Activity Report 2014

Project-Team SECRET

Security, Cryptology and Transmissions

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team SECRET

Keywords: Cryptography, Error Detection And Correction, Information Theory, Security, Privacy, Quantum Physics

Creation of the Project-Team: 2008 July 01.

1. Members

Research Scientists

Anne Canteaut [Team leader, Inria, Senior Researcher, HdR]
André Chailloux [Inria, Researcher]
Pascale Charpin [Emeritus, Senior Researcher, 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

Marion Bellard [Min. de la Défense and Inria, until Jan. 2014]
Kaushik Chakraborty [Inria, from Oct 2014]
Julia Chaulet [Thales, from Feb 2014]
Adrien Hauteville [Univ. Limoges, from October 2014]
Virginie Lallemand [Inria]
Grégory Landais [Univ. Paris VI, until September 2014]
Denise Maurice [Univ. Cergy-Pontoise, until June 2014]
Joëlle Roué [Inria]
Audrey Tixier [Min. de la Défense]
Valentin Suder [Inria, until November 2014]

Post-Doctoral Fellows

Nicky Mouha [FWO grant (Belgium), from July 2014]
Markku-Juhani Saarinen [ERCIM, Nov. 2014]

Administrative Assistant

Christelle Guiziou [Inria]

Others

Kaushik Chakraborty [Inria, Internship, ISI Kolkata, May-June 2014]
Sébastien Duval [Inria, Internship, Telecom Paristech, from July to Dec. 2014]
Adrien Hauteville [Inria, Internship, Univ. Limoges, from March 2014 to August 2014]

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 of the available symmetric and asymmetric primitives have been either threatened by recent progress in cryptanalysis or by the possible invention of a large quantum computer.

In this context, our research work focuses on both families of cryptographic primitives, *symmetric* and *asymmetric* primitives. More precisely, 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 research work is mainly devoted to the design and analysis of cryptographic algorithms, either in the classical or in the quantum setting. Our approach on the previous problems 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.

4. Application Domains

4.1. Domain

Our main application domains are:

- cryptology, including classical cryptology and quantum cryptography,
- error-correcting codes, especially codes for quantum communications and fault-tolerant quantum computing,
- reverse-engineering of communication systems.

5. New Software and Platforms

5.1. New Software

5.1.1. CFS Implementation

Participants: Grégory Landais, Nicolas Sendrier.

https://gforge.inria.fr/projects/cfs-signature/

Reference implementation of parallel CFS (reinforced version of the digital signature scheme CFS [93] due to Matthieu Finiasz [95]). 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.

5.1.2. Collision Decoding

Participants: Grégory Landais, Nicolas Sendrier.

https://gforge.inria.fr/projects/collision-dec/

Implementation of two variants of information set decoding, Stern-Dumer [97], [94] and MMT [96]. 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. This software has the best score for breaking existing publicly available challenges (see http://pqcrypto.org/wild-challenges.html).

6. New Results

6.1. Highlights of the Year

- Rafael Misoczki's PhD thesis on code-based cryptography (defended in November 2013) has been awarded by the Brazilian Society of Computer Science as the best thesis in computer security.
- *Security analysis of some primitives for authentication and authenticated encryption:* authentication is a major functionality in the vast majority of applications. It is usually implemented by a MAC (message authentication code). The main constructions for MAC are based on hash functions, and include the wide-spread HMAC construction. Gaëtan Leurent, together with Itai Dinur, has presented a new generic attack against HMAC when the underlying hash function follows the Haifa construction. This result points out that the hash function in HMAC has to be chosen very carefully and that some of the main families of hash functions may introduce unexpected weaknesses in the associated MAC. Also, the project-team is involved in a national cryptanalytic effort funded by the ANR which aims at evaluating the security of the recently proposed authenticated encryption schemes.
- *Parallel Repetition of Entangled Games:* In a two-player free game G, two cooperating but non communicating players receive inputs taken from two independent probability distributions. Each of them produces an output and they win the game if they satisfy some predicate on their inputs/outputs. The classical (resp. entangled) value of G is the maximum winning probability when the players are allowed to share classical random bits (resp. a quantum state) prior to receiving their inputs. The n-fold parallel repetition of G consists of n instances of G where the parties receive all the inputs at the same time, produce all the outputs at the same time and must win every instance of G. This work by André Chailloux in collaboration with Giannicola Scarpa establishes that the entangled value of the parallel repetition of G decreases exponentially with n, thereby generalizing to the quantum setting Raz's celebrated parallel repetition theorem which is concerned with the classical value of the game. The main tool for proving this result is the introduction of a new information-theoretic quantity: the superposed information cost.

6.2. Symmetric cryptosystems

Participants: Anne Canteaut, Pascale Charpin, Virginie Lallemand, Gaëtan Leurent, María Naya Plasencia, Joëlle Roué, Valentin Suder.

From outside, it might appear that symmetric techniques become obsolete after the invention of public-key cryptography in the mid 1970's. However, they are still widely used because they are the only ones that can achieve some major features like high-speed or low-cost encryption, fast authentication, and efficient hashing. Today, we find symmetric algorithms in GSM mobile phones, in credit cards, in WLAN connections. Symmetric cryptology is a very active research area which is stimulated by a pressing industrial demand for low-cost implementations (in terms of power consumption, gate complexity...). These extremely restricted implementation requirements are crucial when designing secure symmetric primitives and they might be at the origin of some weaknesses. Actually, these constraints seem quite incompatible with the rather complex mathematical tools needed for constructing a provably secure system.

The specificity of our research work is that it considers all aspects in the field, from the practical ones (new attacks, concrete specifications of new systems) to the most theoretical ones (study of the algebraic structure of underlying mathematical objects, definition of optimal objects). But, our purpose is to study these aspects not separately but as several sides of the same domain. Our approach mainly relies on the idea that, in order to guarantee a provable resistance to the known attacks and to achieve extremely good performance, a symmetric cipher must use very particular building blocks, whose algebraic structures may introduce unintended weaknesses. Our research work captures this conflict for all families of symmetric ciphers. It includes new attacks and the search for new building blocks which ensure both a high resistance to the known attacks and a low implementation cost. This work, which combines cryptanalysis and the theoretical study of discrete mathematical objects, is essential to progress in the formal analysis of the security of symmetric systems.

