Activity Report 2015

Project-Team SECRET

Security, Cryptology and Transmissions

RESEARCH CENTER
Paris - Rocquencourt

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
- 7.13. - Quantum algorithms
- 7.2. - Discrete mathematics, combinatorics
- 7.8. - Information theory

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, Emeritus, HdR]
Gaëtan Leurent [Inria, Starting Research position]
Anthony Leverrier [Inria, 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

Rodolfo Canto Torres [Inria, from Sept. 2015]
Kaushik Chakraborty [Inria]
Julia Chaulet [Thales, CIFRE grant]
Sébastien Duval [Univ. Paris VI]
Adrien Hauteville [Univ. Limoges]
Virginie Lallemand [Inria]
Joëlle Roué [Inria, until Oct 2015]
Yann Rotella [Inria, from Oct. 2015]
Audrey Tixier [Min. de la Défense, until Oct 2015]

Post-Doctoral Fellows

Irene Márquez Corbella [Inria, FSMP grant]
Nicky Mouha [FWO grant (Belgium)]

Visiting Scientists

Sumanta Sarkar [ISI Kolkata (India), Feb-Mar. 2015]
Nastja Cepak [visiting PhD student, University of Primoska (Slovenia), from Sep 2015]

Georgi Ivanov [visiting PhD student, Bulgarian Academy of Science, Jan.-Feb 2015]

Administrative Assistant

Christelle Guiziou [Inria]

Others

Victoire Dupont de Dinechin [Inria, Internship, HEC, Jun 2015]
Aurélie Phesso [Inria, Internship, Univ. Bordeaux, from June to Aug. 2015]
Rodolfo Canto Torres [Inria, Intership, Univ. Bordeaux, from March to Aug. 2015]
Yann Rotella [Inria, Internship, MPRI, from March to Sept. 2015]

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 30 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*.

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;

[1] 24 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.

(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.

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. Resistance of equivalent Sboxes to differential and linear attacks

The so-called Sboxes highly influence the security of a block cipher since they are the only nonlinear component in the cipher. It was widely believed that Sboxes which are affine equivalent (i.e., which are the same up to the composition with affine functions) provide the same security level regarding differential and linear cryptanalyses. However, some simulation results on the maximum expected differential probability over two rounds of the AES show that this is not always the case. A. Canteaut and J. Roué [45] have then investigated the effect of affine transformations of the Sbox on the maximal expected differential probability and linear potential over two rounds of a substitution-permutation network, when the diffusion layer is linear over the finite field defined by the Sbox alphabet. They have been able to exhibit different behaviors depending on the choice of the Sbox within a given equivalence class. This includes some unexpected differences: for a given m-bit Sbox, the choice of the basis used for defining the finite field in the description of the linear layer may also affect the value of the two-round MEDP or MELP. They have also shown that the inversion is the mapping within its equivalence class which has the highest two-round MEDP and MELP, independently of the choice of the MDS linear layer. This situation mainly originates from the fact that this Sbox is an involution. This result has been awarded as one of the 3 best papers at Eurocrypt 2015.

5.1.2. 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 might 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 started investigating such questions through the task of bit commitment. In particular, an interesting bit commitment protocol was introduced in 2014 by Lunghi *et al.* and proven secure against arbitrary classical attacks. The drawback however was that the commitment time was quite constrained, as most a few milliseconds. In [16], K. Chakraborty, A. Chailloux and A. Leverrier showed that the same protocol could in fact achieve commitment times that were arbitrarily long, thereby establishing that relativistic cryptography is a very practical solution.

5.1.3. Quantum Expander Codes

In a paper presented at FOCS 2015 [55], A. Leverrier and JP. Tillich, together with G. Zémor, give an efficient decoding algorithm for a certain kind of quantum LDPC codes which provably corrects any pattern of errors of weight proportional to the square-root of the length of the code. The algorithm runs in time linear in the number of qubits, which makes its performance the strongest to date for linear-time decoding of quantum codes. This work can be considered as a further step towards proving that fault tolerant quantum computing is possible by using only a constant multiplicative overhead of additional qubits.

5.1.4. Organization of WCC 2015

The whole project-team has been involved in the organization of the international conference WCC 2015, which was held in Paris (at Institut Henri Poincaré) in April 2015. This was the ninth in the series of biannual workshops on *Coding and Cryptography*. This edition has gathered around 150 participants from many different countries. We received 90 submissions out of which 53 have been selected for presentation at the conference.

5.1.5. Awards

- 1st prize of the Streebog competition [90]
- 2nd prize of the underhanded crypto contest https://underhandedcrypto.com/archive/
- One of the best 3 papers at Eurocrypt 2015 [45]
- Best paper at PQCrypto 2016 [57].

BEST PAPERS AWARDS:

[45]
A. CANTEAUT, J. ROUÉ. *On the behaviors of affine equivalent Sboxes regarding differential and linear attacks*, in "Advances in Cryptology - Eurocrypt 2015 (Part I)", Sofia, Bulgaria, Lecture Notes in Computer Science, Springer, April 2015, vol. 9056, pp. 45-74, https://hal.inria.fr/hal-01104051

6. New Results

6.1. Symmetric cryptology

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

6.1.1. Block ciphers

Most of our work on block ciphers is related to an ANR Project named BLOC. 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 [15], [60].
- Formalization and generic improvements of impossible differential cryptanalysis: our work provides a general framework for impossible differential cryptanalysis including a generic complexity analysis of the optimal attack [36].
- Cryptanalysis of several recently proposed block ciphers which offer an optimal resistance against side-channel attacks in the sense that the cost of Boolean masking is minimized. This includes an attack against Zorro and its variants [39], and an attack against Picaro in the related-key model [44].
- Cryptanalysis of Feistel constructions with secret Sboxes [42].
- Study of the security of the Even-Mansour construction in the multi-key setting [56].

