partner (Institution - Laboratory - Researcher):

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

Duration: 2014 - 2018

Start year: 2014

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

9.3.1.2. Informal International Partners

- Otto-von-Guericke Universität Magdeburg, Institut für Algebra und Geometrie (Germany):
  Study of Boolean functions for cryptographic applications
- Nanyang Technological University (Singapore): cryptanalysis of symmetric primitives.
- Ruhr-Universität Bochum (Germany): design and cryptanalysis of symmetric primitives.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Leo Perrin, University of Luxemburg, visiting PhD student, June 2016.
- Thomas Peyrin, NTU Singapore, visiting scientist, Feb.-March 2016 and June 2016.

9.4.1.1. Internships

- Xavier Bonnetain, MPRI and Telecom ParisTech, March-Aug. 2016
- Rémi Bricout, MPRI and ENS Paris, March-Aug. 2016
- Thomas Debris, MPRI and ENS Cachan, March-Aug. 2016
- Ghazal Kachigar, Master cryptographie et mathématiques de l'information, Univ. Rennes, March-Sept. 2016
- Vivien Londe, Master de mathématiques, UPMC, April-July 2016

9.4.2. Visits to International Teams

9.4.2.1. Short Research Stays Abroad

- Ruhr-Universität Bochum, Bochum, Germany, January 18-22, work with Gregor Leander (G. Leurent)
- Instituto Superior Tecnico, Lisbon, Portugal, May 18-20, 2016, invitation to visit the group of quantum computation of Paulo Mateus (A. Leverrier)
- University of Oxford Mathematical Institute, Oxford, UK, May 25-26, invitation to the cryptography seminar (G. Leurent)

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- DISC 2016, Workshop for early-career symmetric cryptographers funded by the COST Action IC1306, Bochum, Germany, March 23-24 2016. https://disc2016.compute.dtu.dk/, co-organizer: A. Canteaut.
- Research retreat (H2020 PQCRYPTO), September 21-22, 2016, Inria de Paris, organizer: N. Sendrier

10.1.1.2. Member of the Organizing Committees

- EuroS&P 2017: April 26-28, 2015, Paris (France): G. Leurent (poster chair)

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- FSE 2017: March 5-8, 2017, Tokyo, Japan: M. Naya-Plasencia (co-chair).

10.1.2.2. Member of the Conference Program Committees

- PQCrypto 2016: February 24-26, 2016, Fukuoka, Japan (N. Sendrier, J.P. Tillich)
- CT-RSA 2016: Feb. 29- March 4, 2016, San Francisco, USA (M. Naya Plasencia)
- FSE 2016: March 20-23, 2016, Bochum, Germany (A. Canteaut, G. Leurent)
- Eurocrypt 2016: May 8-12, 2016, Vienna, Austria (M. Naya Plasencia)
- Crypto 2016: August 14-18, 2016, Santa Barbara, USA (A. Canteaut)
- ACISP 2016: July 4-6, 2016, Melbourne, Australia (G. Leurent)

- Waifi 2016: July 13-15, 2016, Ghent, Belgium (A. Canteaut)
- YACC 2016: June 6-10, 2016, Porquerolles Island (A. Canteaut)
- SAC 2016: August 10-12, 2016, St. John's, NL, Canada (G. Leurent, M. Naya-Plasencia)
- Lightsec 2016: September 21-22, 2016, Cappadocia, Turkey (M. Naya-Plasencia)
- Redundancy 2016: September 26-29, 2016, St. Petersburg, Russia (P. Charpin)
- TQC 2016: September 27-29, 2016, Berlin, Germany (A. Chailloux);
- SETA 2016 (International Conference on SequEnces and Their Applications): October 9-14, 2016, Chengdu, China (P. Charpin).
- Asiacrypt 2016: December 4-8, 2016, Hanoi, Vietnam (A. Canteaut)
- Indocrypt 2016: December 11-14, 2016, Kolkata, India (G. Leurent)
- QIP 2017: January 16-20, 2017, Seattle, USA (A. Chailloux, A. Leverrier)
- Financial Crypto 2017: April 3-7, 2017, Sliema, Malta (G. Leurent)
- Fq13: June 4-9, 2017, Geata, Italy (A. Canteaut)
- Crypto 2017: August 20-24, 2017, Santa Barbara, CA, USA (G. Leurent)

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

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

P. Charpin serves as a reviewer for *Mathematical Reviews*.

10.1.3.2. Editor for books or special issues

- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, to appear, editors: P. Charpin, N. Sendrier and J-P. Tillich.
- *Contemporary Developments in Finite Fields and Applications*, 2016, World Scientific Publishing [62], co-editor: A. Canteaut.