In this context, the very important challenges are the designs of low-cost ciphers and of authenticated encryption schemes. Most teams in the research community are actually working on the design and on the analysis (cryptanalysis and optimization of the performance) of such primitives.

6.2.1. Block ciphers

Even if the security of the current block cipher standard, AES, is not threatened when it is used in a classical context, there is still a need for the design of improved attacks, and for the determination of design criteria which guarantee that the existing attacks do not apply. This notably requires a deep understanding of all previously proposed attacks. Moreover, there is a high demand from the industry of lightweight block ciphers for some constrained environments. Several such algorithms have been proposed in the last few years and their security should be carefully analyzed. Most of our work in this area is related to an ANR Project named BLOC. Our recent results then mainly concern either the analysis and design of lightweight block ciphers, or the in-depth study of the security of the block cipher standard AES.

Recent results:

- Cryptanalysis of several recently proposed lightweight block ciphers. This includes an attack against the full cipher KLEIN-64 [60], an attack against 8 rounds (out of 12) of PRINCE [48], [77], and an attack against Zorro and its variants [74].
- Formalization and generic improvements of impossible differential cryptanalysis: this type of attacks, even if extensively used, remains not fully understood, and it appears that there are numerous applications where mistakes have been discovered or where the attacks lack optimality. Our work then provides a general framework for impossible differential cryptanalysis including a generic complexity analysis of the optimal attack. Using these advances, we have also presented the best known impossible differential attacks against several ciphers including CLEFIA-128, Camellia, LBlock and Simon [46], [76], [75].
- Design of a new family of block ciphers achieving very good software performance, especially on 8-bit microcontrollers. A nice feature of these ciphers is that they offer an optimal resistance against side-channel attacks in the sense that the cost of Boolean masking is minimized [58].
- 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 [24]
- Proposal of a new family of distinguishers against AES-based permutations, named *limited-birthday distinguishers*; these distinguishers exploit some some improved rebound techniques. They have been successfully applied to various AES-based primitives including AES, ECHO, Grøstl, LED, PHOTON and Whirlpool [18].
- Analysis of the differential and linear properties of the AES Superbox [65].

6.2.2. 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 [1]. Our work related to this competition is then two-fold: G. Leurent has participated to the design of a CAESAR candidate named SCREAM. Also, the project-team is involved in a national cryptanalytic effort led by the BRUTUS project funded by the ANR which aims at evaluating the security of all CAESAR candidates.

Recent results:

- Submission of a proposal to the CAESAR competition [88], [67].
- Cryptanalysis of three CAESAR candidates: Wheesht [64], π-cipher [90], LAC [69].

6.2.3. 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, including HMAC, when the hash function follows the Haifa construction [55], [33];
- Attack against Streebog, the new Russian hash function standard: we show that the specific instantiation of the Haifa construction used in Streebog makes it weak against second-preimage attacks [59].

6.2.4. Cryptographic properties and construction of appropriate building blocks

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

For these reasons, we have investigated several families of filtering functions and of S-boxes which are well-suited for their cryptographic properties or for their implementation characteristics. For instance, bent functions, which are the Boolean functions which achieve the highest possible nonlinearity, have been extensively studied in order to provide some elements for a classification, or to adapt these functions to practical cryptographic constructions. We have also been interested in functions with a low differential uniformity (*e.g.*, APN functions), which are the S-boxes ensuring an (almost) optimal resistance to differential cryptanalysis.

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

Recent results:

- Study of the algebraic properties (e.g. the algebraic degree) of the inverses of APN power permutations [19].
- Study of the cryptographic properties, including the degree, the differential uniformity and the size of the image set of permutations of the form $x \mapsto x^s + \gamma \mathsf{Tr}(x^t)$ over a finite field of characteristic two [15]. Since these functions are obtained by slightly modifying a power function, they share similar interesting implementation properties but do not present the weaknesses coming from their structure. In particular, an infinite family of permutations of this form with differential uniformity 4 has been exhibited.
- Definition of an extended criterion for estimating the resistance of a block cipher to differential attacks. Most notably, this new criterion points out the fact that affinely equivalent Sboxes may not provide the same security level regarding differential and linear cryptanalysis. 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 [65].

6.2.5. Symmetric primitives based on lattices

Lattice-based cryptography is an alternative to number-theoretic constructions for public-key cryptography. Lattice-based constructions enjoy a worst-case security reduction to hard lattice problems, and the area is very active, with many new designs offering attractive features.

Recently, this approach has also been used to build symmetric cryptosystems based on lattice problems. While those systems are less efficient than traditional symmetric systems, they are still reasonably efficient, and their security can be related to hard computational problems rather than being only heuristic. In addition, the underlying mathematical structure can offer extra properties such as parallelizability or easy protection against side-channel attacks.

Recent results:

- Design of a family of pseudo-random functions named SPRING which aims to combine the guarantees of security reductions with good performance [44]; implementation of SPRING on FPGA and protection of this hardware implementation against side-channel attacks [47].
- Implementation and side-channel evaluation of the Lapin authentication protocol, based on the LPN problem [57].

6.3. Code-based cryptography

Participants: Julia Chaulet, Adrien Hauteville, Grégory Landais, Nicolas Sendrier, Jean-Pierre Tillich.

Most popular public-key cryptographic schemes rely either on the factorization problem (RSA, Rabin), or on the discrete logarithm problem (Diffie-Hellman, El Gamal, DSA). These systems have evolved and today instead of the classical groups ($\mathbf{Z}/n\mathbf{Z}$) we may use groups on elliptic curves. They allow a shorter block and key size for the same level of security. An intensive effort of the research community has been and is still being conducted to investigate the main aspects of these systems: implementation, theoretical and practical security. It must be noted that these systems all rely on algorithmic number theory. As they are used in most, if not all, applications of public-key cryptography today (and it will probably remain so in the near future), cryptographic applications are thus vulnerable to a single breakthrough in algorithmics or in hardware (a quantum computer can break all those schemes).

Diversity is a way to dilute that risk, and it is the duty of the cryptographic research community to prepare and propose alternatives to the number-theoretic-based systems. The most serious tracks today are lattice-based cryptography (NTRU,...), multivariate cryptography (HFE,...) and code-based cryptography (McEliece encryption scheme,...). All these alternatives are referred to as *post-quantum cryptosystems*, since they rely on difficult algorithmic problems which would not be solved by the coming-up of the quantum computer.

