Activity Report 2013

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, from Oct. 2013]
Pascale Charpin [Inria, Senior Researcher, HdR]
Gaëtan Leurent [Inria, Starting Research position, from Nov. 2013]
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

Marion Bellard [Min. de la Défense]
Virginie Lallemand [Inria, from Oct. 2013]
Grégory Landais [Univ. Paris VI, until Aug. 2013]
Denise Maurice [Univ. Cergy-Pontoise]
Rafael Misoczki [Inria, until Dec. 2013]
Joëlle Roué [Inria]
Valentin Suder [Inria-DGA]
Audrey Tixier [Min. de la Défense]

Post-Doctoral Fellow

Dimitrios Simos [ERCIM, until February 2013]

Administrative Assistant

Christelle Guiziou [Inria]

Others

Mathieu Aria [ENSTA, Internship, from Jun 2013 until Sep 2013]
Yann Hamdaoui [Ecole Centrale de Paris, Internship, until Mar 2013]

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 algorithms whose security does not rely on computational assumptions but on the laws of quantum physics.

2.2. Highlights of the Year

- *Cryptanalysis of several recently proposed lightweight block ciphers:* The area of lightweight primitives has drawn considerable attention over the last years, due to the need for low-cost cryptosystems for several emerging applications like RFID tags and sensor networks. The strong demand from industry has led to the design of a large number of lightweight block ciphers, with different implementation features. In this context, the need for a significant cryptanalysis effort is obvious. The demand from industry for clearly recommended lightweight ciphers requires that the large number of these potential candidates be narrowed down. In this context, the project-team has obtained cryptanalytic results on several recently proposed lightweight block ciphers, including an attack against the full cipher KLEIN-64, the best known attack against a round-reduced version of PRINCE, and some distinguishers on the internal permutation of LED.
- *Cryptanalysis of a variant of the McEliece public-key cryptosystem based on some wild Goppa codes:* The original McEliece cryptosystem proposed in 1978 uses the class of classical binary Goppa codes as private codes. Many other classes of codes have been suggested since the original proposal, but most of them have been cryptanalysed, while the class of Goppa codes still resists all structural attacks. Then, the use of a more general family of Goppa codes over $\mathbf{F}_q$, $q \geq 2$, named wild Goppa codes, has been proposed in 2010 by Bernstein *et al.* in order to reduce the key size of the system. Our recent work leads to an attack which allows to recover the private key in polynomial time when wild Goppa codes over a quadratic finite field extension are used. This is the very first structural attack of the McEliece cryptosystem when some Goppa codes are used. The key-point in the attack is the behaviour of these codes with respect to component-wise product of codes. A similar technique has also been exploited for breaking some other variants of the McEliece system, including one based on Reed-Solomon codes.
- *Experimental demonstration of long-distance continuous-variable quantum key distribution:* Distributing secret keys with information-theoretic security is arguably one of the most important achievements of the field of quantum information processing and communications. The rapid progress in this field has enabled quantum key distribution in real-world conditions and commercial devices are now readily available. Quantum key distribution systems based on continuous variables provide the major advantage that they only require standard telecommunication technology. However, to date, these systems have been considered unsuitable for long-distance communication. In collaboration with experimental groups, we have overcome all previous limitations and demonstrated for the first time continuous-variable quantum key distribution over 80 km of optical fibre. Our results correspond to an implementation guaranteeing the strongest level of security for quantum key distribution reported so far for such long distances and pave the way to practical applications of secure quantum communications.

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.

We also investigate some cross-disciplinary domains, which require a scientific competence coming from other areas, mainly social aspects of cryptology, cryptology for large databases.

5. New Results

5.1. 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 of 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 secure hash functions. Most teams in the research community are actually working on the design and on the analysis (cryptanalysis and optimisation of the performance) of such primitives.

5.1.1. Hash functions

Following the recent attacks against almost all existing hash functions (MD5, SHA-0, SHA-1...), we have initiated a research work in this area, especially within the Saphir-2 ANR project and with several PhD theses. Our work on hash functions is two-fold: we have designed two new hash functions, named FSB and Shabal, which have been submitted to the SHA-3 competition, and we have investigated the security of several hash functions, including the new SHA-3 standard.

Recent results:

- Upper bounds on the degree of an iterated permutation from the degree of the inverse of the inner transformation; this result has been applied both to hash functions and to block ciphers. Most notably, this work leads to the best (theoretical) analysis of the hash function Keccak, which has been selected for the new SHA-3 standard [11].
- Study of a new technique for attacking symmetric primitives based on the existence of linear relations between some input and output bits of the Sbox. This method has been used for improving the best known attack against the SHA-3 candidate Hamsi [36], [58].

5.1.2. 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 analysed. Most of our work in this area is related to an ANR Project named BLOC.