10.1.4. Invited Talks

- G. Leurent *Breaking Symmetric Cryptosystems Using Quantum Period Finding*, TCCM-CACR 2016, Yinchuan, China, August 2016
- A. Leverrier, *Quantum Expander Codes*, Beyond i.i.d. in Information Theory, Barcelone, Spain, 18-22 June 2016

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

- A. Canteaut, *Another view of the division property* Dagstuhl seminar on symmetric cryptology, Dagstuhl, Germany, Jan. 10-14, 2016.
- A. Canteaut, *Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression*, CryptoAction Symposium 2016, Budapest, Hungary, April 6-8, 2016.
- A. Canteaut, *Algebraic Distinguishers against Symmetric Primitives*, Paris Crypto Day, France, June 30, 2016.

- A. Canteaut, *Comment concevoir un algorithme de chiffrement sûr et efficace : l'héritage de Shannon*, Shannon 100, workshop organized at the occasion of Shannon's 100th birthday, Institut Henri Poincaré, Paris October 26, 2016. The talk is available online at https://www.youtube.com/watch?v=BYlOO4MkVgU.
- A. Chailloux, *Cryptographie relativiste*, Coding, Cryptography and Algorithms (CCA), Paris, July 1, 2016.
- A. Chailloux, *Quantum Information Processing*, Journées Scientifiques Inria 2016, Rennes, France, June 2016.
- V. Lallemand, *Cryptanalysis of the FLIP Family of Stream Ciphers*, Paris Crypto Day, Sept. 6, 2016.
- G. Leurent, *Transcript Collision Attacks*, Dagstuhl seminar on symmetric cryptology, Dagstuhl, Germany, Jan. 10-14, 2016.
- A. Leverrier, *Distributing Secret Keys with Quantum Continuous Variables*, Recent Advances in Continuous-variable Quantum Information Theory, Barcelone, Spain, 16-8 April 2016
- M. Naya-Plasencia: *Pourquoi essaie-t-on de casser les fonctions cryptographiques ?*. Colloquium organised by the pre-GDR Sécurité Informatique: Colloque Sécurité informatique CNRS http://colloque-cybersecu.cnrs.fr/. Paris, France, Dec. 9, 2016.
- J.P. Tillich, *Attaining the capacity with Reed-Solomon codes through the $(U|U+V)$ construction and Koetter-Vardy soft decoding*, Journée Claude Shannon, Paris, July 1, 2016.

10.1.5. Leadership within the Scientific Community

- A. Canteaut serves as a chair of the steering committee of *Fast Software Encryption (FSE)*.
- N. Sendrier serves on the steering committee of *Post-quantum cryptography (PQCrypto)*.
- M. Naya Plasencia serves on the steering committee of the *Coding and Cryptography* group of GDR-IM https://crypto.di.ens.fr/c2:main;
- N. Sendrier is a member of the "Comité de pilotage" of the ANR (défi 9);
- Since 2014, JP. Tillich organizes a working group on code-based cryptography which meets on a monthly/bimonthly basis. It gathers people from the project-team, from the GRACE project-team (Inria Saclay), from the University of Limoges, from the University of Rennes and from the University of Rouen who all work on this topic.

10.1.6. Research Administration

- N. Sendrier has been a vice-chair of the "Commission d'Evaluation" at Inria until October 2016;
- A. Canteaut is a member of the "Comité de pilotage" of the Fondation Sciences Mathématiques de Paris;
- M. Naya-Plasencia is a member of *Inria Paris CES Committee* (Comité de suivi doctoral).
- M. Naya-Plasencia is a member of *Inria Paris Scientific Hiring Committee* (Assignement of PhD, post-doctoral and delegation Inria fundings).
- N. Sendrier served on the jury of PEDR CNRS INSII 2016.
- J.-P. Tillich is in charge of "Formation par la recherche" for the Paris Inria center;
- **Committees for the selection of professors, assistant professors and researchers**: Inria Paris Chargés de recherche (A. Canteaut), University Paris 8 assistant professor (A. Canteaut, M. Naya-Plasencia, JP Tillich), Inria Directeurs de recherche (N. Sendrier)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: A. Canteaut, *Introduction to Symmetric Cryptography*, 7 hours, M1, Telecom ParisTech, France;