The code-based primitives have been investigated in details within the project-team. 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:

- Cryptanalysis of McEliece system based on Wild Goppa codes from a quadratic finite field extension. This polynomial-time structural attack relies on some filtration of nested subcodes which will reveal the secret algebraic description of the underlying secret code [16], [17].
- Structural cryptanalysis of some variants of McEliece scheme based on alternant codes which have a quasi-cyclic or quasi-dyadic generator matrix [86].
- Cryptanalysis of a variant of the McEliece cryptosystem based on Reed-Solomon codes [16].
- Design of a new variant of McEliece using quasi-cyclic Moderate Density Parity Check (MDPC) codes [39].

6.4. Reverse-engineering of communication systems

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

To assess the quality of a cryptographic algorithm, it is usually assumed that its specifications are public, as, in accordance with Kerckhoffs principle [2], 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, are observed out of a noisy channel. To access the information, the whole communication system has first to be disassembled and every constituent reconstructed. 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:

- Reconstruction of the constellation labelling (i.e. used in the modulator of a communication system) in the presence of errors and when the underlying code is convolutional [10].
- Reconstruction of a convolutional code. This reconstruction technique is based on a new method for detecting whether a given binary sequence is a noisy convolutional codeword obtained from an unknown convolutional code [45].
- Reconstruction of the interleaver of a turbo-code from the knowledge of several noisy codewords [63].

6.5. Quantum information theory

Participants: André Chailloux, Anthony Leverrier, Denise Maurice, Jean-Pierre Tillich.

[2] Kerckhoffs stated that principle in a paper entitled *La Cryptographie militaire*, published in 1883.

The field of Quantum Information and Computation aims at exploiting the laws of quantum physics to manipulate information in radically novel ways. Two main applications come to mind: quantum computers, that offer the promise of solving some problems intractable with classical computers (for instance, factorization); and quantum cryptography, which provides new ways to exchange data in a provably secure fashion.

The main obstacle towards the development of quantum computing is decoherence, a consequence of the interaction of the computer with a noisy environment. We investigate approaches to quantum error-correction as a way to fight against this effect, and we study more particularly some families of quantum error-correcting codes which generalize the best classical codes available today.

Our research also covers quantum cryptography where we study the security of efficient protocols for key distribution or coin flipping, in collaboration with experimental groups. More generally, we investigate how quantum theory severely constrains the action of honest and malicious parties in cryptographic scenarios.

Finally, a promising approach to better understand the possibilities of quantum information consists in studying quantum correlations via the notion of nonlocal games, where different parties need to coordinate to answer some questions, but without communicating. The goal here is to analyze the optimal strategies and to quantify the quantum advantage, i.e. how much sharing an entangled quantum state helps compared to sharing classical randomness.

6.5.1. 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. Our approach for overcoming this problem has been to study whether or not the family of turbo-codes and LDPC codes (and the associated iterative decoding algorithms) have a quantum counterpart.

Recent results:

- Construction of quantum LDPC codes with fixed non-zero rate and a minimum distance which grows proportionally to the square root of the block-length. This greatly improves the previously best known construction whose minimum distance was logarithmic in the block-length [23].
- Design of a decoding algorithm for the family of quantum codes due to Calderbank, Shor and Steane [84].
- Study of quantum error correcting codes with an iterative decoding algorithm [12].
- Error analysis for Boson Sampling, a simplified model for quantum computation [91].

6.5.2. 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:

- Composable security proof for a continuous-variable quantum key distribution protocol with coherent states [92], [71], [70].
- Proof of existence of quantum weak coin flipping with arbitrarily small bias [80].
- Experimental implementation of quantum coin flipping [20].
- Study of connections between quantum encodings, non-locality and quantum cryptography [22].

6.5.3. 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:

- Proof of parallel repetition of entangled games with exponential decay [52],[82],[32].
- Development of a general framework for the study of quantum correlations with combinatorial tools [35].
- New bounds on the quantum value of nonlocal games with graph-theoretical arguments [51].
- Optimal bounds for parity-oblivious random access codes [50].
- Study of Local Orthogonality, a physical principle upper bounding quantum correlations [21].
- Considerations on the notion of dimension of physical systems and its implications for information processing [14].

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **High Tech Communications Services** (09/13 → 09/14)
  Recovering a convolutional encoder followed by a block interleaver
  19 kEuros.

7.2. Bilateral Grants with Industry

- **Thales** (02/14 → 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 → 09/15)
  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 → 12/15)
  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 → 10/17)
  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 → 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 → 09/15)
  Funding for the supervision of Audrey Tixier's PhD.
  30 kEuros.
- **PEPS IQC 2013** (04/13 → 03/14)
  Topology and quantum codes
  coordinated by G. Zémor, Institut de Mathématiques de Bordeaux.
  http://www.cnrs.fr/mi/spip.php?article301
- **PEPS IQC 2013** (04/13 → 03/14)
  Quantum Cryptography and distributed computing
  coordinated by Frédéric Grosshans, Laboratoire Aimé Cotton.
  http://www.cnrs.fr/mi/spip.php?article301

8.2. European Initiatives

8.2.1. 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.

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)

Duration: 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

- Dimitrios Simos, SBA Research, Vienna, Austria, February 9-15, 2014;
- Marco Tomamichel, University of Sydney, Sydney, Australia, September 30-October 9, 2014;
- Markku-Juhani O. Saarinen, Norwegian University of Science and Technology, Norway, November 8-30, 2014;
- Céline Blondeau, Aalto University, Finland, November 12-13, 2014.

8.4.2. Internships

- Kaushik Chakraborty, ISI Kolkata (India), May 15-June 15, 2014
- Sébastien Duval, Telecom ParisTech, July-December 2014
- Adrien Hauteville, Univ. Limoges, March-August 2014

8.4.3. Visits to International Teams

- Simons Institute for the Theory of Computing, Berkeley, California, February - March, *Quantum Hamiltonian Complexity Program*: A. Chailloux and A. Leverrier;
- Université Catholique de Louvain-la-Neuve, Belgium, visiting Franoįs-Xavier Standaert, March 10-11: G. Leurent;
- UAB, Barcelona, Spain, visiting Andreas Winter, October 26 - November 4: A. Chailloux;
- Nanyang Technological University, Singapore, visiting Thomas Peyrin, May 19-June 6: G. Leurent.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. general chair, scientific chair

- 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;
- J.-P. Tillich served as a scientific organizer of the International workshop on quantum LDPC codes, July 14-16, Waterloo (Canada).
- WCC 2015 to be held in Paris, April 13-17, 2015, is organized by the project-team. The organizing committee is composed of A. Canteaut, G. Leurent, M. Naya Plasencia.