Recent results:

- Cryptanalysis of several recently proposed lightweight block ciphers. This includes an attack against the full cipher KLEIN-64 [66], [49], and an attack against 8 rounds (out of 12) of PRINCE [37].
- Analysis of the resistance of AES-like permutations to improved rebound attacks. Most notably, this improved technique leads to a distinguisher on 10 rounds of the internal permutation of the SHA-3 candidate Grøstl [14].
- 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 [42].
- Design of an improved variant of Meet-in-the-Middle attacks, named *Sieve-in-the-Middle*: instead of selecting the key candidates by searching for a collision in an intermediate state which can be computed forwards and backwards, we here look for the existence of valid transitions through some middle Sbox. In the same paper, an improved technique is also proposed to build bicliques without needing any additional data (on the contrary to classical biclique attacks). These new methods have been exploited to break 8 rounds (out of 12) of the lightweight block cipher PRINCE [37], [59], [30].
- Analysis of the differential properties of the AES Superbox [48].
- Design of a new block cipher, named ZORRO, for which physical security is considered as an optimisation criterion [41].
- Design and study of a new construction for low-latency block ciphers, named *reflection ciphers*, which generalises the so-called α-reflection property exploited in PRINCE. This construction aims at reducing the implementation overhead of decryption on top of encryption [24].

5.1.3. Cryptographic properties and construction of appropriate building blocks

The construction of building blocks which guarantee a high resistance against the known attacks is a major topic within our project-team, for stream ciphers, block ciphers and hash functions. The use of such optimal objects actually leads to some mathematical structures which may be at the origin of new attacks. This work involves fundamental aspects related to discrete mathematics, cryptanalysis and implementation aspects. Actually, characterising 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.

Recent results:

- Study of the algebraic properties (e.g. the algebraic degree) of the inverses of APN power permutations [16], [51].
- Definition of a new criterion for Sboxes and link with some recent algebraic attacks on the hash function Hamsi [36], [58].
- Definition of some 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 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 [21], [48].
- A new sufficient (and simpler) condition for checking that a mapping is APN has been established [62].
- Surveys of PN and APN mappings [55], [54].

5.2. Code-based cryptography

Participants: Grégory Landais, Rafael Misoczki, Nicolas Sendrier, Dimitrios Simos, Jean-Pierre Tillich.

Most popular public-key cryptographic schemes rely either on the factorisation 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:

- Design of a new variant of McEliece using Moderate Density Parity Check (MDPC) codes [45];
- 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 [39], [63].
- Cryptanalysis of a variant of the McEliece cryptosystem based on Reed-Solomon codes [38].
- Cryptanalysis of a variant of the McEliece cryptosystem based on convolutional codes proposed by Löndahl and Johansson in 2012 [43].
- Design of the first algorithm for distinguishing between Goppa codes (or alternant codes) over any field and random codes. Provided that the codes have sufficiently large rates, this technique can solve in polynomial-time the Goppa-Code-Distinguishing problem, which is an assumption in the security proof of McEliece cryptosystem [12].
- Study of the hardness of the code equivalence problem over $\mathbf{F}_q$. This problem has been extensively studied for permutation-equivalence (which covers all cases for $q = 2$). For $q \in \{3, 4\}$, we have generalised the support-splitting algorithm, and we have shown that the problem seems intractable for most instances when $q \geq 5$ [46]. This property has been exploited in an improvement version of an identification protocol due to Girault [47].

5.3. 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 [1], 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 DGA.

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 (Marion Bellard's PhD).

5.4. Quantum information theory

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

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 generalise the best classical codes available today.

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

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

5.4.1. 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 codes combining an improved version of a family of spatially coupled quantum LDPC codes with a family of error reducing turbo-codes [44];
- 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 [19].
- Mamdouh Abbara's PhD thesis [9]

5.4.2. 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 with security properties based on quantum theory.

Recent results:

- Experimental demonstration of quantum key distribution with continuous variables over 80 km [15], greatly improving over previous records around 25 km.
- Security proof of continuous-variable quantum key distribution protocols against general attacks [17], [29].
- Security proof of device-independent quantum key distribution in the bounded storage model [18].
- Study of BosonSampling, a recently introduced problem where quantum computers offer a provable speedup over classical computers [67], [28].
- Introduction and study of "Local Orthogonality", an information-theoretical principle for quantum correlations [13], [68].
- Introduction of a general formalism for the study of contextuality and non locality in quantum theory, based on the combinatorics of hypergraphs [65], [27].