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

Master: A. Chailloux, *Quantum computing*, 6 hours, M2, University Paris-Diderot (MPRI), France;

Master: N. Sendrier, *Code-based cryptography*, 4.5 hours, M2, University Paris-Diderot (MPRI), France;

Master: N. Sendrier, Information theory, 32 hours, M1, University of Versailles-St Quentin (MINT), France;

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

The members of the project-team also gave advanced lectures to summer schools for PhD students:

- *UbiCrypt Spring School on Symmetric Cryptography*, Bochum, Germany, March 2016: A. Canteaut (9 hours). Some of the lectures are available online.

E-learning

Mooc: I. Marquez-Corbella and N. Sendrier, *Code-based cryptography*, 5 weeks, FUN, Inria, undergraduate and Master's degree students in mathematics or computer science.

Pedagogical resources: https://www.fun-mooc.fr/courses/inria/41006S02/session02/about

10.2.2. Supervision

PhD: Virginie Lallemand, *Cryptanalysis for symmetric cryptography*, University Pierre-et-Marie Curie, October 5, 2016, supervisors: M. Naya-Plasencia and A. Canteaut

PhD in progress: Julia Chaulet, *Study of public-key cryptosystems based on MDPC quasi-cyclic codes*, since February 2014, CIFRE convention with Thales, supervisor: N. Sendrier

PhD in progress: Kaushik Chakraborty, *Position-based Quantum Cryptography*, since October 2014, supervisors: A. Leverrier, J.P. Tillich

PhD in progress: Adrien Hauteville, *Rank-metric-based Cryptosystems*, since October 2014, supervisors: P. Gaborit (Univ. Limoges) and J.-P. Tillich

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

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

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

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

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

10.2.3. Juries

- Mohamed Nidhal Mejri, *Securing Vehicular Networks against Denial of Service attacks*, University Paris 13, May 19, 2016, committee: A. Canteaut;

- Tung Chou *Accelerating Pre- and Post-quantum Cryptography*, TU Eindhoven, The Netherlands, June 26, 2016, committee: N. Sendrier;
- Jean-Marie Le Bars, *Some studies about randomness in Computer Science*, HdR, University of Caen, June 29, 2016, committee: J.P. Tillich (reviewer);
- Tom Douce, *Realistic quantum information processing: from devices to computational models*, Université Paris Diderot, September 9, 2016, committee: A. Leverrier;
- Virginie Lallemand, *Cryptanalysis for symmetric cryptography*, University Pierre-et-Marie Curie, October 5, 2016, committee: M. Naya-Plasencia and A. Canteaut (supervisors)
- Brice Minaud, *Analysis of recent cryptographic primitives*,University of Rennes 1, October 7, 2016, committee: A. Canteaut;
- Pierre Karpmann, *Analysis of symmetric primitives*, University Paris-Saclay, October 18, 2016, committee: A. Canteaut (reviewer);
- Jean-Christophe De Neuville, *Contributions to post-quantum cryptography*, University of Limoges, December 1, 2016, committee: J.P. Tillich (reviewer).
- Zoé Amblard , *Quantum cryptography and applications to spatial communications*, University of Limoges, December 5, 2016, committee: J.P. Tillich (reviewer).
- Qian Guo, *Using coding techniques for attacking post-quantum cryptographic assumptions and systems*, Lund University, Sweden, December 13, 2016, committee: J.P. Tillich.