9.1.1.2. member of the organizing committee

- QCrypt 2014: September 1-5, Paris (France): A. Leverrier.
- 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 the conference program committee

- 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 committee

- FSE 2014: March 2-5, 2014, London, UK (A. Canteaut);
- Africacrypt 2014: May, 28-30, 2014, Marrakech, Morocco (M. Naya-Plasencia);
- Eurocrypt 2014: May, 11-15, 2014, Copenhagen, Denmark (M. Naya-Plasencia);
- YACC 2014: June, 9-14, 2014, Porquerolles, France (N. Sendrier, J.-P. Tillich);
- ACNS 2014: June 10-13, 2014, Lausanne, Switzerland (A. Canteaut);
- SAC 2014: August 14-15, 2014, Montréal, Canada (A. Canteaut, M. Naya-Plasencia);
- Crypto 2014: August 17-21, 2014, Santa Barbara, USA (M. Naya-Plasencia);
- SCN 2014: September 3-5, 2014, Amalfi, Italy (G. Leurent);
- WAIFI 2014: September 26-28, 2014 (J.-P. Tillich);
- PQCrypto 2014: October 1-3 2014, Waterloo, Canada (N. Sendrier, J.-P. Tillich);
- Latincrypt 2014: September, 17-19, 2014, Florianópolis, Brazil (N. Sendrier);
- SETA 2014: November 24-28, 2014, Melbourne, Australia (P. Charpin);
- Asiacrypt 2014: December 7-11, 2014, China (M. Naya-Plasencia);
- Indocrypt 2014: December 14-17, 2014, New Delhi, India (A. Canteaut).
- 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);
- 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), March 24-28, 2014, Les Sept Laux, France, (M. Naya-Plasencia, J.-P. Tillich).

9.1.3. Journal

9.1.3.1. member of the editorial board

- *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.

9.1.4. Other responsibilities in the national community

- 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 served on the selection committee for "Directeurs de recherche (DR2)" at Inria;
- A. Canteaut served on the selection committee for "chargés de recherche" at the Paris-Rocquencourt Inria research center;
- N. Sendrier served on the selection committee for "chargés de recherche" at the Sophia Antipolis - Méditerranée Inria research center;
- A. Canteaut served on the selection committee for promotion to the position of associate professor at DTU (Denmark);
- A. Canteaut served on the selection committee for promotion to the position of associate professor at ISI Kolkata (India);
- J.-P. Tillich is in charge of "Formation par la recherche" for the Paris-Rocquencourt Inria center.
- A. Chailloux served on the jury for the 2014 Gilles Kahn thesis prize, November 2014, Paris.

9.1.5. Invited talks

- A. Canteaut, *Chiffrements à bas coût : comment chiffrer et déchiffrer avec des opérations similaires*, Journées Nationales du GDR Informatique Mathématique, Paris, France, January 2014.
- A. Chailloux, *Parallel repetition of entangled games via the superposed information cost*, Quantum Information Processing - QIP 2014, Barcelona, Spain, February 2014.
- A. Chailloux, *Parallel repetition of entangled games via the superposed information cost*, Asian Quantum Information Science Conference - AQIS 2014, Tokyo, Japan, August 2014.
- M. Naya Plasencia, *On Lightweight Block Ciphers and Their Security*, Indocrypt 2014, New Delhi, India, December 2014.
- N. Sendrier, *QC-MDPC-McEliece: A public-key code-based encryption scheme based on quasi-cyclic moderate density parity check codes*, Workshop "Post-Quantum Cryptography: Recent Results and Trends", Fukuoka, Japan, November 3-4, 2014.
- 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, NJ, USA, January 12-16, 2015.
- J.P. Tillich, *Recent attacks on McEliece schemes based on Goppa codes*, Yet Another Conference on Cryptography - YACC 2014, Porquerolles Island, France, June 2014;
- J.P. Tillich, *Turning error-reducing quantum turbo codes into error-correcting codes*, Third International Conference on Quantum Error Correction - QEC 14, Zurich, Switzerland, December 2014.

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

- G. Leurent, *New Generic Attacks on Hash-based MACs*, Dagstuhl Seminar 14021 - Symmetric Cryptography, Dagstuhl, Germany, January 2014.
- A. Leverrier, *A combinatorial approach to contextuality*, Meeting on Reliability, Security and Quality Assurance, Bordeaux, France, September 2014.
- A. Chailloux, *Strong connections between quantum encodings, non-locality and quantum cryptography*, Dimension Witness workshop - DIMWIT 2014, Sopot, Poland, June 2014.
- A. Chailloux, *Parallel repetition of entangled games via the superposed information cost*, Workshop on quantum games, Berkeley, U.S.A., February 2014.
- A. Chailloux, *Parallel Repetition of Free Entangled Games: Simplification and Improvements*, PCQC inaugural meeting, Paris, France, August 2014.
- A. Chailloux, *Parallel Repetition of Free Entangled Games: Simplification and Improvements*, Theory Seminar of UAB, Barcelona, Spain, November 2014.

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: 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 several summer schools for PhD students:

- *Design and security of cryptographic algorithms and devices for real-world applications*, Sibenik, Croatia, June 1-6, 2014: A. Canteaut and M. Naya-Plasencia.
- *Post-Quantum Cryptography Summer School*, Waterloo, Ontario, Canada, September 29-30, 2014: N. Sendrier.