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Contracts with Industry

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

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- **ANR SAPHIR-2** (03/09 → 03/13)
  Security and Analysis of Primitives of Hashing Innovatory and Recent 2
  http://www.saphir2.fr/
  ANR program: VERSO (Reseaux du Futur et Services)
  Partners: France Telecom, Gemalto, Cryptolog international, EADS SN, Sagem Securite, ENS/LIENS, UVSQ/PRISM, Inria (project-team SECRET), ANSSI
  153 kEuros
  This industrial research project aims at participating to the NIST competition (cryptanalysis, implementations, optimizations, etc.), and in supporting the SHA-3 candidates proposed by its partners.
- **ANR BLOC** (10/11 → 09/15)
  Conception et analyse de chiffrements par blocs efficaces pour les environnements contraints
  ANR program: Ingénierie numérique et sécurité
  Partners: INSA Lyon, Inria (project-team SECRET), University of Limoges (XLIM), CryptoExperts
  446 kEuros
  The BLOC project aims at providing strong theoretical and practical results in the domain of cryptanalyses 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, UVSQ (Prism), 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, EPI 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.

7.1.2. Others

- **French Ministry of Defense** (01/11 → 12/13)
  Funding for the supervision of Marion Bellard's PhD.
  30 kEuros.
- **French Ministry of Defense** (10/12 → 09/15)
  Funding for the supervision of Audrey Tixier's PhD.
  30 kEuros.
- **DGA-MI** (12/11 → 02/13)
  Analysis of binary streams.
  20 kEuros.

- **PEPS IQC 2013** ($04/13 \rightarrow 03/14$)
  Topology and quantum codes
  coordinated by G. Zémor, Institut de Mathématiques de Bordeaux.
  http://www.cnrs.fr/mi/spip.php?article301
- **PEPS IQC 2013** ($04/13 \rightarrow 03/14$)
  Quantum Cryptography and distributed computing
  coordinated by Frédéric Grosshans, Laboratoire Aimé Cotton.
  http://www.cnrs.fr/mi/spip.php?article301

7.2. European Initiatives

7.2.1. Collaborations in European Programs, except FP7

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.

7.3. International Initiatives

7.3.1. Inria International Partners

7.3.1.1. Informal International Partners

- Otto-von-Guericke Universität Magdeburg, Institut für Algebra und Geometrie (Germany):
  Study of Boolean functions for cryptographic applications
- DTU - Danmarks Tekniske Universitet, Department of Mathematics:
  Lightweight symmetric crytography and code-based cryptography
- Indian Statistical Institute, Kolkata, India:
  Symmetric cryptography

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- Grigory Kabatianskiy, Institute for Problems of Information Transmission, Moscow, Russia, November 23-30
- Paulo Barreto, University of Sao Paulo, Brazil, November 22-30
- Dimitrios Simos, SBA Research, Vienna, Austria, June 30-July 6
- Bimal Roy, Indian Statistical Institute, Kolkata, India, June 15-23

7.4.2. Visits to International Teams

- University of Sherbrooke, Canada, July 14-21 (J.P. Tillich)
- Newton Institute for Mathematical Sciences, Cambridge, United Kingdom, November 6-8, invitation to the *Mathematical Challenges in Quantum Information* Program, (A. Leverrier)

- CWI, Amsterdam, Netherlands, November 26-27, collaboration with Christian Schaffner, (A. Leverrier)
- FHNW, Windisch, Switzerland, May 27-31, visiting Willi Meier (M. Naya-Plasencia)

8. Dissemination

8.1. Scientific Animation

8.1.1. Workshop organization

- *CBC 2013 - the fourth Code-based Cryptography Workshop*, Rocquencourt, June 10-12, 2013. Organizing committee: G. Landais, Rafael Misoczki, N. Sendrier (chair) http://cbc2013.inria.fr/.

8.1.2. Editorial activities

- *Designs, Codes and Cryptography*, associate editor: P. Charpin, since 2003.
- *Finite Fields and Their Applications* associate editors: A. Canteaut, P. Charpin.
- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, 2013, co-editor: A. Canteaut.
- *Finite Fields and Their Applications. Character Sums and Polynomials*, Radon Series on Computational and Applied Mathematics, Degruyter, In Press. Editeurs: P. Charpin, A. Pott (U. Magdeburg) et A. Winterhof (Austrian Acad. of Sc.)
- A. Canteaut serves on 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.

8.1.3. Program committees

- FSE 2013: March 11-13, 2013, Singapore, Singapore (A. Canteaut, M. Naya-Plasencia);
- WCC 2013: April 15-19, 2013, Bergen, Norway (A. Canteaut, N. Sendrier);
- PQCrypto 2013: June 4-7, 2013, Limoges, France (N. Sendrier, JP. Tillich);
- CBC 2013: June, 10-12, 2013, Rocquencourt, France (N. Sendrier, JP. Tillich);
- SAC 2013: August, 14-16, 2013, Vancouver, Canada (A. Canteaut, M. Naya-Plasencia);
- MoCrySEn 2013: September, 2-6, 2013, Regensburg, Germany (N. Sendrier, co-chair; D. Simos, chair; M. Naya-Plasencia, J.P. Tillich);
- Asiacrypt 2013: December 1-5, 2013, Bangalore, India (A. Canteaut, N. Sendrier);
- *IMA International Conference on Cryptography and Coding*: December 17-19, 2013, Oxford, UK (P. Charpin, M. Naya-Plasencia);
- *Optimal Codes and Related Topics - OC 2013*, September 6-8, 2013, Albena, Bulgaria (P. Charpin);
- 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, JP. 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);

- Latincrypt 2014: September, 17-19, 2014, Florianópolis, Brazil (N. Sendrier);
- Asiacrypt 2014: December 7-11, 2014, China (M. Naya-Plasencia);
- Indocrypt 2014: December 14-17, 2014, New Delhi, India (A. Canteaut).