10.3. Popularization

- Nicolas Sendrier and Jean-Pierre Tillich, *Code-Based Cryptography: New Security Solutions Against a Quantum Adversary*, ERCIM News [67].
- Anne Canteaut gave a talk at the *dotSecurity 2016* conference for developers, at Théâtre des Variétés, Paris, April 2016 http://www.thedotpost.com/2016/05/anne-canteaut-the-struggle-for-secure-cryptography.
- Anne Canteaut gave a talk at *Séminaire général du département d'informatique de l'ENS* for Master students in computer science at ENS Paris, April 13, 2016 http://savoirs.ens.fr/expose.php?id=2516.
- André Chailloux gave a talk entitled *L'ordinateur quantique*, at Journées Art, Cerveau, Futur; Mouans-Sartoux, France, September 2016;
- Anne Canteaut gave a talk on cryptography at lycée Rodin, Paris, February 2, 2016.
- Sébastien Duval gave a talk on cryptography at lycée des 7 Mares, Maurepas, December 2, 2016
- Anne Canteaut has been involved in the AlKindi competition, which is a national competition on cryptanalysis for students in "Seconde" http://www.concours-alkindi.fr/.

  The best teams from Paris have been visiting the SECRET project-team in June 2016 https://www.youtube.com/watch?v=EVLHEOWAORc.
- Julia Chaulet participated to a general-public mediation about the use of mathematics in industry at "Salon Culture & Jeux Mathématiques", Paris, May 28, 2016.
- Yann Rotella hold a stand to explain cryptography at Futur en Seine, Carreau du Temple, Paris, June 12, 2016.

11. Bibliography

Major publications by the team in recent years

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

[2] A. CANTEAUT, M. NAYA-PLASENCIA, B. VAYSSIÈRE. *Sieve-in-the-Middle: Improved MITM Attacks*, in "Advances in Cryptology - CRYPTO 2013, Part I", Lecture Notes in Computer Science, Springer, 2013, vol. 8042, pp. 222–240

[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] 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

[5] P. CHARPIN, G. 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

[6] 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

[7] I. DINUR, G. LEURENT. *Improved Generic Attacks Against Hash-based MACs and HAIFA*, in "Advances in Cryptology - CRYPTO 2014", Santa Barbara, CA, United States, LNCS, Springer, August 2014, vol. 8616 [*DOI :* 10.1007/978-3-662-44371-2_9], https://hal.archives-ouvertes.fr/hal-01086177

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

[9] P. JOUGUET, S. KUNZ-JACQUES, A. LEVERRIER, P. GRANGIER, E. DIAMANTI. *Experimental demonstration of long-distance continuous-variable quantum key distribution*, in "Nature Photonics", 2013, vol. 7, pp. 378-381 [*DOI :* 10.1038/NPHOTON.2013.63], https://hal.archives-ouvertes.fr/hal-00798855

[10] R. MISOCZKI, J.-P. TILLICH, N. SENDRIER, P. S. 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] V. LALLEMAND. *Cryptanalysis of symmetric ciphers*, Université Pierre et Marie Curie - Paris VI, October 2016, https://hal.inria.fr/tel-01405436

Articles in International Peer-Reviewed Journals

[12] D. AHARONOV, A. CHAILLOUX, M. GANZ, I. KERENIDIS, L. MAGNIN. *A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias*, in "SIAM Journal on Computing", May 2016, 48 p. [*DOI :* 10.1137/14096387X], https://hal.inria.fr/hal-01094114

[13] C. BOURA, A. CANTEAUT, L. R. KNUDSEN, G. LEANDER. *Reflection ciphers*, in "Designs, Codes and Cryptography", January 2016, pp. 1-23 [*DOI :* 10.1007/S10623-015-0143-X], https://hal.inria.fr/hal-01237135

[14] N. CEPAK, P. CHARPIN, E. PASALIC. *Permutations via linear translators*, in "Finite Fields and Their Applications", 2017, https://hal.inria.fr/hal-01412487

[15] A. CHAILLOUX, G. GUTOSKI, J. SIKORA. *Optimal bounds for quantum weak oblivious transfer*, in "Chicago Journal of Theoretical Computer Science", September 2016 [*DOI :* 10.4086/CJTCS.2016.013], https://hal.archives-ouvertes.fr/hal-00927537

[16] K. CHAKRABORTY, A. CHAILLOUX, A. LEVERRIER. *Robust Relativistic Bit Commitment*, in "Physical Review A", December 2016 [*DOI :* 10.1103/PHYSREVA.94.062314], https://hal.inria.fr/hal-01409562