9.2.2. Supervision

PhD: Marion Bellard, *Influence of the mapping in the reverse-engineering of a communication systems*, University Pierre-et-Marie Curie, January 30, 2014, supervisor: N. Sendrier

PhD: Grégory Landais, *Implementations of code-based cryptosystems and of their cryptanalyses*, University Pierre-et-Marie Curie, September 18, 2014, supervisor: N. Sendrier

PhD: Denise Maurice, *Quantum error-correcting codes with an efficient decoding algorithm*, University Pierre-et-Marie Curie, June 26, 2014, supervisor: J.-P. Tillich

PhD: Valentin Suder, *Differential properties of permutations and applications in symmetric cryptography*, University Pierre-et-Marie Curie, November 5, 2014, supervisor: P. Charpin

PhD in progress: Virginie Lallemand, *Cryptanalysis for symmetric cryptography*, since October 2013, supervisors: M. Naya-Plasencia and A. Canteaut

PhD in progress: Joëlle Roué, *Security analysis of block ciphers*, since September 2012, supervisor: A. Canteaut

PhD in progress: Audrey Tixier, *Recovering turbo-codes and LDPC codes*, since October 2013, supervisor: J.P. Tillich

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

9.2.3. Juries

- Marion Bellard, *Influence of the mapping in the reverse-engineering of a communication system*, University Pierre-et-Marie Curie, January 30, 2014, committee: N. Sendrier (supervisor) and J.-P. Tillich;
- Nathan Walk, *Continuous Variable Quantum Communication*, The University of Queensland, Australia, March 2014, A. Leverrier (reviewer).
- Florian Caullery, *Polynomials over finite fields for cryptography*, Université Aix-Marseille, May 28, 2014, A. Canteaut (chair);
- Denise Maurice, *Quantum error-correcting codes with an efficient decoding algorithm*, University Pierre-et-Marie Curie, June 26, 2014, committee: J.-P. Tillich (supervisor);
- Deng Tang, *Boolean functions for stream and block-ciphers*, Université Paris 8, July 1, 2014, A. Canteaut (chair);
- Anna Pappa, *Quantum cryptographic primitives in realistic scenarios*, Télécom ParisTech, July 10, committee: J.-P. Tillich;
- Gregory Landais, *Implementations of code-based cryptosystems and of their cryptanalyses*, University Pierre-et-Marie Curie, September 18, 2014, committee: N. Sendrier (supervisor) and J.-P. Tillich;
- Valentin Suder, *Differential properties of permutations and applications in symmetric cryptography*, Université Pierre et Marie Curie, November 5, 2014, P. Charpin (supervisor), A. Canteaut;
- François Arnault, *Contributions in discrete mathematics and cryptographic applications* (Habilitation), University of Limoges, November 12, 2014, committee: J.-P. Tillich (reviewer);
- Marion Candau, *Non Abelian convolutional codes*, University de Bretagne Occidentale, December 9, 2014, committee: J.-P. Tillich (reviewer);
- Gaétan Murat, *Weakly structured error correcting codes for the rank metric with applications to cryptography*, University of Limoges, December 9, 2014, committee: J.P. Tillich (reviewer).
- S. Raizada, *Some Results On Analysis And Implementation Of HC-128 Stream Cipher*, ISI Kolkata (India), January 2015, A. Canteaut (reviewer).

9.3. Popularization

- Anne Canteaut has been invited to give the annual Computer Science Talk for the new students at Ecole Polytechnique, Palaiseau, June 2014 [79].

10. Bibliography

Major publications by the team in recent years

[1] C. Blondeau, B. Gérard, J.-P. Tillich. *Accurate estimates of the data complexity and success probability for various cryptanalyses*, in "Designs, Codes and Cryptography", 2011, vol. 59, n^{o} 1-3, pp. 3–34, http://dx.doi.org/10.1007/s10623-010-9452-2

[2] 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

[3] 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

[4] 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

[5] P. CHARPIN, G. GONG. *Hyperbent functions, Kloosterman sums and Dickson polynomials*, in "IEEE Transactions on Information Theory", September 2008, vol. 54, n^{o} 9, pp. 4230-4238, Regular paper

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

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

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

[9] R. OVERBECK, N. SENDRIER. *Code-based cryptography*, in "Post-Quantum Cryptography", Springer, 2009, pp. 95-145

Publications of the year

Doctoral Dissertations and Habilitation Theses

[10] M. BELLARD. *Influence of the constellation labeling on the recognition of a communication system*, Université Pierre et Marie Curie, January 2014, https://tel.archives-ouvertes.fr/tel-00959782

[11] G. LANDAIS. *Code-based cryptosystems and cryptanalysis implementation*, Université Pierre et Marie Curie, September 2014, https://hal.inria.fr/tel-01097806

[12] D. MAURICE. *Iteratively Decodable Quantum Error-Correcting Codes*, Université Pierre et Marie Curie, June 2014, https://hal.archives-ouvertes.fr/tel-01076833

[13] V. SUDER. *Differential Properties of Permutations and Application in Symmetric Cryptography*, Université Pierre et Marie Curie, November 2014, https://tel.archives-ouvertes.fr/tel-01093026

Articles in International Peer-Reviewed Journals

[14] N. BRUNNER, M. KAPLAN, A. LEVERRIER, P. SKRZYPCZYK. *Dimension of physical systems, information processing, and thermodynamics*, in "New Journal of Physics", December 2014, vol. 16, 123050 [*DOI :* 10.1088/1367-2630/16/12/123050], https://hal.inria.fr/hal-01092228

[15] 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

[16] A. COUVREUR, P. GABORIT, V. GAUTHIER-UMANA, A. OTMANI, J.-P. TILLICH. *Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes*, in "Designs, Codes and Cryptography", 2014, vol. 73, n^{o} 2, pp. 641-666 [*DOI :* 10.1007/S10623-014-9967-Z], https://hal.archives-ouvertes.fr/hal-01096172

[17] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *New identities relating wild Goppa codes*, in "Finite Fields and Their Applications", September 2014, vol. 29, pp. 178-197 [*DOI :* 10.1016/J.FFA.2014.04.007], https://hal.archives-ouvertes.fr/hal-00880994

[18] J. JEAN, M. NAYA-PLASENCIA, T. PEYRIN. *Improved Cryptanalysis of AES-like Permutations*, in "Journal of Cryptology", 2014, pp. 772–798, https://hal.inria.fr/hal-01092270

[19] G. KYUREGHYAN, V. SUDER. *On inversion in Z_{2^n-1}*, in "Finite Fields and Their Applications", January 2014, vol. 25, pp. 234-254, https://hal.archives-ouvertes.fr/hal-00879490