8.1.4. Invited talks

- A. Canteaut, *Extended differential properties of cryptographic functions*, The 11th International Conference on Finite Fields and their Applications - Fq11, Magdeburg, Germany, July 2013.
- A. Canteaut, *Similarities between Encryption and Decryption: How far can we go?* (Stafford Tavares lecture,), Selected Areas in Cryptography - SAC 2013, Vancouver, Canada, August 2013.
- A. Leverrier, *A Combinatorial Approach to Nonlocality and Contextuality*, Quo Vadis, Quantum Physics?, Natal, Brazil, February 2013.
- A. Leverrier, *Security of continuous-variable quantum key distribution against general attacks*, APS March Meeting 2013, Baltimore, United States of America, March 2013.
- N. Sendrier, *The Construction of Code-Based Cryptosystems*, The 14th IMA International Conference on Cryptography and Coding, Oxford, United Kingdom, December 2013.

A. Canteaut and M. Naya-Plasencia have been invited to give a talk to the *Keccak & SHA-3 Day* organized in Brussels, following the selection of the hash function Keccak as the new SHA-3 standard:

- A. Canteaut, *On some algebraic properties of Keccak*, Keccak & SHA-3 Day, Brussels, Belgium, March 2013;
- M. Naya-Plasencia, *First practical results on reduced-round Keccak and Unaligned rebound attack*, Keccak & SHA-3 Day, Brussels, Belgium, March 2013.

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

- P. Charpin, *On binary* $[2^n - 1, 2^n - 1 - 2n, d]$ *codes*, workshop "Coding Theory", Dagstuhl Seminar 13351, August 2013.
- A. Leverrier. *Does BosonSampling need Fault-Tolerance?*, Journées Informatique Quantique 2013, Nancy, France, October 2013.
- M. Naya-Plasencia, *Meet-in-the-middle through an Sbox*, ESC 2013 - Early Symmetric Crypto seminar, Luxembourg, Luxembourg, January 2013.
- N. Sendrier, *Classical algorithm techniques for decoding generic linear codes*, workshop “Quantum Cryptanalysis”, Dagstuhl Seminar 13371, September 2013.

8.1.5. Other responsibilities in the national community

- N. Sendrier is a vice-chair of the “Commission d’Evaluation” at Inria;
- N. Sendrier served on the following Inria juries: admissibilité DR2, admissibilité CR2 Rennes, admission CR;
- N. Sendrier has served on the selection committee of PEPS IQC (quantum information and communication, CNRS);
- A. Canteaut is a member of the “Comité de pilotage” of the Fondation Sciences Mathématiques de Paris;
- JP. Tillich is in charge of “Formation par la recherche” for the Paris-Rocquencourt Inria center.
- P. Charpin served on the selection committee for postdoctoral positions, Inria Paris-Rocquencourt.
- P. Charpin served on the selection committee for PhD fundings in Computer Science at University Pierre-et-Marie Curie (theme: *Software and Algorithms*).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master: A. Canteaut, *Stream ciphers*, 9 hours, M2, Telecom ParisTech, France;

Master: A. Canteaut, *Introduction to symmetric cryptography*, 4.5 hours, M2, Telecom ParisTech, France;

Master: A. Canteaut, *Error-correcting codes and applications to cryptlogy*, 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 h, M2, Ecole Polytechnique, France.

The members of the project-team also gave advanced lectures to several summer schools for PhD students: *Icebreak 2013* (Reykjavik, Iceland, June 2013) [22], [25]; *Summer school on Design and Security of Cryptographic Functions, Algorithms and Devices* (Albena, Bulgaria, June 2013) [31]; *2013 Indian National Workshop on Cryptology* (Delhi, India, October 2013) [33]; *Forum des jeunes mathématicien-ne-s 2013* (Lyon, France, November 2013) [48].