[17] K. CHAKRABORTY, S. SARKAR, S. MAITRA, B. MAZUMDAR, D. MUKHOPADHYAY, E. PROUFF. *Redefining the transparency order*, in "Designs, Codes and Cryptography", 2016 [*DOI :* 10.1007/S10623-016-0250-3], https://hal.archives-ouvertes.fr/hal-01399584

[18] P. CHARPIN, G. M. KYUREGHYAN. *On sets determining the differential spectrum of mappings*, in "International journal of information and Coding Theory", 2017, Special issue on the honor of Gerard Cohen, https://hal.inria.fr/hal-01406589

[19] P. CHARPIN, S. MESNAGER, S. SARKAR. *Involutions over the Galois field F2n*, in "IEEE Transactions on Information Theory", 2016, vol. 62, n^{o} 4 [*DOI :* 10.1109/TIT.2016.2526022], https://hal.inria.fr/hal-01272943

[20] I. DINUR, G. LEURENT. *Improved Generic Attacks Against Hash-Based MACs and HAIFA*, in "Algorithmica", November 2016 [*DOI :* 10.1007/S00453-016-0236-6], https://hal.inria.fr/hal-01407953

[21] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, F. DE PORTZAMPARC, J.-P. TILLICH. *Folding Alternant and Goppa Codes with Non-Trivial Automorphism Groups*, in "IEEE Transactions on Information Theory", 2016, vol. 62, n^{o} 1, pp. 184 - 198 [*DOI :* 10.1109/TIT.2015.2493539], https://hal.inria.fr/hal-01244609

[22] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, F. DE PORTZAMPARC, J.-P. TILLICH. *Structural Cryptanalysis of McEliece Schemes with Compact Keys*, in "Designs, Codes and Cryptography", April 2016, vol. 79, n^{o} 1, pp. 87-112 [*DOI :* 10.1007/S10623-015-0036-Z], https://hal.inria.fr/hal-00964265

[23] M. KAPLAN, G. LEURENT, A. LEVERRIER, M. NAYA-PLASENCIA. *Quantum Differential and Linear Cryptanalysis*, in "IACR Transactions on Symmetric Cryptology", 2016, vol. 2016, n^{o} 1, https://hal.inria.fr/hal-01237242

[24] W. MC CUTCHEON, A. PAPPA, B. A. BELL, A. MCMILLAN, A. CHAILLOUX, T. LAWSON, M. S. MAFU, D. MARKHAM, E. DIAMANTI, I. KERENIDIS, J. RARITY, M. TAME. *Experimental verification of multipartite entanglement in quantum networks*, in "Nature Communications", November 2016, vol. 7, 8 p. [*DOI :* 10.1038/NCOMMS13251], https://hal.inria.fr/hal-01409559

[25] I. MÁRQUEZ-CORBELLA, R. PELLIKAAN. *A characterization of MDS codes that have an error correcting pair*, in "Finite Fields and Their Applications", 2016, vol. 40, pp. 224 - 245 [*DOI :* 10.1016/J.FFA.2016.04.004], https://hal.inria.fr/hal-01408412

Invited Conferences

[26] C. BOURA, A. CANTEAUT. *Another view of the division property*, in "Symmetric Cryptography (Dagstuhl Seminar 16021)", Dagstuhl, Germany, January 2016, https://hal.inria.fr/hal-01401320

[27] A. CANTEAUT. *Algebraic Distinguishers against Symmetric Primitives*, in "Paris Crypto Day", Paris, France, June 2016, https://hal.inria.fr/hal-01401286

[28] A. CANTEAUT. *Chiffrer mieux pour (dé)chiffrer plus*, in "Conférence d'Informatique de l'ENS", Paris, France, April 2016, https://hal.inria.fr/hal-01401333

[29] A. CANTEAUT. *Comment concevoir un algorithme de chiffrement sûr et efficace : l'héritage de Shannon*, in "Théorie de l'information : nouvelles frontières (dans le cadre du centenaire de Claude Shannon)", Paris, France, IHP, October 2016, https://hal.inria.fr/hal-01401325

[30] 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 "CryptoAction Symposium 2016", Budapest, Hungary, April 2016, https://hal.inria.fr/hal-01401328

[31] A. CHAILLOUX. *Cryptographie relativiste*, in "CCA 2016", Paris, France, July 2016, https://hal.inria.fr/hal-01409564