6.1.2. Authenticated encryption

A limitation of all classical block ciphers is that they aim at protecting confidentiality only, while most applications need both encryption and authentication. These two functionalities are provided by using a block cipher like the AES together with an appropriate mode of operation. However, it appears that the most widely-used mode of operation for authenticated encryption, AES-GCM, is not very efficient for high-speed networks. Also, the security of the GCM mode completely collapses when an IV is reused. These severe drawbacks have then motivated an international competition named CAESAR, partly supported by the NIST, which has been recently launched in order to define some new authenticated encryption schemes [4]. Our work related to this competition is then two-fold: G. Leurent and N. Mouha have participated to the design of some CAESAR candidates; Also, the project-team is involved in a national cryptanalytic effort led by the BRUTUS project funded by the ANR.

Recent results:

- Design of new authenticated encryption schemes submitted to the CAESAR competition: SCREAM v3.0 [72] and PRIMATES 2[58]
- Cryptanalysis of the CAESAR candidates: collision attacks [49] against several candidates including AEZ and Marble, attack against LAC [53].

6.1.3. 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:

- Cryptanalysis of the recently proposed lightweight stream cipher Sprout [52], [71].
- New types of correlation attacks against filter generators exploiting the approximation of the filtering function composed with non-bijective monomial mappings [63], [87].
- Design of encryption schemes for efficient homomorphic-ciphertext compression: 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. 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 [78].

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

6.1.4. Hash functions and MACS

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. In this context, we have investigated the security of some of these constructions, in order to determine whether some particular constructions for hash functions may affect the security of the associated MACs.

Recent results:

- Improved generic attacks against hash-based MAC [30], [31]
- Cryptanalysis of 7 (out of 8) rounds of the Chaskey MAC [32]. This work has led the designers of Chaskey to increase the number of rounds [80].
- Attack against the XOR of two hash functions, using complex structures build from collisions [54]. This work by G. Leurent and L. Wang shows that, surprisingly, the construction $H_1(M) \oplus H_2(M)$ with common hash functions H_1 and H_2 (e.g. SHA-256 and BLAKE-256) is actually be less secure than each function on their own.

6.1.5. Security of Internet protocols

Hash functions are used to in key-exchange protocols such as TLS, IKE and SSH, to verify the integrity of the exchange. 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]. Since many protocols still allow the use of MD5 or SHA-1 (for which collision attacks are known), this result 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

6.1.6. 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:

- Definition of an extended criterion for estimating the resistance of a block cipher to differential attacks. This work emphasizes the role played by the affine permutation of the set of 8-bit words which follows the inverse function in the AES [45], [25], [26], [64], [24] (see Section 5.1.1).
- Construction of new Sboxes for lightweight ciphers: A. Canteaut, S. Duval and G. Leurent have investigated several constructions for obtaining good cryptographic Sboxes (especially 8-bit Sboxes) with a low implementation cost [43], [62], [84].
- 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 [47]. Most notably, they have focused on the class of involutions defined by Dickson polynomials [70], [79].

6.2. Code-based cryptography

Participants: Rodolfo Canto Torres, Julia Chaulet, Adrien Hauteville, Irene Márquez Corbella, Aurélie Phesso, 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, 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:

- 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 [20]. This result is obtained thanks to a new operation on codes called folding that exploits the knowledge of the automorphism group of the code [19].
- Cryptanalysis of a variant of McEliece cryptosystem based on polar codes [40], [59].
- Cryptanalysis of a code-based encryption scheme proposed by Baldi *et al.* in the *Journal of Cryptology* [48].
- Cryptanalysis of a code-based signature scheme proposed at PQCrypto 2013 by Baldi at al. [57].
- Improved algorithm for decoding in the rank metric when some additional information about the targeted codeword is provided [51]; this algorithm used together with a folding technique leads to a feasible attack on the LRPC cryptosystem.
- Design on a new code-based stream cipher, named RankSynd, variant of Synd for the rank metric [50].
- In-depth analysis of the complexity of generic decoding algorithms for linear codes [37]. Most notably, 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 based in quasi-cyclic Moderate Density Parity Check (MDPC) codes.

6.3. Quantum Information

Participants: Kaushik Chakraborty, André Chailloux, Anthony Leverrier, Jean-Pierre Tillich.

6.3.1. Quantum codes

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

Recent results:

- A. Leverrier and JP. Tillich, together with G. Zémor, proposed a new class of quantum LDPC codes, “Quantum expander codes”, which feature 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 (see Section 5.1.3) [55], [35], [73].
- Error analysis for Boson Sampling, a simplified model for quantum computation [21]

6.3.2. 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. Leverrier gave the first composable security proof for a continuous-variable quantum key distribution protocol with coherent states [22]. This essentially completes the security analysis of continuous-variable protocols with coherent states, which are by far the most practical protocols relying on continuous variables.
- A. Leverrier and E. Diamanti reviewed the state-of-the-art concerning quantum key distribution with continuous variables [18].
- A. Leverrier and M. Tomamichel gave the most complete security proof of the BB84 protocol to date, including all finite-size effects and a full description of the protocol [89].
- K. Chakraborty and A. Leverrier studied a general family of quantum protocols for position verification and present a new class of attacks based on the Clifford hierarchy that outperform previously known attacks [17].