8.2.2. Supervision

PhD: Mamdouh Abbara, *Quantum turbo-codes*, Ecole Polytechnique, April 9, 2013 (supervisor: JP. Tillich)

PhD: Rafael Misoczki, *Two Approaches for Achieving Efficient Code-Based Cryptosystems*, Université Pierre-et-Marie Curie, November 25, 2013 (supervisor: N. Sendrier)

PhD: Jean-Christophe Sibel, *Region-based approximation to solve inference in loopy factor graphs: decoding LDPC codes by the Generalized Belief Propagation*, Université de Cergy-Pontoise, June 7, 2013 (supervisor : D. Declercq)

PhD in progress: Marion Bellard, *Influence du mapping pour la reconnaissance d'un système de communication*, since January 2011, supervisors: N. Sendrier and J.-P. Tillich

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

PhD in progress: Grégory Landais, *Implementations of code-based cryptosystems and of their cryptanalyses*, since October 2010, supervisors: M. Finiasz and N. Sendrier

PhD in progress: Denise Maurice, *Quantum LDPC codes*, since September 2010, supervisor: JP. Tillich

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

PhD in progress: Valentin Suder, *Permutations for symmetric cryptography*, since October 2011, supervisor: P. Charpin

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

8.2.3. Juries

- Risto Hakala, *Results on Linear Models in Cryptography*, Aalto University, Helsinki, Finlande, February 2013, committee: P. Charpin (reviewer).
- Mohamed Ahmed Abdelraheem, *Cryptanalysis of Some Lightweight Symmetric Ciphers*, Danmarks Tekniske Universitet, Denmark, February 7, 2012, committee: A. Canteaut (reviewer);
- Mamdouh Abbara, *Turbo-codes quantiques*, Ecole Polytechnique, April 9, 2013, committee: JP. Tillich (supervisor);
- Paul Stankovski, Lunds University, Sweden, June 17, 2013, committee: A. Canteaut (opponent);
- Alexander Zeh, *Algebraic Soft- and Hard-Decision Decoding of Generalized Reed–Solomon and Cyclic Codes*, Ecole Polytechnique/University of Ulm, September 2, 2013, committee: P. Charpin (reviewer), JP. Tillich;

- Anne Marin, *Utilisation d'états multigraphes pour le partage de secret quantique*, Télécom ParisTech, September 17, 2013, committee: J.P. Tillich;
- Jérémy Jean, *Cryptanalyse de primitives symétriques basées sur le chiffrement AES*, École Normale Supérieure, September 24, 2013, committee: A. Canteaut (reviewer);
- Rafael Misoczki, *Two Approaches for Achieving Efficient Code-Based Cryptosystems*, University Pierre-et-Marie-Curie, November 25, 2013, committee: N. Sendrier (supervisor), JP. Tillich;
- Julien Schrek, *Signatures et authentification pour les cryptosystèmes basés sur les codes correcteurs en métrique de Hamming et en métrique rang*, University of Limoges, November 27, 2013, committee: N. Sendrier (reviewer), J.P. Tillich;
- Patrick Debrez, *Attaques par Rencontre par le Milieu sur l'AES*, École Normale Supérieure, December 9, 2013, committee: G. Leurent
- Alberto Passuello, *Semidefinite programming in combinatorial optimization with applications to coding theory and geometry*, University of Bordeaux, December 17, 2013, committee: J.P. Tillich

9. Bibliography

Major publications by the team in recent years

[1] C. BOURA, A. CANTEAUT, C. DE CANNIÈRE. *Higher-Order Differential Properties of Keccak and Luffa*, in "Fast Software Encryption - FSE 2011", LNCS, Springer, 2011, vol. 6733, pp. 252-269

[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] 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

[4] 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

[5] 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

[6] F. DIDIER, J.-P. TILLICH. *Computing the algebraic immunity efficiently*, in "Fast Software Encryption - FSE 2006", LNCS, Springer, 2006, vol. 4047, pp. 359-374

[7] 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

[8] 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

[9] M. ABBARA. , *Turbo-codes quantiques*, Ecole Polytechnique X, April 2013, http://hal.inria.fr/pastel-00842327

[10] R. MISOCZKI. , *Two Approaches for Achieving Efficient Code-Based Cryptosystems*, Université Pierre et Marie Curie - Paris VI, November 2013, http://hal.inria.fr/tel-00931811

Articles in International Peer-Reviewed Journals

[11] 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", January 2013, vol. 59, n^{o} 1, pp. 691-702 [*DOI :* 10.1109/TIT.2012.2214203], http://hal.inria.fr/hal-00738398

[12] J.-C. FAUGÈRE, V. GAUTHIER-UMANA, A. OTMANI, L. PERRET, J.-P. TILLICH. *A Distinguisher for High Rate McEliece Cryptosystems*, in "IEEE Transactions on Information Theory", June 2013, vol. 59, n^{o} 10, pp. 6830-6844 [*DOI :* 10.1109/TIT.2013.2272036], http://hal.inria.fr/hal-00776068