[20] A. PAPPA, P. JOUGUET, T. LAWSON, A. CHAILLOUX, M. LEGRÉ, P. TRINKLER, I. KERENIDIS, E. DIAMANTI. *Experimental plug and play quantum coin flipping*, in "Nature Communications", April 2014, 9 p. [*DOI :* 10.1038/NCOMMS4717], https://hal.inria.fr/hal-01094106

[21] A. B. SAINZ, T. FRITZ, R. AUGUSIAK, J. B. BRASK, R. CHAVES, A. LEVERRIER, A. ACÍN. *Exploring the Local Orthogonality Principle*, in "Physical Review A", 2014, vol. 89, 032117 [*DOI :* 10.1103/PHYSREVA.89.032117], https://hal.archives-ouvertes.fr/hal-00931591

[22] J. SIKORA, A. CHAILLOUX, I. KERENIDIS. *Strong connections between quantum encodings, non-locality and quantum cryptography*, in "Physical Review A", February 2014, 9 p. , https://hal.inria.fr/hal-01093921

[23] J.-P. TILLICH, G. ZÉMOR. *Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength*, in "IEEE Transactions on Information Theory", 2014, vol. 60, n^{o} 2, pp. 1193-1202 [*DOI :* 10.1109/TIT.2013.2292061], https://hal.archives-ouvertes.fr/hal-00931764

Invited Conferences

[24] A. CANTEAUT. *Chiffrements à bas coût : comment chiffrer et déchiffrer avec des opérations similaires*, in "Journées Nationales du GDR Informatique Mathématique", Paris, France, January 2014, https://hal.inria.fr/hal-01092632

[25] A. CANTEAUT. *Cryptographic S-Boxes* , in "Summer School on design and security of cryptographic algorithms and devices for real-world applications", Sibenik, Croatia, June 2014, https://hal.inria.fr/hal-01093333

[26] A. CANTEAUT. *Stream ciphers* , in "Summer school on design and security of cryptographic algorithms and devices for real-world applications", Sibenik, Croatia, June 2014, https://hal.inria.fr/hal-01092636

[27] 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

[28] A. Chailloux. *Parallel repetition of entangled games via the superposed information cost* , in "Workshop on quantum games", Berkeley, United States, Berkeley Simons Institute, February 2014, https://hal.inria.fr/hal-01100011

[29] A. Chailloux. *Parallel Repetition of Free Entangled Games: Simplification and Improvements*, in "Theory Seminar of UAB", Barcelone, Spain, Université Autonome de Barcelone, November 2014, https://hal.inria.fr/hal-01100015

[30] A. Chailloux. *Parallel Repetition of Free Entangled Games: Simplification and Improvements*, in "PCQC inaugural meeting", Paris, France, August 2014, https://hal.inria.fr/hal-01100014

[31] A. Chailloux. *Strong connections between quantum encodings, non-locality and quantum cryptography*, in "Dimension Witness workshop - DIMWIT 2014", Sopot, Poland, June 2014, https://hal.inria.fr/hal-01100007

[32] A. Chailloux, G. Scarpa. *Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost*, in "QIP 2014 - Quantum Information Processing", Barcelona, Spain, February 2014, https://hal.inria.fr/hal-00927544

[33] G. Leurent. *New Generic Attacks on Hash-based MACs*, in "Dagstuhl Seminar 14021 Symmetric Cryptography", Dagstuhl, Germany, January 2014, https://hal.inria.fr/hal-01093543

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

[35] A. Leverrier. *Approche combinatoire pour l'étude des corrélations quantiques*, in "Meeting on Reliability, Security and Quality Assurance", Bordeaux, France, September 2014, https://hal.inria.fr/hal-01094190

[36] M. Naya-Plasencia. *Cryptanalysis of lightweight block ciphers* , in "Summer School on design and security of cryptographic algorithms and devices for real-world applications", Sibenik, Croatia, June 2014, https://hal.inria.fr/hal-01093421

[37] M. Naya-Plasencia. *Dedicated Cryptanalysis of Lightweight Block Ciphers*, in "Summer School on design and security of cryptographic algorithms and devices for real-world applications", Sibenik, Croatia, June 2014, https://hal.inria.fr/hal-01093424

[38] M. Naya-Plasencia. *On Lightweight Block Ciphers and Their Security* , in "Indocrypt 2014", New Delhi, India, December 2014, https://hal.inria.fr/hal-01097348

[39] N. Sendrier. *QC-MDPC-McEliece: A public-key code-based encryption scheme based on quasi-cyclic moderate density parity check codes*, in "Workshop “Post-Quantum Cryptography: Recent Results and Trends”", Fukuoka, Japan, November 2014, https://hal.inria.fr/hal-01095935

[40] 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

[41] J.-P. TILLICH. *Recent attacks on McEliece schemes based on Goppa codes*, in "Yet Another Conference on Cryptography - YACC 2014", Porquerolles, France, June 2014, https://hal.inria.fr/hal-01099816

[42] J.-P. TILLICH. *Turning error-reducing quantum turbo codes into error-correcting codes*, in "Third International Conference on Quantum Error Correction - QEC 2014", zurich, Switzerland, December 2014, https://hal.inria.fr/hal-01099818

[43] J.-P. TILLICH. *A survey on decoding quantum LDPC codes*, in "QIP 2015 - The 18th Conference on Quantum Information Processing", Sydney, Australia, Stephen Bartlett (USYD) (Co-Chair) Gavin Brennen (MQ) (Co-Chair) Gerard J. Milburn (UQ) (Co-Chair) Mingsheng Ying , January 2015, https://hal.archives-ouvertes.fr/hal-01105219

International Conferences with Proceedings

[44] A. BANERJEE, H. BRENNER, G. LEURENT, C. PEIKERT, A. ROSEN. *SPRING: Fast Pseudorandom Functions from Rounded Ring Products*, in "Fast Software Encryption - FSE 2014", Londres, United Kingdom, March 2014, https://hal.inria.fr/hal-01093487

[45] M. BELLARD, J.-P. TILLICH. *Detecting and reconstructing an unknown convolutional code by counting collisions*, in "IEEE International Symposium on Information Theory - ISIT 2014", Honolulu, United States, June 2014, pp. 2967-2971, https://hal.archives-ouvertes.fr/hal-01096175

[46] C. BOURA, M. NAYA-PLASENCIA, V. SUDER. *Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon*, in "Advances in Cryptology - Asiacrypt 2014", Kaoshiung, Taiwan, Lecture Notes in Computer Science, 2014, vol. 8873, pp. 179-199, https://hal.inria.fr/hal-01092274