6.3.3. Quantum correlations and nonlocality

Since the seminal work from Bell in the 60's, it has been known that classical correlations obtained via shared randomness cannot reproduce all the correlations obtained by measuring entangled quantum systems. This impossibility is for instance witnessed by the violation of a Bell inequality and is known under the name of "Quantum Nonlocality". In addition to its numerous applications for quantum cryptography, the study of quantum nonlocality and quantum games has become a central topic in quantum information theory, with the hope of bringing new insights to our understanding of quantum theory.

Recent results:

- Development of a general framework for the study of quantum correlations with combinatorial tools [14]

6.3.4. Relativistic cryptography

(see Section 5.1.2).

6.3.5. 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. G. Leurent, A. Leverrier and M. Naya Plasencia have recently started working in this area in collaboration with M. Kaplan, especially on differential cryptanalysis. Some preliminary results show that counter-intuitive and surprising cases appear: in general, it is not sufficient to consider the best classical attacks and try to "quantize" them if one wants to find the best post-quantum attack [34], [85].

6.4. Reverse-engineering of communication systems

Participants: Nicolas Sendrier, Jean-Pierre Tillich, Audrey Tixier.

Our activity within this domain, whose first aim is to establish the scientific and technical foundations of a discipline which does not exist yet at an academic level, has been supported by some industrial contracts driven by the Ministry of Defense.

Recent results:

- Efficient algorithm for recovering the block interleaver and the convolutional code when several noisy interleaver codewords are given [76], [13].

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Grants with Industry

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

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR BLOC** ($10/11 \rightarrow 03/16$)
  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** ($12/11 \rightarrow 02/16$)
  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 CLE** ($10/13 \rightarrow 12/15$)
  Cryptography from learning with errors
  ANR program: Jeunes Chercheurs, SIMI2
  Coordinator: Vadim Lyubashevsky (Inria, project-team Cascade)
  The aim of this project is to combine algorithmic and algebraic techniques coming from asymmetric and symmetric cryptology in order to improve some attacks and to design some symmetric primitives which have a good resistance to side-channel attacks.

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

8.1.2. Others

- **French Ministry of Defense (**$10/12 \rightarrow 09/15$**)**
  Funding for the supervision of Audrey Tixier's PhD.
  30 kEuros.
- **DGA-MI (**$09/15 \rightarrow 09/16$**)**
  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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

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

8.2.2. 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.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Declared Inria International Partners

Title: Discrete Mathematics, Codes and Cryptography

International Partner (Institution): Indian Statistical Institute, Kolkata (India)

Start year: 2014

This collaboration investigates the three following topics: Quantum information and cryptography; Design and maintenance of primitives for symmetric cryptography; Low-cost cryptography designs from coding theory and combinatorics.

8.3.1.2. 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.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Georgi Ivanov, Bulgarian Academy of Science, Sofia, Bulgaria, visiting PhD student (COST CryptoAction), Jan.-Feb. 2015
- Sumanta Sarkar, ISI Kolkata, India, visiting scientist, Feb.-March 2015
- Dimitrios Simos, SBA Research, Vienna, Austria, visiting scientist, July 2015
- Nastja Cepak, University of Primoska, Koper, Slovenia, visiting PhD student, from Sept. 2015.
- Enes Pasalic, University of Primoska, Koper, Slovenia, visiting scientist, Oct. 2015.

8.4.1.1. Internships

- Rodolfo Canto Torres, Univ. Bordeaux (M2), March-Aug. 2015
- Yann Rotella, MPRI and Telecom ParisTech (M2), March-Sept. 2015
- Aurélie Phesso, Univ. Bordeaux (M1), June-Aug. 2015
- Victoire Dupont de Dinechin, HEC (L3), June 2015

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

- WCC 2015 (Paris, April 13-17, 2015) has been organized by the project-team. The organizing committee is composed of A. Canteaut, G. Leurent, M. Naya Plasencia.
- N. Sendrier, co-organizer of Dagstuhl Seminar 15371, "Quantum Cryptanalysis", September 7-11, 2015, Dagstuhl, Germany.

9.1.1.2. Member of the organizing committees

- Advances in Quantum Cryptography Workshop, AQC 2015: March 23-24, 2015, Paris (France): A. Chailloux and A. Leverrier

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

- WCC 2015: April 13-17, 2015, Paris (France): P. Charpin, N. Sendrier and J.P. Tillich (co-chairs).

9.1.2.2. Member of the conference program committees

- FSE 2015: March 8-11, 2015, Istanbul, Turkey (A. Canteaut, G. Leurent, M. Naya-Plasencia);
- CT-RSA 2015: April 20-24, 2015, San Francisco, USA (M. Naya-Plasencia);
- Eurocrypt 2015: April 26-30, 2015, Sofia, Bulgaria (A. Canteaut);
- Codes, Cryptology, and Information Security - C2SI 2015: May 26-28, 2015, Rabat, Morocco (A. Canteaut).
- Finite Fields and their applications $F_{q^{12}}$, Saratoga, USA, July 13-17, 2015 (A. Canteaut);
- SAC 2015: August 12-14, 2015, Sackville, Canada (M. Naya-Plasencia);
- Crypto 2015: August 16-20, 2015, Santa Barbara, USA (A. Canteaut);
- National workshop on Coding and Cryptography (Journées C2), October 5-9, 2015, La-Londe-Les-Maures, France (M. Naya-Plasencia, JP. Tillich);

- QCrypt 2015, Fifth annual conference on Quantum Cryptography, 28 September - 2 October 2015, Tokyo, Japan (A. Leverrier);
- ICCC 2015, International Conference on Coding and Cryptography, Alger, Algeria, November 2-5, 2015 (P. Charpin)
- Indocrypt 2015: December 6-9, 2015, Bangalore, India (A. Canteaut, G. Leurent)
- IMA-CC 2015, December 15-17, 2015, Oxford, UK (P. Charpin)
- 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 (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)

9.1.3. Journal

9.1.3.1. 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.