[13] T. FRITZ, A. B. SAINZ, R. AUGUSIAK, J. B. BRASK, R. CHAVES, A. LEVERRIER, A. ACÍN. *Local orthogonality as a multipartite principle for quantum correlations*, in "Nature Communications", August 2013, vol. 4 [*DOI :* 10.1038/NCOMMS3263], http://hal.inria.fr/hal-00917114

[14] J. JEAN, M. NAYA-PLASENCIA, T. PEYRIN. *Improved Cryptanalysis of AES-like Permutations*, in "Journal of Cryptology", July 2013, http://hal.inria.fr/hal-00907706

[15] 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], http://hal.inria.fr/hal-00798855

[16] G. KYUREGHYAN, V. SUDER. *On inversion in Z_2n-1*, in "Finite Fields and Their Applications", January 2014, vol. 25, pp. 234-254, http://hal.inria.fr/hal-00879490

[17] A. LEVERRIER, R. GARCÍA-PATRÓN, R. RENNER, N. J. CERF. *Security of Continuous-Variable Quantum Key Distribution Against General Attacks*, in "Physical Review Letters", January 2013, vol. 110, n^{o} 3 [*DOI :* 10.1103/PHYSREVLETT.110.030502], http://hal.inria.fr/hal-00917115

[18] S. PIRONIO, L. MASANES, A. LEVERRIER, A. ACÍN. *Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model*, in "Physical Review X", July 2013, vol. 3, n^{o} 3 [*DOI :* 10.1103/PHYSREVX.3.031007], http://hal.inria.fr/hal-00917113

[19] 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, à paraître, http://hal.inria.fr/hal-00931764

Invited Conferences

[20] A. CANTEAUT. *Comment concevoir un algorithme de chiffrement sûr et efficace*, in "Forum des jeunes mathématicien-ne-s 2013", Lyon, France, November 2013, http://hal.inria.fr/hal-00931566

[21] A. CANTEAUT. *Extended differential properties of cryptographic functions*, in "The 11th International Conference on Finite Fields and their Applications - Fq11", Magdeburg, Germany, July 2013, http://hal.inria.fr/hal-00859027

[22] A. CANTEAUT. *Foundations of cryptanalysis: On Boolean functions*, in "Icebreak 2013", Reykjavik, Ireland, June 2013, http://hal.inria.fr/hal-00931689

[23] A. CANTEAUT. *On some algebraic properties of Keccak*, in "Keccak & SHA-3 Day", Bruxelles, Belgium, March 2013, http://hal.inria.fr/hal-00807475

[24] A. CANTEAUT. *Similarities between Encryption and Decryption: How far can we go?*, in "Selected Areas in Cryptography - SAC 2013", Vancouver, Canada, LNCS, Springer, August 2013, http://hal.inria.fr/hal-00858933

[25] A. CANTEAUT. *Stream cipher cryptanalysis*, in "Icebreak 2013", Reykjavik, Iceland, June 2013, http://hal.inria.fr/hal-00931697

[26] A. CHAILLOUX, S. GIANNICOLA. *Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost*, in "QIP 2014 - Quantum Information Processing", Barcelona, Spain, February 2014, http://hal.inria.fr/hal-00927544

[27] A. LEVERRIER. *A Combinatorial Approach to Nonlocality and Contextuality*, in "Quo Vadis, Quantum Physics?", Natal, Brazil, 2013, http://hal.inria.fr/hal-00931941

[28] A. LEVERRIER. *Does Boson Sampling need Fault-Tolerance?*, in "Journées Informatique Quantique 2013", Nancy, France, October 2013, http://hal.inria.fr/hal-00932345

[29] A. LEVERRIER. *Security of continuous-variable quantum key distribution against general attacks*, in "APS March Meeting 2013", Baltimore, United States, March 2013, http://hal.inria.fr/hal-00926300

[30] M. NAYA-PLASENCIA. *"Meet-in-the-middle" through an Sbox*, in "ESC 2013 - Early Symmetric Crypto seminar", Luxembourg, January 2013, http://hal.inria.fr/hal-00907735

[31] M. NAYA-PLASENCIA. *Cryptanalysis of lightweight block ciphers*, in "Summer school on Design and Security of Cryptographic Functions, Algorithms and Devices", Albena, Bulgaria, July 2013, http://hal.inria.fr/hal-00933553

[32] M. NAYA-PLASENCIA. *First practical results on reduced-round Keccak and Unaligned rebound attack*, in "Keccak & SHA-3 Day", Bruxelles, Belgium, March 2013, http://hal.inria.fr/hal-00907715

[33] N. SENDRIER. *An Introduction to Code Based Cryptography*, in "2013 Indian National Workshop on Cryptology", Delhi, India, October 2013, http://hal.inria.fr/hal-00932120

[34] N. SENDRIER. *Classical algorithm techniques for decoding generic linear codes*, in "Dagstuhl Seminar 13371, Quantum Cryptanalysis", Dagstuhl, Germany, September 2013, http://hal.inria.fr/hal-00864837