[32] V. LALLEMAND. *Cryptanalysis of the FLIP Family of Stream Ciphers*, in "Paris Crypto Day", Paris, France, September 2016, https://hal.inria.fr/hal-01405423

[33] G. LEURENT. *Breaking Symmetric Cryptosystems Using Quantum Period Finding*, in "TCCM-CACR 2016", Yinchuan, China, August 2016, https://hal.inria.fr/hal-01407929

[34] G. LEURENT. *Transcript Collision Attacks*, in "Symmetric Cryptography (Dagstuhl Seminar 16021)", Dagstuhl, Germany, January 2016, https://hal.inria.fr/hal-01407921

[35] A. LEVERRIER. *Distributing Secret Keys with Quantum Continuous Variables*, in "Recent Advances in Continuous-variable Quantum Information Theory", Barcelone, Spain, April 2016, https://hal.inria.fr/hal-01407434

[36] A. LEVERRIER. *Quantum Expander Codes*, in "Beyond i.i.d. in Information Theory", Barcelone, Spain, July 2016, https://hal.inria.fr/hal-01407431

[37] J.-P. TILLICH. *Attaining the capacity with Reed-Solomon codes through the $(U|U+V)$construction and Koetter-Vardy soft decoding*, in "Journée Claude Shannon", Paris, France, François Baccelli, Marc Lelarge, July 2016, https://hal.inria.fr/hal-01413503

International Conferences with Proceedings

[38] M. BARDET, J. CHAULET, V. DRAGOI, A. OTMANI, J.-P. TILLICH. *Cryptanalysis of the McEliece Public Key Cryptosystem based on Polar Codes*, in "Post-Quantum Cryptography - PQCrypto 2016", Fukuoka, Japan, T. TAKAGI (editor), LNCS - Lecture Notes in Computer Science, Springer, February 2016, vol. 9606 [*DOI :* 10.1007/978-3-319-29360-8_9], https://hal.inria.fr/hal-01240856

[39] M. Bardet, V. Dragoi, A. Otmani, J.-P. Tillich. *Algebraic properties of polar codes from a new polynomial formalism*, in "International Symposium on Information Theory ISIT 2016", Barcelona, Spain, July 2016, pp. 230 - 234 [*DOI :* 10.1109/ISIT.2016.7541295], https://hal.inria.fr/hal-01410210

[40] K. Bhargavan, G. Leurent. *On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN*, 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

[41] *Best Paper*
K. Bhargavan, G. Leurent. *Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH*, in "Network and Distributed System Security Symposium – NDSS 2016", San Diego, United States, February 2016 [*DOI :* 10.14722/ndss.2016.23418], https://hal.inria.fr/hal-01244855.

[42] C. Boura, A. Canteaut. *Another View of the Division Property*, in "Crypto 2016 (part I) - 36th Annual International Cryptology Conference", Santa Barbara, United States, Lecture Notes in Computer Science, Springer, August 2016, vol. 9814, pp. 654 - 682 [*DOI :* 10.1007/978-3-662-53018-4_24], https://hal.inria.fr/hal-01401016

[43] C. Boura, A. Chakraborti, G. Leurent, G. Paul, D. Saha, H. Soleimany, V. Suder. *Key Recovery Attack Against 2.5-Round Pi-Cipher*, in "FSE 2016 - 23rd International Conference Fast Software Encryption", Bochum, Germany, T. Peyrin (editor), LNCS - Lecture Notes in Computer Science, Springer, March 2016, vol. 9783, pp. 535 - 553 [*DOI :* 10.1007/978-3-662-52993-5_27], https://hal.inria.fr/hal-01404164

[44] 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 "FSE 2016 : 23rd International Conference on Fast Software Encryption", Bochum, Germany, Fast Software Encryption 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016,, Springer, March 2016, vol. 9783 - LNCS (Lecture Notes in Computer Science), pp. 313-333 [*DOI :* 10.1007/978-3-662-52993-5_16], https://hal.archives-ouvertes.fr/hal-01280479

[45] A. Canteaut, Y. Rotella. *Attacks Against Filter Generators Exploiting Monomial Mappings*, in "Fast Software Encrytion - FSE 2016", Bochum, Germany, Lecture Notes in Computer Science, Springer, March 2016, vol. 9783, pp. 78 - 98 [*DOI :* 10.1007/978-3-662-52993-5_5], https://hal.inria.fr/hal-01401009