9.1.3.2. Guest editor for books or special issues

- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, 2015, co-editors: P. Charpin, N. Sendrier and J-P. Tillich.
- *Contemporary Developments in Finite Fields and Applications*, 2016, World Scientific Publishing, co-editor: A. Canteaut.

9.1.4. Invited talks

- A. Canteaut, *Differential Attacks Against SPN: A Thorough Analysis*, Codes, Cryptology, and Information Security - C2SI 2015, Rabat, Marocco, May 2015.
- G. Leurent, *Generic Attacks against MAC Algorithms*, Selected Areas in Cryptography - SAC 2015, Sackville, Canada, August 2013
- A. Leverrier, *Introduction to Quantum Cryptography*, WIC Symposium on Information Theory in the Benelux Brussels, Belgium, May 2015.
- J.P. Tillich *A survey on decoding quantum LDPC codes*, Quantum Information Processing - QIP 2015, Sydney, Australia, January 2015.

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

- A. Canteaut, *On the behaviors of affine equivalent Sboxes regarding differential and linear attacks*, Early Symmetric Crypto - ESC 2015, Clervaux, Luxemburg, January 2015.
- A. Canteaut, *Sur la résistance aux cryptanalyses différentielles et linéaires*, Journées Codage et Cryptographie 2015, La Londe-les-Maures, France, October 2015.
- A. Chailloux *Arbitrarily long relativistic bit commitment*, QuPa - Quantum Information in Paris, Paris, France, December 2015.
- A. Chailloux *Introduction to Quantum Cryptography*, 9ème Journées Scientifiques de l'Université de Toulon - France, April 2015.
- A. Chailloux *Introduction à l'Informatique Quantique*, ENS Lyon Seminar, France, January 2015.

- G. Leurent, *On cryptanalysis of the Chaskey MAC*, Early Symmetric Crypto - ESC 2015, Clervaux, Luxemburg, January 2015.
- G. Leurent, *Generic Attacks against MAC Algorithms*, Asian Workshop on Symmetric Key Cryptography - ASK 2015, Singapore, September 201
- A. Leverrier, *Quantum differential cryptanalysis*, Dagstuhl Seminar Quantum Cryptanalysis, Dagstuhl, Germany, 7-11 September 2015.
- A. Leverrier, *Quantum expander codes*, QuPa - Quantum information in Paris, France, 7-8 December 2015.
- M. Naya-Plasencia, *On impossible differential attacks*, Early Symmetric Crypto - ESC 2015, Clervaux, Luxemburg, January 2015.
- N. Sendrier, *Best known attacks on code-based cryptosystems: state of the art and perspectives*, DIMACS Workshop on the Mathematics of Post-Quantum Cryptography, Piscataway, USA, January 2015.

9.1.5. 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;
- Since Autumn 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.

9.1.6. Research administration

- N. Sendrier is a vice-chair of the "Commission d'Evaluation" at Inria;
- A. Canteaut is a member of the "Comité de pilotage" of the Fondation Sciences Mathématiques de Paris;
- N. Sendrier is a member of the committee PEDR INS2I (CNRS) 2015
- N. Sendrier is a member of the committee for PhD fundings, EDITE, Commission thématique O (RO, Algo, Calcul et Programmation).
- J.-P. Tillich is in charge of "Formation par la recherche" for the Paris-Rocquencourt Inria center.
- **Committees for the selection of professors, assistant professors and researchers**: Inria Directeurs de recherche (N. Sendrier), Inria Paris-Rocquencourt Chargés de recherche (A. Canteaut), Université Rennes 1 MC (M. Naya Plasencia), Université de Limoges PR (A. Canteaut)
- Inria Jury d'admission, Directeurs de recherche and Chargés de recherche (N. Sendrier)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: A. Canteaut, *Stream ciphers*, 6 hours, M1, Telecom ParisTech, France;

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

Master: A. Canteaut, *Error-correcting codes and applications to cryptology*, 11 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: 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:

- *IACR School on Design and security of cryptographic algorithms and devices*, Sardinia, Italy, Oct. 18-23, 2015: A. Canteaut.

A. Canteaut, M. Naya-Plasencia and JP. Tillich gave several lectures on symmetric cryptography at Thales.

9.2.2. Supervision

PhD: Joëlle Roué, *Analysis of the resistance of block ciphers against linear and differential attacks*, University Pierre-et-Marie Curie, October 14, 2015, supervisor: A. Canteaut

PhD: Audrey Tixier, *Blind identification of error-correcting codes*, University Pierre-et-Marie Curie, October 14, 2015, supervisor: J.P. Tillich

PhD in progress: Virginie Lallemand, *Cryptanalysis for symmetric cryptography*, since October 2013, 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, , 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

9.2.3. Juries

- Martin M. Lauridsen, *Design and Analysis of Symmetric primitives*, Technical University of Denmark (DTU), October 26, 2015, committee: A. Canteaut (reviewer).
- Carl Löndahl, *Some Notes on Code-Based Cryptography*, Lund University, February 6, 2015, committee: N. Sendrier (opponent)
- Joëlle Roué, *Analysis of the resistance of block ciphers against linear and differential attacks*, University Pierre-et-Marie Curie, October 14, 2015, committee: A. Canteaut (supervisor), M. Naya Plasencia.
- Sylvain Ruhault, *Security Analysis for Pseudo-Random Number Generators*, École Normale Supérieure, June 30, 2015, committee: N. Sendrier
- Audrey Tixier, *Blind identification of error-correcting codes*, University Pierre-et-Marie Curie, October 14, 2015, committee: J.P. Tillich (supervisor), N. Sendrier
- Gaël Thomas, *Design and security analysis for constructions in symmetric cryptography*, University of Limoges, May 13, 2015, committee: A. Canteaut (chair).