[35] N. SENDRIER. *The Construction of Code-Based Cryptosystems*, in "Fourteenth IMA International Conference on Cryptography and Coding", Oxford, United Kingdom, December 2013, http://hal.inria.fr/hal-00932115

International Conferences with Proceedings

[36] C. BOURA, A. CANTEAUT. *A new criterion for avoiding the propagation of linear relations through an Sbox*, in "FSE 2013 - Fast Software Encryption", Singapour, Singapore, Lecture Notes in Computer Science, Springer, January 2014, http://hal.inria.fr/hal-00931535

[37] A. CANTEAUT, M. NAYA-PLASENCIA, B. VAYSSIÈRE. *Sieve-in-the-Middle: Improved MITM Attacks*, in "CRYPTO 2013 - 33rd Annual Cryptology Conference", Santa Barbara, United States, R. CANETTI, J. A. GARAY (editors), Lecture Notes in Computer Science, Springer, June 2013, vol. 8042, pp. 222-240 [*DOI :* 10.1007/978-3-642-40041-4_13], http://hal.inria.fr/hal-00857358

[38] A. COUVREUR, P. GABORIT, V. GAUTIER, A. OTMANI, J.-P. TILLICH. *Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes*, in "WCC 2013 - International Workshop on Coding and Cryptography", Bergen, Norway, Selmer Center at the University of Bergen, Norway and Inria, Rocquencourt, France, 2013, pp. 181-193, http://hal.inria.fr/hal-00830594

[39] A. COUVREUR, A. OTMANI, J.-P. TILLICH. *Polynomial Time Attack on Wild McEliece Over Quadratic Extensions*, in "EUROCRYPT 2014", Copenhagen, Denmark, 2014, à paraître, http://hal.inria.fr/hal-00931774

[40] L. GASPAR, G. LEURENT, F.-X. STANDAERT. *Hardware Implementation and Side-Channel Analysis of Lapin*, in "CT-RSA 2014", San Francisco, United States, J. BENALOH (editor), February 2014, http://hal.inria.fr/hal-00934054

[41] B. GÉRARD, V. GROSSO, M. NAYA-PLASENCIA, F.-X. STANDAERT. *Block Ciphers that are Easier to Mask: How Far Can we Go?*, in "CHES 2013", Santa Barbara, United States, Springer, 2013, vol. 8086, pp. 383-399, http://hal.inria.fr/hal-00907727

[42] J. JEAN, M. NAYA-PLASENCIA, T. PEYRIN. *Multiple Limited-Birthday Distinguishers and Applications*, in "Selected Areas in Cryptography - SAC 2013", Vancouver, Canada, August 2013, To appear, http://hal.inria.fr/hal-00870452

[43] G. LANDAIS, J.-P. TILLICH. *An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes*, in "PQCrypto 2013", Limoges, France, P. GABORIT (editor), LNCS 7932, Springer, 2013, pp. 102-117 [*DOI :* 10.1007/978-3-642-38616-9_7], http://hal.inria.fr/hal-00880654

[44] D. MAURICE, J.-P. TILLICH, I. ANDRIYANOVA. *A family of quantum codes with performances close to the hashing bound under iterative decoding*, in "ISIT 2013 - IEEE International Symposium on Information Theory", Turkey, IEEE, July 2013, pp. 907-914, http://hal.inria.fr/hal-00862460

[45] R. MISOCZKI, J.-P. TILLICH, P. S. L. M. BARRETO, N. SENDRIER. *MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes*, in "ISIT 2013 - IEEE International Symposium on Information Theory", Istanbul, Turkey, July 2013, http://hal.inria.fr/hal-00870929

[46] N. SENDRIER, D. E. SIMOS. *How easy is code equivalence over Fq?*, in "WCC 2013 - International Workshop on Coding and Cryptography", Bergen, Norway, April 2013, http://hal.inria.fr/hal-00790861

[47] N. SENDRIER, D. E. SIMOS. *The Hardness of Code Equivalence over $mathbf{F}_q$ and its Application to Code-based Cryptography*, in "PQCrypto 2013", Limoges, France, P. GABORIT (editor), LNCS, Springer, June 2013, vol. 7932, pp. 203-216 [*DOI :* 10.1007/978-3-642-38616-9], http://hal.inria.fr/hal-00863598

Conferences without Proceedings

[48] A. CANTEAUT, J. ROUÉ. *Amélioration des critères de résistance aux attaques différentielles*, in "Forum des jeunes mathématicien-ne-s 2013", Lyon, France, November 2013, http://hal.inria.fr/hal-00931561

[49] V. LALLEMAND. *Cryptanalysis of KLEIN*, in "Icebreak 2013", Reykjavik, Iceland, June 2013, http://hal.inria.fr/hal-00931699