[47] H. BRENNER, L. GASPAR, G. LEURENT, A. ROSEN, F.-X. STANDAERT. *FPGA implementations of SPRING And their Countermeasures against Side-Channel Attacks*, in "Cryptographic Hardware and Embedded Systems – CHES 2014", Busan, South Korea, Lecture Notes in Computer Science, September 2014, vol. 8731, pp. 414-432 [*DOI :* 10.1007/978-3-662-44709-3_23], https://hal.inria.fr/hal-01093472

[48] A. CANTEAUT, T. FUHR, H. GILBERT, M. NAYA-PLASENCIA, J.-R. REINHARD. *Multiple Differential Cryptanalysis of Round-Reduced PRINCE*, in "Fast Software Encryption - FSE 2014", London, United Kingdom, 2014, https://hal.inria.fr/hal-01092305

[49] 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

[50] A. CHAILLOUX, I. KERENIDIS, S. KUNDU, J. SIKORA. *Optimal bounds for parity-oblivious random access codes*, in "TQC 2014", Singapour, Singapore, May 2014, https://hal.inria.fr/hal-01094121

[51] A. CHAILLOUX, L. MANČINSKA, G. SCARPA, S. SEVERINI. *Graph-theoretical Bounds on the Entangled Value of Non-local Games*, in "TQC 2014", Singapour, Singapore, May 2014 [*DOI :* 10.4230/LIPICS.XXX.YYY.P], https://hal.inria.fr/hal-01094118

[52] 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

[53] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions*, in "EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques", Copenhagen, Denmark, P. Q. NGUYEN, E. OSWALD (editors), Lecture Notes in Computer Science, Springer, May 2014, vol. 8441, pp. 17-39 [*DOI :* 10.1007/978-3-642-55220-5_2], https://hal.archives-ouvertes.fr/hal-00931774

[54] N. DELFOSSE, J.-P. TILLICH. *A decoding algorithm for CSS codes using the X/Z correlations*, in "IEEE International Symposium on Information Theory - ISIT 2014", Honolulu, United States, June 2014, pp. 1071-1075, https://hal.archives-ouvertes.fr/hal-01081586

[55] 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

[56] J.-C. FAUGÈRE, L. PERRET, F. DE PORTZAMPARC, A. OTMANI, J.-P. TILLICH. *Structural weakness of compact variants of the McEliece cryptosystem*, in "IEEE International Symposium on Information Theory - ISIT 2014", Honolulu, United States, June 2014, pp. 1717-1721, https://hal.archives-ouvertes.fr/hal-01096180

[57] L. GASPAR, G. LEURENT, F.-X. STANDAERT. *Hardware Implementation and Side-Channel Analysis of Lapin*, in "Topics in Cryptology - CT-RSA 2014", San Francisco, United States, J. BENALOH (editor), Lecture Notes in Computer Science, February 2014, vol. 8366, pp. 206-226 [*DOI :* 10.1007/978-3-319-04852-9_11], https://hal.inria.fr/hal-00934054

[58] V. GROSSO, G. LEURENT, F.-X. STANDAERT, K. VARICI. *LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations*, in "Fast Software Encryption - FSE 2014", Londres, United Kingdom, March 2014, https://hal.inria.fr/hal-01093491

[59] 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

[60] V. LALLEMAND, M. NAYA-PLASENCIA. *Cryptanalysis of KLEIN*, in "Fast Software Encryption - FSE 2014", London, United Kingdom, 2014, https://hal.inria.fr/hal-01092301

[61] G. LEURENT, L. WANG. *The Sum Can Be Weaker Than Each Part*, in "Eurocrypt 2015", Sofia, Bulgaria, April 2015, https://hal.inria.fr/hal-01105129

[62] N. SENDRIER. *Code-Based Public-Key Cryptography*, in "Post-Quantum Cryptography Summer School", Waterloo, Canada, Waterloo University, September 2014, https://hal.inria.fr/hal-01095951

[63] J.-P. TILLICH, A. TIXIER, N. SENDRIER. *Recovering the interleaver of an unknown Turbo-Code*, in "IEEE International Symposium on Information Theory - ISIT 2014", Honolulu, United States, IEEE, June 2014, pp. 2784-2788, https://hal.inria.fr/hal-01095970

Conferences without Proceedings

[64] A. CANTEAUT, G. LEURENT. *Cryptanalysis of Wheesht*, in "DIAC 2014", Santa Barbara, United States, August 2014, https://hal.inria.fr/hal-01093428

[65] A. CANTEAUT, J. ROUÉ. *Amélioration des critères de résistance aux attaques différentielles*, in "Journées codage et cryptographie 2014", Les sept Laux, France, March 2014, https://hal.inria.fr/hal-01092790

[66] P. CHARPIN, G. KYUREGHYAN, V. SUDER. *Sparse Permutations with Low Differential Uniformity*, in "Journées codage et cryptographie 2014", Les sept Laux, France, March 2014, https://hal.inria.fr/hal-01100190

[67] V. GROSSO, G. LEURENT, F.-X. STANDAERT, K. VARICI, F. DURVAUX, L. GASPAR, S. KERCKHOF. *CAESAR candidate SCREAM*, in "DIAC 2014", Santa Barbara, United States, August 2014, https://hal.inria.fr/hal-01093528

[68] V. LALLEMAND, M. NAYA-PLASENCIA. *Amélioration des attaques différentielles sur KLEIN*, in "Journées Codage et Cryptographie 2014", Les Sept Laux, France, March 2014, https://hal.inria.fr/hal-01093053

[69] G. LEURENT. *Differential Forgery Attack against LAC*, in "DIAC 2014", Santa Barbara, United States, August 2014, https://hal.inria.fr/hal-01094140

[70] A. LEVERRIER. *Composable security proof for continuous-variable quantum key distribution with coherent states* , in "SPIE Security + Defence 2014, Quantum-Physics-Based Information Security", Amsterdam, Netherlands, September 2014, https://hal.inria.fr/hal-01094198

[71] A. LEVERRIER. *Composable security proof for continuous-variable quantum key distribution with coherent states*, in "4th International Conference on Quantum Cryptography (QCrypt 2014)", Paris, France, September 2014, https://hal.inria.fr/hal-01094186