9.3. Popularization

- André Chailloux published a paper in the general-audience journal *La Recherche*: Calcul quantique sans erreurs.
- Gaëtan Leurent took part to the radio program *Service Public: "Mot de passe partout"*, France Inter, April 2015 http://www.franceinter.fr/emission-service-public-mot-de-passe-partout
- Anne Canteaut gave a talk on cryptography for female students in “Première” and “Terminale” attending the *Girls can code!* week organized at EPITA, August 24-29, 2015 https://gcc.prologin.org/.

10. Bibliography

Major publications by the team in recent years

[1] C. BOURA, A. CANTEAUT. *On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$*, in "IEEE Transactions on Information Theory", 2013, vol. 59, n^{o} 1, pp. 691–702, http://dx.doi.org/10.1109/TIT.2012.2214203

[2] A. CANTEAUT, B. CHEVALLIER-MAMES, A. GOUGET, P. PAILLIER, T. PORNIN, E. BRESSON, C. CLAVIER, T. FUHR, T. ICART, J.-F. MISARSKY, M. NAYA-PLASENCIA, J.-R. REINHARD, C. THUILLET, M. VIDEAU. *Shabal, a Submission to NIST's Cryptographic Hash Algorithm Competition*, October 2008, Submission to NIST

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

[4] A. CHAILLOUX, G. SCARPA. *Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost*, in "ICALP 2014", Copenhague, Denmark, June 2014, pp. 296 - 307 [*DOI :* 10.1007/978-3-662-43948-7_25], https://hal.inria.fr/hal-01094111

[5] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *Divisibility properties of classical binary Kloosterman sums*, in "Discrete Mathematics", June 2009, vol. 309, n° 12, pp. 3975-3984

[6] 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

[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° 2248, pp. 157–174

[8] 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

[9] 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° 6110, pp. 279-298, http://dx.doi.org/10.1007/978-3-642-13190-5_14

[10] 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

[11] 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

[12] J. ROUÉ. *On the resistance of block ciphers to differential and linear cryptanalyses*, UPMC Université Paris VI, October 2015, https://hal.inria.fr/tel-01245102

[13] A. TIXIER. *Blind identification of error correcting codes*, Université Pierre et Marie Curie, October 2015, https://hal.archives-ouvertes.fr/tel-01238629

Articles in International Peer-Reviewed Journals

[14] A. ACIN, T. FRITZ, A. LEVERRIER, A. B. SAINZ. *A Combinatorial Approach to Nonlocality and Contextuality*, in "Communications in Mathematical Physics", January 2015, vol. 334, n° 2, pp. 533-628 [*DOI :* 10.1007/s00220-014-2260-1], https://hal.archives-ouvertes.fr/hal-00931582

[15] C. BOURA, A. CANTEAUT, L. R. KNUDSEN, G. LEANDER. *Reflection ciphers*, in "Designs, Codes and Cryptography", November 2015, pp. 1-23 [*DOI :* 10.1007/s10623-015-0143-x], https://hal.inria.fr/hal-01237135

[16] 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

[17] K. CHAKRABORTY, A. LEVERRIER. *Practical Position-Based Quantum Cryptography*, in "Physical Review A", 2015, vol. 92, n° 5 [*DOI :* 10.1103/PHYSREVA.92.052304], https://hal.inria.fr/hal-01237233

[18] E. DIAMANTI, A. LEVERRIER. *Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations*, in "Entropy", 2015, vol. 17, n° 9, pp. 6072-6092 [*DOI :* 10.3390/E17096072], https://hal.inria.fr/hal-01237232

[19] 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", 2015, vol. 62, n° 1, pp. 184 - 198 [*DOI :* 10.1109/TIT.2015.2493539], https://hal.inria.fr/hal-01244609

[20] 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", January 2015, 26 p. , https://hal.inria.fr/hal-00964265

[21] A. LEVERRIER, R. GARCÍA-PATRÓN. *Analysis of circuit imperfections in BosonSampling*, in "Quantum Information & Computation", April 2015, vol. 15, n° 5-6, pp. 0489-0512, https://hal.archives-ouvertes.fr/hal-00931587

[22] A. LEVERRIER. *Composable security proof for continuous-variable quantum key distribution with coherent states*, in "Physical Review Letters", 2015 [*DOI :* 10.1103/PHYSREVLETT.114.070501], https://hal.inria.fr/hal-01092234

[23] I. MÁRQUEZ-CORBELLA, E. MARTINEZ-MORO, S.-C. EMILIO. *On the ideal associated to a linear code*, in "Accepted for publication in Journal Advances in Mathematics of Communications", November 2015, https://hal.inria.fr/hal-01243389

Invited Conferences

[24] A. CANTEAUT. *Sur la résistance aux cryptanalyses différentielles et linéaires*, in "Journées Codage et Cryptographie 2015", La Londe-les-Maures, France, October 2015, https://hal.inria.fr/hal-01237299

[25] A. CANTEAUT, J. ROUÉ. *Differential Attacks Against SPN: A Thorough Analysis*, in "Codes, Cryptology, and Information Security - C2SI 2015", Rabat, Morocco, Lecture Notes in Computer Science, Springer, May 2015, vol. 9084, pp. 45-62 [*DOI :* 10.1007/978-3-319-18681-8_4], https://hal.inria.fr/hal-01237293