[46] R. Canto Torres, N. Sendrier. *Analysis of Information Set Decoding for a Sub-linear Error Weight*, in "Post-Quantum Cryptography - PQCrypto 2016", Fukuoka, Japan, February 2016, https://hal.inria.fr/hal-01244886

[47] J. Chaulet, N. Sendrier. *Worst case QC-MDPC decoder for McEliece cryptosystem*, in "IEEE International Symposium on Information Theory, ISIT 2016", Barcelone, Spain, ISIT 2016, proceedings, July 2016, 5 p. [*DOI :* 10.1109/ISIT.2016.7541522], https://hal.inria.fr/hal-01408633

[48] S. Duval, V. Lallemand, Y. Rotella. *Cryptanalysis of the FLIP Family of Stream Ciphers*, 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. 9814, pp. 457 - 475 [*DOI :* 10.1007/978-3-662-53018-4_17], https://hal.inria.fr/hal-01404145

[49] P. Gaborit, A. Hauteville, J.-P. Tillich. *RankSynd a PRNG Based on Rank Metric*, in "Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016", Fukuoka, Japan, T. Takagi (editor), Lecture Notes in Computer Science, Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Springer, February 2016, vol. 9606, pp. 18-28 [*DOI :* 10.1007/978-3-319-29360-8_2], https://hal.inria.fr/hal-01289338

[50] S. Gueron, N. Mouha. *Simpira v2: A Family of Efficient Permutations Using the AES Round Function*, in "Advances in Cryptology - ASIACRYPT 2016", Hanoi, Vietnam, Lecture Notes in Computer Science, December 2016, vol. 10031, pp. 95-125 [*DOI :* 10.1007/978-3-662-53887-6_4], https://hal.inria.fr/hal-01403414

[51] 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

[52] L. Khati, N. Mouha, D. Vergnaud. *Full Disk Encryption: Bridging Theory and Practice*, in "CT-RSA 2017 - RSA Conference Cryptographers' Track", San Francisco, United States, Lecture Notes in Computer Science, February 2017, 16 p. , https://hal.inria.fr/hal-01403418

[53] B. Lac, M. Beunardeau, A. Canteaut, J. J. A. Fournier, R. Sirdey. *A First DFA on PRIDE: from Theory to Practice*, in "International Conference on Risks and Security of Internet and Systems - CRISIS 2016", Roscoff, France, Lecture Notes in Computer Science, September 2016, https://hal.inria.fr/hal-01401271

[54] G. Leurent. *Improved Differential-Linear Cryptanalysis of 7-Round Chaskey with Partitioning*, in "EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic", Vienna, Austria, M. Fischlin, J.-S. Coron (editors), Springer, May 2016, pp. 344 - 371 [*DOI :* 10.1007/978-3-662-49890-3_14], https://hal.inria.fr/hal-01404221

[55] I. Márquez-Corbella, E. Martínez-Moro. *Betti Numbers and Generalized Hamming Weights*, in "22nd Conference on Applications of Computer Algebra (ACA 2016)", Kassel, Germany, August 2016, https://hal.inria.fr/hal-01409298

[56] I. Márquez-Corbella, R. Pellikaan. *Is it hard to retrieve an error-correcting pair?*, in "22nd Conference on Applications of Computer Algebra (ACA 2016)", Kassel, Germany, August 2016, https://hal.inria.fr/hal-01409299

[57] I. Márquez-Corbella, J.-P. Tillich. *Using Reed-Solomon codes in the $(U \mid U + V)$ construction and an application to cryptography*, in "International Symposium on Information Theory", Barcelona, Spain, July 2016, https://hal.inria.fr/hal-01410201

[58] *Best Paper*
A. PHESSO, J.-P. TILLICH. *An Efficient Attack on a Code-Based Signature Scheme*, in "Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016", Fukuoka, Japan, T. TAKAGI (editor), Lecture Notes in Computer Science, Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Springer, February 2016, vol. 9606, pp. 86-103 [*DOI :* 10.1007/978-3-319-29360-8_7], https://hal.inria.fr/hal-01289044.