[50] G. LANDAIS. *Information Set Decoding Implementation*, in "Fourth Code-based Cryptography Workshop 2013", Rocquencourt, France, June 2013, http://hal.inria.fr/hal-00931673

[51] V. SUDER, G. KYUREGHYAN. *On Inversion in Z_2n-1*, in "The 11th International Conference on Finite Fields and their Applications", Magdeburg, Germany, July 2013, http://hal.inria.fr/hal-00931646

[52] J.-P. TILLICH. *Survey on attacks against structured alternant codes (part 1)*, in "CBC 2013 - Fourth Code-based Cryptography Workshop", Rocquencourt, France, June 2013, http://hal.inria.fr/hal-00931777

[53] J.-P. TILLICH. *Survey on attacks against structured alternant codes (part 2)*, in "CBC 2013 - Fourth Code-based Cryptography Workshop", Rocquencourt, France, June 2013, http://hal.inria.fr/hal-00931779

Scientific Books (or Scientific Book chapters)

[54] P. CHARPIN. *PN and APN functions*, in "Handbook of Finite Fields", G. MULLEN, D. PANARIO (editors), Discrete Mathematics and Its Applications, Chapman and Hall/CRC Press, June 2013, http://hal.inria.fr/hal-00932157

[55] G. KYUREGHYAN. *Special mappings of finite fields*, in "Finite Fields and Their Applications. Character Sums and Polynomials", P. CHARPIN, A. POTT, A. WINTERHOF (editors), Radon Series on Computational and applied mathematics, De Gruyter, May 2013, vol. 11, pp. 117-144, http://hal.inria.fr/hal-00931607

Books or Proceedings Editing

[56] D. AUGOT, A. CANTEAUT, G. KYUREGHYAN, F. SOLOV'EVA, Ø. YTREHUS (editors). , *Designs, Codes and Cryptography (Special Issue in Coding and Cryptography)*, Springer, January 2013, vol. 66, 399 p. , http://hal.inria.fr/hal-00931522

[57] P. CHARPIN, A. POTT, A. WINTERHOF (editors). , *Finite Fields and Their Applications - Character Sums and Polynomials*, Radon Series on Computational and applied mathematics, De Gruyter, May 2013, vol. 11, 274 p. , http://hal.inria.fr/hal-00931614

Other Publications

[58] C. BOURA, A. CANTEAUT. , *A new criterion for avoiding the propagation of linear relations through an Sbox (Full version)*, April 2013, IACR Cryptology ePrint Archive 2013/211, http://hal.inria.fr/hal-00859030

[59] A. CANTEAUT, M. NAYA-PLASENCIA, B. VAYSSIÈRE. , *Sieve-in-the-Middle: Improved MITM Attacks (Full Version)*, May 2013, IACR Cryptology ePrint Archive 2013/324, http://hal.inria.fr/hal-00857369

[60] A. CHAILLOUX, S. GIANNICOLA. *Parallel Repetition of entangled games on the uniform distribution*, in "Journées d'Informatique Quantique", Nancy, France, October 2013, Journées d'Informatique Quantique, Présentation, http://hal.inria.fr/hal-00934611

[61] A. CHAILLOUX, G. GUTOSKI, J. SIKORA. , *Optimal bounds for quantum weak oblivious transfer*, 2013, arXiv:1310.3262 [quant-ph], http://hal.inria.fr/hal-00927537

[62] P. CHARPIN, G. KYUREGHYAN. , *A note on verifying the APN property*, August 2013, IACR Cryptology ePrint Archive 2013/475, http://hal.inria.fr/hal-00932161

[63] A. COUVREUR, A. OTMANI, J.-P. TILLICH. , *New Identities Relating Wild Goppa Codes*, 2013, http://hal.inria.fr/hal-00880994

[64] N. DELFOSSE, J.-P. TILLICH. , *A decoding algorithm for CSS codes using the X/Z correlations*, 2014, http://hal.inria.fr/hal-00937128

[65] T. FRITZ, A. LEVERRIER, A. B. SAINZ. , *Probabilistic models on contextuality scenarios*, 2013, To be published in the proceedings of Quantum Physics and Logic (QPL, 2013). Overview and discussion of the results in arXiv:1212.4084, http://hal.inria.fr/hal-00931584

[66] V. LALLEMAND. , *Amélioration des attaques différentielles sur KLEIN*, Université de Limoges, September 2013, http://hal.inria.fr/hal-00931253

[67] A. LEVERRIER, R. GARCÍA-PATRÓN. , *Does Boson Sampling need Fault-Tolerance?*, 2013, http://hal.inria.fr/hal-00931587

[68] A. B. SAINZ, T. FRITZ, R. AUGUSIAK, J. B. BRASK, R. CHAVES, A. LEVERRIER, A. ACÍN. , *Exploring the Local Orthogonality Principle*, 2013, http://hal.inria.fr/hal-00931591