[26] A. CANTEAUT, J. ROUÉ. *On the behaviors of affine equivalent Sboxes regarding differential and linear attacks*, in "Early Symmetric Crypto - ESC 2015", Clervaux, Luxembourg, January 2015, https://hal.inria.fr/hal-01104052

[27] A. CHAILLOUX. *Arbitrarily long relativistic bit commitment*, in "QuPa (Quantum Paris)", Paris, France, December 2015, https://hal.inria.fr/hal-01245257

[28] A. CHAILLOUX. *Introduction to Quantum Cryptography*, in "9eme Journees Scientifiques de l'Universite de Toulon", Toulon, France, April 2015, https://hal.inria.fr/hal-01245258

[29] A. CHAILLOUX. *Introduction à l'Informatique Quantique*, in "Séminaire Informatique de l'ENS Lyon", Lyon, France, January 2015, https://hal.inria.fr/hal-01245259

[30] G. LEURENT. *Generic Attacks against MAC Algorithms*, in "Asian Workshop on Symmetric Key Cryptography - ASK 2015", Singapore, Singapore, September 2015, https://hal.inria.fr/hal-01243175

[31] G. LEURENT. *Generic Attacks against MAC Algorithms*, in "Selected Areas in Cryptography - SAC 2015", Sackville, Canada, August 2015, https://hal.inria.fr/hal-01243151

[32] G. LEURENT. *On cryptanalysis of the Chaskey MAC*, in "Early Symmetric Crypto - ESC 2015", Clervaux, Luxembourg, January 2015, https://hal.inria.fr/hal-01105128

[33] A. LEVERRIER. *Introduction to Quantum Cryptography*, in "36th WIC Symposium on Information Theory in the Benelux", Bruxelles, Belgium, May 2015, https://hal.inria.fr/hal-01237244

[34] A. LEVERRIER. *Quantum differential cryptanalysis*, in "Dagstuhl Seminar 15371 Quantum Cryptanalysis", Dagstuhl, Germany, September 2015, https://hal.inria.fr/hal-01237243

[35] A. LEVERRIER. *Quantum Expander Codes*, in "QuPa (Quantum Paris)", Paris, France, , December 2015, https://hal.inria.fr/hal-01237245

[36] M. NAYA-PLASENCIA. *On impossible differential attacks*, in "Early Symmetric Crypto - ESC 2015", Clervaux, Luxembourg, January 2015, https://hal.inria.fr/hal-01108324

[37] N. SENDRIER. *Best known attacks on code-based cryptosystems: state of the art and perspectives*, in "DIMACS Workshop on The Mathematics of Post-Quantum Cryptography", Piscataway, United States, January 2015, https://hal.inria.fr/hal-01095945

[38] J.-P. TILLICH. *A survey on decoding quantum LDPC codes*, in "Quantum Information Processing - QIP 2015", Sydney, Australia, January 2015, https://hal.archives-ouvertes.fr/hal-01105219

International Conferences with Proceedings

[39] A. BAR-ON, I. DINUR, O. DUNKELMAN, N. KELLER, V. LALLEMAND, B. TSABAN. *Cryptanalysis of SP Networks with Partial Non-Linear Layers*, in "Advances in Cryptology - Eurocrypt 2015", Sofia, Bulgaria, 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, April 2015, pp. 315-342 [*DOI :* 10.1007/978-3-662-46800-5_13], https://hal.inria.fr/hal-01108331

[40] 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, February 2016, https://hal.inria.fr/hal-01240856

[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, https://hal.inria.fr/hal-01244855

[42] A. BIRYUKOV, G. LEURENT, L. PERRIN. *Cryptanalysis of Feistel Networks with Secret Round Functions*, in "Selected Areas in Cryptography - SAC 2015", Sackville, Canada, August 2015, https://hal.inria.fr/hal-01243130

[43] A. CANTEAUT, S. DUVAL, G. LEURENT. *Construction of Lightweight S-Boxes using Feistel and MISTY structures*, in "Selected Areas in Cryptography - SAC 2015", Sackville, Canada, Springer, August 2015, https://hal.inria.fr/hal-01205187

[44] A. CANTEAUT, V. LALLEMAND, M. NAYA-PLASENCIA. *Related-Key Attack on Full-Round PICARO*, in "Selected Areas in Cryptography - SAC 2015", Sackville, Canada, Springer, August 2015, https://hal.inria.fr/hal-01205209

[45] *Best Paper*
A. CANTEAUT, J. ROUÉ. *On the behaviors of affine equivalent Sboxes regarding differential and linear attacks*, in "Advances in Cryptology - Eurocrypt 2015 (Part I)", Sofia, Bulgaria, Lecture Notes in Computer Science, Springer, April 2015, vol. 9056, pp. 45-74, https://hal.inria.fr/hal-01104051.

