INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team secret

Security, Cryptology and Transmissions

Paris - Rocquencourt

Theme : Algorithms, Certification, and Cryptography

Table of contents

1. Team

Research Scientists

Anne Canteaut [Team Leader, Senior Researcher (DR) Inria, HdR]
Nicolas Sendrier [Senior Researcher (DR) Inria, HdR]
Pascale Charpin [Senior Researcher (DR) Inria, HdR]
Jean-Pierre Tillich [Junior Researcher (CR) Inria, HdR]
Ayoub Otmani [On leave from University of Caen]

External Collaborators

Matthieu Finiasz [Assistant Professor (MC) ENSTA, Paris]
Yann Laigle-Chapuy [Éducation Nationale, until Sept 2010]

PhD Students

Mamdouh Abbara [détachement du Corps des Mines]
Bhaskar Biswas [INRIA grant, Ecole Polytechnique, until April 2010]
Céline Blondeau [INRIA grant, Univ. P. et M. Curie]
Christina Boura [CIFRE grant, Univ. P. et M. Curie]
Maxime Côte [CIFRE grant, Ecole Polytechnique, until March 2010]
Benoît Gérard [DGA grant, Univ. P. et M. Curie]
Vincent Herbert [INRIA grant, Univ. P. et M. Curie]
Stéphane Jacob [AMX grant, Univ. P. et M. Curie]
Stéphane Manuel [ATER, Univ. Paris 8]
Denise Maurice [Ecole Normale Supérieure, Paris]
Rafael Misoczki [INRIA grant, Univ. P. et M. Curie, since Nov. 2010]
Grégory Landais [DGA grant, since Oct 2010]

Post-Doctoral Fellows

Sumanta Sarkar [University H. Poincaré, Nancy]
Ayca Cesmelioglu [from Oct. to Dec. 2010]

Visiting Scientist

Sugata Gangopadhyay [Indian Institute of Technology, Roorkee, June-July 2010]

Administrative Assistant

Christelle Guiziou [Secretary (TR) Inria]

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, especially through the study of the involved discrete structures. This work is essential since the current situation of cryptography is rather fragile: many cryptographic protocols are now known whose security can be formally proved assuming that the involved cryptographic primitives are ideal (random oracle model, ideal cipher model,...). However, the security of the available primitives has been so much threatened by the recent progress in cryptanalysis that only a few stream ciphers and hash functions are nowadays considered to be secure. In other words, there is usually no concrete algorithm available to instantiate the ideal "black boxes" used in these protocols!

In this context, our research work focuses on both families of cryptographic primitives, *symmetric* and *asymmetric* primitives. More precisely, our domain in cryptology includes the analysis and the design of symmetric algorithms (a.k.a. secret-key algorithms), and also the study of the public-key algorithms based on hard problems coming from coding theory. Moreover, 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... Most of our work mix 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.

2.2. Highlights

- **Cryptanalysis of several variants of McEliece cryptosystems with compact public-keys**: reducing the size of the public-key by using some particular families of error-correcting codes is one of the main issues for code-based cryptosystems. Several variants of the original McEliece cipher have been proposed so far to solve this problem. Some researchers of the project-team have shown that these variants can be cryptanalysed by some key-recovery algebraic attacks exploiting the structural properties of the involved families of codes.
- **Cryptanalysis of several hash functions proposed to the SHA-3 competition**: this international competition, launched by the American National Institute of Standards and Technology, aims at selecting a new standard for hash functions[1]. The revision of the current standard FIPS 180-2 has actually been decided by NIST in response to the recent attacks against almost all existing hash functions (e.g. MD5, SHA-0, SHA-1). Among the 64 hash function proposals submitted to the SHA-3 competition, three have been cryptanalyzed by some researchers of the project-team, namely MCSSHA-3 and its variants proposed by M. Maslennikov from Korea, Maraca proposed by R.J. Jenkins Jr. from Microsoft and ESSENCE proposed by J.W. Martin from James Madison University (Virginia, USA). More recently, some weaknesses have been exhibited on 3 of the 14 candidates selected for the second round of the competition: Keccak, Hamsi and Luffa.