[72] J.-P. TILLICH, A. TIXIER, N. SENDRIER. *Reconstruction de la permutation d'un turbo-code*, in "Journées codage et cryptographie 2014", Les sept Laux, France, March 2014, https://hal.inria.fr/hal-01100197

Scientific Books (or Scientific Book chapters)

[73] A. CANTEAUT, J. ROUÉ. *Extended differential properties of cryptographic functions*, in "Theory and Applications of Finite Fields", contemporary mathematics series, AMS, December 2014, vol. 632, https://hal.inria.fr/hal-01093322

Research Reports

[74] A. BAR-ON, I. DINUR, O. DUNKELMAN, V. LALLEMAND, B. TSABAN. *Improved Analysis of Zorro-Like Ciphers*, IACR, March 2014, http://eprint.iacr.org/2014/228, https://hal.inria.fr/hal-01092323

[75] C. Boura, M. Minier, M. Naya-Plasencia, V. Suder. *Improved Impossible Differential Attacks against Round-Reduced LBlock*, IACR, April 2014, http://eprint.iacr.org/2014/279, https://hal.archives-ouvertes.fr/hal-01068887

[76] C. Boura, M. Naya-Plasencia, V. Suder. *Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon (Full Version)*, IACR, September 2014, http://eprint.iacr.org/2014/699, https://hal.archives-ouvertes.fr/hal-01068894

[77] A. Canteaut, T. Fuhr, M. Naya-Plasencia, H. Gilbert, J.-R. Reinhard. *Multiple Differential Cryptanalysis of Round-Reduced PRINCE (Full version)*, IACR, February 2014, This article is the full version of the paper to appear in the proceedings of FSE 2014, https://hal.inria.fr/hal-01092624

[78] V. Lallemand, M. Naya-Plasencia. *Cryptanalysis of KLEIN (Full version)*, IACR, February 2014, http://eprint.iacr.org/2014/090, https://hal.inria.fr/hal-01098779

Scientific Popularization

[79] A. Canteaut. *Chiffrer mieux pour chiffrer plus*, June 2014, Conference scientifique d'informatique pour les nouveaux eleves de l'Ecole Polytechnique, https://hal.inria.fr/hal-01099759

Other Publications

[80] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, L. Magnin. *A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias*, February 2014, submitted to SIAM Journal of Computing, https://hal.inria.fr/hal-01094114

[81] A. Canteaut, G. Leurent. *Distinguishing and Key-recovery Attacks against Wheesht*, March 2014, https://hal.inria.fr/hal-00966346

[82] A. Chailloux, G. Scarpa. *Parallel Repetition of Free Entangled Games: Simplification and Improvements*, December 2014, 17 pages, this paper is a follow up and supersedes our previous paper 'Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost' [CS14, arXiv:1310.7787], https://hal.inria.fr/hal-01094123

[83] A. Couvreur, A. Otmani, T. Jean-Pierre, V. Gauthier-Umana. *A Polynomial-Time Attack on the BBCRS Scheme*, January 2015, Accepted at the conference Public Key Cryptography (PKC) 2015, https://hal.archives-ouvertes.fr/hal-01104078

[84] N. Delfosse, J.-P. Tillich. *A decoding algorithm for CSS codes using the X/Z correlations*, January 2014, https://hal.archives-ouvertes.fr/hal-00937128

[85] J.-C. Faugère, A. Otmani, L. Perret, F. De Portzamparc, J.-P. Tillich. *Folding Alternant and Goppa Codes with Non-Trivial Automorphism Groups*, May 2014, Under submission, https://hal.inria.fr/hal-00992389

[86] J.-C. Faugère, A. Otmani, L. Perret, F. De Portzamparc, J.-P. Tillich. *Structural Cryptanalysis of McEliece Schemes with Compact Keys*, March 2014, https://hal.inria.fr/hal-00964265

[87] T. FUHR, G. LEURENT, V. SUDER. *Forgery and Key-Recovery Attacks on CAESAR Candidate Marble*, January 2015, https://hal.inria.fr/hal-01102031

[88] V. GROSSO, G. LEURENT, F.-X. STANDAERT, K. VARICI, F. DURVAUX, L. GASPAR, S. KERCKHOF. *SCREAM & iSCREAM*, March 2014, Submission to the CAESAR competition, https://hal.inria.fr/hal-01093512

[89] G. LEURENT. *Differential Forgery Attack against LAC*, July 2014, https://hal.inria.fr/hal-01017048

[90] G. LEURENT. *Tag Second-preimage Attack against π-cipher*, March 2014, https://hal.inria.fr/hal-00966794

[91] A. LEVERRIER, R. GARCIA-PATRON. *Does Boson Sampling need Fault-Tolerance?*, February 2014, Seventeenth conference on Quantum Information Processing (QIP 2014), https://hal.inria.fr/hal-01094201

[92] A. LEVERRIER. *Composable security proof for continuous-variable quantum key distribution with coherent states*, December 2014, https://hal.inria.fr/hal-01092234

References in notes

[93] N. COURTOIS, M. FINIASZ, N. SENDRIER. *How to achieve a McEliece-based Digital Signature Scheme*, in "Advances in Cryptology - ASIACRYPT 2001", C. BOYD (editor), LNCS, Springer, 2001, vol. 2248, pp. 157-174

[94] I. DUMER. *On Minimum Distance Decoding of Linear Codes*, in "Proc. 5th Joint Soviet-Swedish Int. Workshop Inform. Theory", Moscow, 1991, pp. 50-52

[95] M. FINIASZ. *Parallel-CFS: Strengthening the CFS McEliece-Based Signature Scheme*, in "Selected Areas in Cryptography", A. BIRYUKOV, G. GONG, D. STINSON (editors), LNCS, Springer, 2010, vol. 6544, pp. 159-170

[96] A. MAY, A. MEURER, E. THOMAE. *Decoding Random Linear Codes in $\widetilde{O}(2^{0.054n})$*, in "Advances in Cryptology - ASIACRYPT 2011", D. LEE, X. WANG (editors), LNCS, Springer, 2011, vol. 7073, pp. 107-124

[97] J. STERN. *A method for finding codewords of small weight*, in "Coding theory and applications", G. COHEN, J. WOLFMANN (editors), LNCS, Springer, 1989, vol. 388, pp. 106-113