[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] P. CHARPIN, S. MESNAGER, S. SARKAR. *On involutions of finite fields*, in "International Symposium on Information Theory - ISIT 2015", Hong-Kong, China, June 2015, https://hal.inria.fr/hal-01151196

[48] A. COUVREUR, A. OTMANI, J.-P. TILLICH, V. GAUTHIER-UMANA. *A Polynomial-Time Attack on the BBCRS Scheme*, in "Practice and Theory in Public-Key Cryptography - PKC 2015", Washington, United States, LNCS, March 2015, https://hal.archives-ouvertes.fr/hal-01104078

[49] T. FUHR, G. LEURENT, V. SUDER. *Collision Attacks against CAESAR Candidates*, in "Advances in Cryptology - ASIACRYPT 2015 - Part II", Sofia, Bulgaria, Lecture Notes in Computer Science, April 2015, vol. 9453, 510 p. [*DOI :* 10.1007/978-3-662-48800-3_21], https://hal.inria.fr/hal-01102031

[50] P. GABORIT, A. HAUTEVILLE, J.-P. TILLICH. *RankSynd a PRNG Based on Rank Metric*, in "Post-Quantum Cryptography - PQCrypto 2016", Fukuoka, Japan, Springer Verlag, February 2016, https://hal.inria.fr/hal-01244635

[51] A. HAUTEVILLE, J.-P. TILLICH. *New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem*, in "IEEE International Symposium on Information Theory - ISIT 2015", Hong Kong, China, June 2015, pp. 2747-2751 [*DOI :* 10.1109/ISIT.2015.7282956], https://hal.inria.fr/hal-01244619

[52] V. LALLEMAND, M. NAYA-PLASENCIA. *Cryptanalysis of Full Sprout*, in "Advances in Cryptology - CRYPTO 2015 (Part I)", Santa Barbara, United States, Lecture Notes in Computer Science, Springer, August 2015, vol. 9215, pp. 663-682, https://hal.inria.fr/hal-01237150

[53] G. LEURENT. *Differential Forgery Attack against LAC*, in "Selected Areas in Cryptography - SAC 2015", Sackville, Canada, August 2015, https://hal.inria.fr/hal-01017048

[54] G. LEURENT, L. WANG. *The Sum Can Be Weaker Than Each Part*, in "Advances in Cryptology - Eurocrypt 2015 (Part I) - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Sofia, Bulgaria, E. OSWALD, M. FISCHLIN (editors), Lecture Notes in Computer Science, Springer, April 2015, vol. 9056, pp. 345-367 [*DOI :* 10.1007/978-3-662-46800-5_14], https://hal.inria.fr/hal-01105129

[55] A. LEVERRIER, J.-P. TILLICH, G. ZÉMOR. *Quantum Expander Codes*, in "FOCS 2015 - IEEE Annual Symposium on the Foundations of Computer Science", Berkeley, United States, IEEE, October 2015, pp. 810-824 [*DOI :* 10.1109/FOCS.2015.55], https://hal.inria.fr/hal-01244657

[56] N. MOUHA, A. LUYKX. *Multi-key Security: The Even-Mansour Construction Revisited*, in "Advances in Cryptology - CRYPTO 2015", Santa Barbara, United States, Lecture Notes in Computer Science, Springer, August 2015, vol. 9215, n^{o} 1, pp. 209-223 [*DOI :* 10.1007/978-3-662-47989-6_10], https://hal.inria.fr/hal-01240988

[57] A. PHESSO, J.-P. TILLICH. *An Efficient Attack on a Code-Based Signature Scheme*, in "Post-Quantum Cryptography - PQCrypto 2016", Fukuoka, Japan, T. TAKAGI (editor), Springer , February 2016, https://hal.inria.fr/hal-01244640

Conferences without Proceedings

[58] E. ANDREEVA, B. BILGIN, A. BOGDANOV, A. LUYKX, F. MENDEL, B. MENNINK, N. MOUHA, Q. WANG, K. YASUDA. *PRIMATEs v2.0*, in "DIAC 2015 - Directions in Authenticated Ciphers", Singapore, Singapore, September 2015, https://hal.inria.fr/hal-01241081

[59] M. BARDET, J. CHAULET, V. DRAGOI, A. OTMANI, J.-P. TILLICH. *Etude d'un système de chiffrement de type McEliece à base de codes polaires*, in "Journées Codage et Cryptographie 2015", La Londe-les-Maures, France, October 2015, https://hal.inria.fr/hal-01240843

[60] C. BOURA, A. CANTEAUT, L. R. KNUDSEN, G. LEANDER. *Reflection Ciphers (Extended abstract)*, in "Workshop on Coding and Cryptography - WCC 2015", Paris, France, April 2015, https://hal.inria.fr/hal-01237291

[61] A. CANTEAUT. *Cryptographic S-boxes*, in "IACR School on Design and Security of Cryptographic Algorithms and Devices", Chia Laguna, Italy, October 2015, https://hal.inria.fr/hal-01237302

[62] A. CANTEAUT, S. DUVAL, G. LEURENT. *Construction de S-Boxes à Bas Coût par des Réseaux de Feistel et des réseaux MISTY*, in "Journées Codage et Cryptographie 2015", La Londe-les-Maures, France, October 2015, https://hal.inria.fr/hal-01240845

[63] A. CANTEAUT, Y. ROTELLA. *Attaques exploitant les représentations équivalentes des LFSR filtrés*, in "Journées codage et cryptographie 2015", La Londe-les-Maures, France, October 2015, https://hal.inria.fr/hal-01240743

[64] A. CANTEAUT, J. ROUÉ. *On the Differential Probability of Substitution-Permutation Networks*, in "The 12th International Conference on Finite Fields and Their Applications - Fq12", Saratoga Springs, United States, July 2015, https://hal.inria.fr/hal-01237300

[65] R. CANTO TORRES, N. SENDRIER. *Décodage générique pour des erreurs de poids faible*, in "Journées Codage et Cryptographie 2015", La Londe-les-Maures, France, October 2015, https://hal.inria.fr/hal-01245087

[66] K. CHAKRABORTY, A. CHAILLOUX, A. LEVERRIER. *Arbitrarily long relativistic bit commitment*, in "Journées Codage et Cryptographie 2015", La Londe-les-Maures, France, October 2015, https://hal.inria.fr/hal-01246237