3. Scientific Foundations

3.1. Scientific foundations

Our research work is mainly devoted to the design and analysis of cryptographic algorithms. Our approach on the previous problems based on discrete mathematics and algorithmics, and some of our long-term research works have a much wider impact.

4. Application Domains

4.1. Application domains

Our main application domains are:

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

[1] http://csrc.nist.gov/groups/ST/hash/sha-3/

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: Céline Blondeau, Christina Boura, Anne Canteaut, Ayca Cesmelioglu, Pascale Charpin, Benoît Gérard, Stéphane Jacob, Yann Laigle-Chapuy, Stéphane Manuel, Jean-Pierre Tillich.

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 as 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 restricting 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, two very important challenges are the designs of low-cost stream ciphers and of secure hash functions. 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.

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 previous standards (SHA-0, SHA-1...) and some other SHA-3 candidates.
Recent results:

- Evaluation of the security of several constructions for hash functions when the inner primitive is not ideal: [20], [30];
- Cryptanalysis of the successive versions of the SHA-3 candidate MCSSHA-3 : [25];
- Collision attacks on the SHA-3 candidate ESSENCE, and applications to the forge of valid message/MAC pairs for HMAC-ESSENCE-256 and HMAC-ESSENCE-512: [38];
- Internal collisions on the SHA-3 candidate Maraca. Since this attack exploits of a structural property of Sboxes with a low differential uniformity, it points out that, in this context, the use of functions which provide with a good resistance to differential cryptanalysis introduces a weakness: [31];

- study of the algebraic properties based on zero-sum structures. These properties have been recently introduced in order to distinguish a given family of functions from randomly chosen functions. Such structures have been exhibited on the SHA-3 candidates Keccak, Hamsi and Luffa: [29], [28], [40];
- Classification of the disturbance vectors for collision attacks on SHA-1: [17], [12].

5.1.2. Stream ciphers.

Our research work on stream ciphers is a long-term work which is currently developed within the 4-year ANR RAPIDE project. The project-team is involved in some concrete realizations through the international call for proposals eSTREAM. Our work within the RAPIDE project also includes an important cryptanalytic effort on stream ciphers.

Recent results:

- Evaluation of the bias of parity-check relations in the context of cryptanalysis of combination generators with constituent devices which generate period sequences.

5.1.3. Block ciphers.

Even if the security of the current block cipher standard, AES, is not threaten, 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.

Recent results:

- Determination of the data complexity (*i.e.*, of the required number of plaintexts-ciphertexts) and of the success probability of all statistical attacks against block ciphers: an approximation of this complexity was known for differential and linear attacks, but the problem was still open for other types of attacks such as truncated differential attacks: [14];
- Linear cryptanalysis with multiple approximations: [11];
- Differential cryptanalysis with multiple differentials, investigation of several usual hypotheses for differential cryptanalysis and comparison with experiments on the lightweight block cipher Present: [39], [11]

5.1.4. Cryptographic properties and construction of appropriate building blocks.

The construction of building blocks which guarantee a high resistance to 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 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.

Recent results:

- Study of power permutations which are 4-differentially uniform: the motivation of this study is that APN permutations (*i.e.,* 2-differentially uniform) do not exist for power functions, which have a low-cost implementation. In that case, the best resistance to differential attacks is then provided by 4-differentially uniform permutations: [13], [22];

- Construction and study of the properties of new families of permutation polynomials over the field with 2^m elements; study of permutations with a linear structure: [32], [33], [16], [21], [19];
- Study of the properties of the family of power functions with exponents $2^t - 1$. This family notably includes the cube function x^3 and the inverse function over a finite field with characteristic 2. In this work, the whole Walsh spectrum of x^7 is determined: [27].

5.1.5. Symmetric encryption for large databases.

Database encryption is a complex topic. Indeed, we can not apply classical encryption techniques since they will not respect the structure of the databasis and thus will not allow efficient queries. For this reason, a lot of encryption schemes have been proposed specifically for databases purpose with good properties for building indices on encrypted data and therefore querying the databasis efficiently. But they also have their own issues, which mainly result in leaking a lot of information. A proper use of encryption in databases is thus still to be found.