Conferences without Proceedings

[59] A. LEVERRIER, J.-P. TILLICH, G. ZÉMOR. *Quantum Expander Codes*, in "19th International Conference on Quantum Information Processing", Banff, Canada, January 2016, https://hal.inria.fr/hal-01244685

[60] J.-P. TILLICH. *Attaining the capacity with Reed-Solomon codes through the* $(U|U+V)$*construction and Koetter-Vardy soft decoding*, in "CohenFest 2016", Paris, France, July 2016, https://hal.inria.fr/hal-01413506

Scientific Books (or Scientific Book chapters)

[61] P. CHARPIN, S. MESNAGER, S. SARKAR. *Dickson Polynomials that are Involutions*, in "Contemporary Developments in Finite Fields and Their Applications", A. CANTEAUT, G. EFFINGER, S. HUCZYNSKA, D. PANARIO, L. STORME (editors), World Scientific Press, 2016, pp. 22-45 [*DOI :* 10.1142/9789814719261_0003], https://hal.inria.fr/hal-01237332

Books or Proceedings Editing

[62] A. CANTEAUT, G. EFFINGER, S. HUCZYNSKA, D. PANARIO, L. STORME (editors). *Contemporary Developments in Finite Fields and Applications* , World Scientific, August 2016, 362 p. [*DOI :* 10.1142/9762], https://hal.inria.fr/hal-01401266

[63] P. CHARPIN, T. JOHANSSON, G. M. KYUREGHYAN, N. SENDRIER, J.-P. TILLICH (editors). *Special issue on coding and cryptography*, Design, Codes and Cryptography - Special issue on coding and cryptography, Springer, 2016 [*DOI :* 10.1007/s10623-016-0307-3], https://hal.archives-ouvertes.fr/hal-01406954

Research Reports

[64] A. CANTEAUT, S. DUVAL, L. PERRIN. *A generalisation of Dillon's APN permutation with the best known differential and linear properties for all fields of size* 2^{4k+2}, IACR Cryptology ePrint Archive, September 2016, n^{o} 2016/887, 29 p. , https://hal.inria.fr/hal-01401245

Scientific Popularization

[65] A. CANTEAUT. *On the Origin of Trust: Struggle for Secure Cryptography*, in "Dot Security 2016", Paris, France, April 2016, https://hal.inria.fr/hal-01401311

[66] A. CHAILLOUX. *L'ordinateur quantique*, in "Art, cerveau, futur", Mouans Sartoux, France, September 2016, https://hal.inria.fr/hal-01409565

[67] N. SENDRIER, J.-P. TILLICH. *Code-Based Cryptography: New Security Solutions Against a Quantum Adversary*, in "ERCIM News", July 2016, vol. Special Theme Cybersecurity, n^{o} 106, https://hal.archives-ouvertes.fr/hal-01410068

Other Publications

[68] X. Bonnetain. *Cryptanalyse quantique de primitives symétriques*, Télécom ParisTech ; Paris Diderot, September 2016, https://hal.inria.fr/hal-01409206

[69] R. Bricout. *Protocole de mise en gage de bit relativiste*, MPRI, September 2016, https://hal.inria.fr/hal-01419367

[70] R. Bricout, A. Chailloux. *Recursive cheating strategies for the relativistic F_Q bit commitment protocol*, August 2016, working paper or preprint, https://hal.inria.fr/hal-01409563

[71] K. Chakraborty, A. Chailloux, A. Leverrier. *Robust Relativistic Bit Commitment*, October 2016, International Conference for Young Quantum Information Scientists, Poster, https://hal.inria.fr/hal-01409527

[72] K. Chakraborty, A. Chailloux, A. Leverrier. *Robust Relativistic Bit Commitment*, December 2016, working paper or preprint, https://hal.inria.fr/hal-01407421

[73] A. Couvreur, I. Márquez-Corbella, R. Pellikaan. *Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and their subcodes*, March 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01280927

[74] T. Debris. *Décodage Statistique*, MPRI, September 2016, https://hal.inria.fr/hal-01413092

[75] G. Kachigar. *Étude et conception d'algorithmes quantiques pour le décodage de codes linéaires* , Université de Rennes 1, France, September 2016, 127 p. , https://hal.inria.fr/hal-01371018