[67] K. CHAKRABORTY, A. CHAILLOUX, A. LEVERRIER. *Arbitrarily long relativistic bit commitment*, in "Journées Informatique Quantique 2015", Grenoble, France, November 2015, https://hal.inria.fr/hal-01246243

[68] K. CHAKRABORTY, A. LEVERRIER. *Attack strategies for position-based quantum cryptography based on the Clifford Hierarchy*, in "QuPa (Quantum Paris)", Paris, France, June 2015, https://hal.inria.fr/hal-01246249

[69] K. CHAKRABORTY, S. SARKAR, S. MAITRA, M. BODHISATWA, M. DEBDEEP, E. PROUFF. *Redefining the Transparency Order*, in "Workshop on Coding and Cryptography - WCC 2015", Paris, France, April 2015, https://hal.inria.fr/hal-01246218

[70] P. CHARPIN, S. MESNAGER, S. SARKAR. *Dickson polynomials that are involutions*, in "Finite Fields and Applications - Fq12 -", Saratoga Springs, United States, July 2015, https://hal.inria.fr/hal-01237342

[71] V. LALLEMAND, M. NAYA-PLASENCIA. *Cryptanalyse de la Version Complète de Sprout*, in "Journées codage et cryptographie 2015", La Londe-les-Maures, France, October 2015, https://hal.inria.fr/hal-01237163

[72] G. LEURENT. *SCREAM v3.0*, in "Directions in Authenticated Ciphers - DIAC 2015", Singapore, Singapore, September 2015, https://hal.inria.fr/hal-01243177

[73] 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

[74] N. MOUHA. *Chaskey: a Lightweight MAC Algorithm for Microcontrollers*, in "NIST Lightweight Cryptography Workshop 2015", Gaithersburg, United States, July 2015, https://hal.inria.fr/hal-01241083

[75] N. MOUHA. *The Design Space of Lightweight Cryptography*, in "NIST Lightweight Cryptography Workshop 2015", Gaithersburg, United States, July 2015, https://hal.inria.fr/hal-01241013

[76] A. TIXIER. *Blind identification of an unknown interleaved convolutional code* , in "IEEE International Symposium on Information Theory - ISIT 2015", Hong-Kong, China, June 2015 [*DOI :* 10.1109/ISIT.2015.7282419], https://hal.archives-ouvertes.fr/hal-01238624

Research Reports

[77] R. BHAUMIK, A. DUTTA, J. GUO, J. JEAN, N. MOUHA, I. NIKOLIĆ. *More Rounds, Less Security?*, Inria Paris Rocquencourt, May 2015, https://hal.inria.fr/hal-01241075

[78] A. CANTEAUT, S. CARPOV, C. FONTAINE, T. LEPOINT, M. NAYA-PLASENCIA, P. PAILLIER, R. SIRDEY. *How to Compress Homomorphic Ciphertexts*, IACR Cryptology ePrint Archive, February 2015, n^{o} 2015/113, 21 p. , https://hal.inria.fr/hal-01237297

[79] P. CHARPIN, S. MESNAGER, S. SARKAR. *Dickson Polynomials that are Involutions*, IACR Cryptology ePrint Archive, 2015, n^{o} 434, https://hal.inria.fr/hal-01237332

[80] N. MOUHA. *Chaskey: a MAC Algorithm for Microcontrollers – Status Update and Proposal of Chaskey-12* –, Inria Paris Rocquencourt, December 2015, https://hal.inria.fr/hal-01242648

Scientific Popularization

[81] A. CANTEAUT. *Introduction à la cryptographie*, in "Girls Can Code!", Le Kremlin-Bicetre, France, August 2015, https://hal.inria.fr/hal-01237306

[82] A. CHAILLOUX. *Calcul Quantique sans erreurs*, July 2015, 2 p. , Article de vulgarisation dans le magasine La Recherche. Numéro 501-502, Juillet - Août 2015, https://hal.inria.fr/hal-01246505

Other Publications

[83] K. CHAKRABORTY, A. LEVERRIER. *Attack strategies for position-based quantum cryptography based on the Clifford Hierarchy*, September 2015, QCrypt 2015, Poster, https://hal.inria.fr/hal-01246251

[84] S. DUVAL. *Étude d'outils cryptographiques*, Telecom ParisTech, January 2015, https://hal.inria.fr/hal-01109071

[85] M. KAPLAN, G. LEURENT, A. LEVERRIER, M. NAYA-PLASENCIA. *Quantum Differential and Linear Cryptanalysis* , December 2015, working paper or preprint, https://hal.inria.fr/hal-01237242

[86] G. LEURENT. *Differential and Linear Cryptanalysis of ARX with Partitioning*, 2015, working paper or preprint, https://hal.inria.fr/hal-01243166

[87] Y. ROTELLA. *Les représentations équivalentes d'un LFSR et leur impact en cryptanalyse*, Télécom ParisTech ; Université Paris Diderot, September 2015, https://hal.inria.fr/hal-01240725

[88] A. TIXIER. *Blind identification of an unknown interleaved convolutional code*, December 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01238628

[89] M. TOMAMICHEL, A. LEVERRIER. *A Rigorous and Complete Proof of Finite Key Security of Quantum Key Distribution* , December 2015, working paper or preprint, https://hal.inria.fr/hal-01237240

References in notes

[90] J. GUO, J. JEAN, G. LEURENT, T. PEYRIN, L. WANG. *The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function*, in "Selected Areas in Cryptography - SAC 2014", Montreal, Canada, Lecture Notes in Computer Science, August 2014, vol. 8781, pp. 195-211 [*DOI :* 10.1007/978-3-319-13051-4_12], https://hal.inria.fr/hal-01093450