Recent results:

- Security evaluation of some existing techniques for encrypting large databases (this study is a joint work with the SMIS project-team); Cryptanalysis of a fast encryption scheme proposed by Ge and Zdonic [2] and of its tweaked variant: [37], [50].

5.2. Code-based cryptography

Participants: Bhaskar Biswas, Matthieu Finiasz, Rafael Misoczki, Ayoub Otmani, 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 scheme).

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,
- address new functionalities, like hashing or symmetric encryption.

[2] T. Ge and S.B. Zdonik. *Fast, Secure Encryption for Indexing in a Column-Oriented DBMS.* Proceedings of the 23rd International Conference on Data Engineering, ICDE 2007, pages 676-685, 2007.

Recent results:

- Cryptanalysis of several variants of McEliece cryptosystems based on particular families of codes: [18], [36], [42], [41];
- discovery of a distinguishing property for the family of Goppa codes which are used in the original McEliece cipher and the CFS signature scheme; this property invalidates the previously known security proofs of these systems: [43];
- PhD thesis of Bhaskar Biswas on the implementation aspects of code-based cryptosystems:[9].

5.3. Error-correcting codes and applications

Participants: Mamdouh Abbara, Maxime Côte, Matthieu Finiasz, Vincent Herbert, Grégory Landais, Denise Maurice, Sumanta Sarkar, Nicolas Sendrier, Jean-Pierre Tillich.

Decoding algorithms are extensively used for cryptanalyses. For instance, a classical cryptanalysis of the stream ciphers which rely on linear feedback shift register filtered by a Boolean function models the attacked cipher as the result of the transmission of a linear function through a very highly noisy channel. Then, removing the noise amounts to decoding a certain linear code. This code is highly structured, and one of the most efficient methods to decode it exploits the fact that it has low density parity-check equations, and thus can be decoded as a low-density parity-check code, with iterative algorithms. Furthermore, the problem of finding good approximations of ciphers amounts to a decoding problem of the first order Reed-Muller code. Local decoding is then used in this context, and enables various attacks, such as correlation attacks or linear cryptanalysis.

Besides the cryptographic applications of decoding algorithms, we also investigate two new application domains for decoding algorithms: reverse engineering of communication systems, and quantum error correcting codes for which we have shown that some of them can be decoded successfully with iterative decoding algorithms.

5.3.1. Quantum codes.

The knowledge we have acquired in iterative decoding techniques has also led to study whether or not the very same techniques could also be used to decode quantum codes. Part of the old ACI project "RQ" in which we were involved and the new ANR project "COCQ" are about this topic. It is worth noticing that 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: we have constructed for any rate, families of quantum LDPC codes with minimum distance of order the square root of the block-length. This beats all known constructions, most of them having only constant minimum distance. Only very few constructions, namely quantum LDPC codes based on tessellations of surfaces had unbounded minimum distance. For these last examples, the minimum distance was at most logarithmic for non vanishing rates. Our construction does not only display better minimum distance properties, it has many degrees of freedom which opens the way to optimization procedures aiming at maximizing the performances under iterative decoding.
- Quantum turbo-codes: recently, by modifying one of our previous constructions of quantum serial turbo-codes which had the drawback of a constant minimum distance, we have come up with a quantum code of rate $\frac{1}{8}$ with minimum distance of order $\Omega\left(n^{\frac{1}{3}}\right)$ (where n is the block-length) and reducing strongly under iterative decoding the channel noise up to a negligible level for depolarizing

error probability $p \approx 0.146$ [48]. This gives a coding scheme which is almost as good as the celebrated toric codes, but instead of encoding a constant number of qubits it encodes an arbitrary number of them. On the other hand, it is not an error-correcting in the usual sense : there remains a tiny fraction of qubits in error after decoding. However, this is the first construction of a quantum serial turbo-code with good minimum distance where iterative decoding is (almost) successful. It should be interesting to use them in concatenated coding schemes and to study whether other decoding algorithms could be used after iterative decoding in order to clean up the remaining errors.

5.3.2. Reverse engineering of communication systems.

To evaluate the quality of a cryptographic algorithm, it is usually assumed that its specifications are public, as, in accordance with Kerckhoffs principle[3], it would be dangerous to rely, even partially, on the fact that the adversary does not know those specifications. However, this fundamental rule does not mean that the specifications are known to the attacker. In practice, before mounting a cryptanalysis, it is necessary to strip off the data. This reverse engineering process is often subtle, even when the data formatting is not concealed on purpose. A typical case is interception; some raw data, not necessarily encrypted, is observed out of a noisy channel. To access the information, the whole communication system has first to be disassembled and every constituent reconstructed. 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:

- Ph.D thesis of Maxime Côte on code reconstruction: [10];
- new algorithm for reconstruction parallel turbo codes: [34];
- reconstruction of turbo-code interleaver in a noisy context: [35];
- implementation aspects of turbo-code reconstruction: [51].

6. Contracts and Grants with Industry

6.1. Contracts with Industry

- **I2E/AMESYS** ($01/07 \rightarrow 06/10$)
  Recognition of a coding scheme
  Partners: ENSTA, LIX, XLIM, INRIA projet-team SECRET.
  221 kEuros.

  This contract is funded by the DGA AINTERCOM call for offers. The context of this work is the analysis of a binary string in a non-cooperative environment. The purpose is an academic research on related reconstruction problems, with a focus on error-correcting codes.

6.2. Grants with Industry

- **Gemalto** ($01/10 \rightarrow 12/12$)
  CIFRE grant for Christina Boura.

7. Other Grants and Activities

7.1. National Initiatives

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

- **ANR RAPIDE** (01/07 → 03/11)
  Design and analysis of stream ciphers dedicated to constraint environments
  http://rapide-anr2006.gforge.inria.fr/index.html
  Partners: LORIA (project-team CACAO), INRIA (project-team SECRET), INSA Lyon (team Middleware/Security), University of Limoges (XLIM).
  151 kEuros.

  This project focuses on stream ciphers and especially on stream ciphers with an internal state governed by a non-linear transition function. We particularly draw our attention to ciphers whose characteristics make them especially fit constrained environments. These systems were not particularly studied up to now but could be good candidates to the replacement of stream ciphers based on linear transition functions (LFSR based) whose security tends to be less and less satisfying. The results of the project are practical as well as theoretical and concern both design and analysis of such stream ciphers.
- **ANR DEMOTIS** (02/09 → 02/12)
  Collaborative Analysis, Evaluation and Modelling of Health Information Technology
  http://www.demotis.org/
  ANR program: ARPEGE (Systèmes Embarqués et Grandes Infrastructures)
  Partners: Sopinspace, INRIA (project-teams SECRET and SMIS), CNRS/CECOJI
  55 kEuros.
  DEMOTIS brings together computer scientists and legal scholars. The project experiments new methods for the multidisciplinary design of large information systems that have to take in account legal, social and technical constraints. Its main field of application is personal health information systems. Most notably, work is conducted in priority on the infrastructure for the French personal medical file system (DMP) and secondarily on the data infrastructure for the research and public health networks associated with specific diseases (AIDS, cancer).

  At the heart of the DEMOTIS project is the aim to understand how the intrication between the legal and technical domains constrains the design of such data infrastructures. DEMOTIS consists of two interdependent facets: legal and computer science (database security, cryptographical techniques for data protection).
- **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 (Réseaux du Futur et Services)
  Partners: France Telecom, Gemalto, Cryptolog international, EADS SN, Sagem Sécurité, 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 COCQ** (01/09 → 01/12)
  Codes correcteurs quantiques http://www-roc.inria.fr/secret/Jean-Pierre.Tillich/COCQ.html
  ANR program: Domaines émergents
  Partners: ENSEA, INRIA (project-team SECRET), Université de Bordeaux, Telecom ParisTech
  117 kEuros
  This project deals with the development of fundamental research on error correcting codes for quantum channels. In particular, we aim to suggest suitable generalizations to the quantum setting of the best known families of quantum codes (such as LDPC or turbo-codes) and to analyze their performance.

7.2. European Initiatives

Associate member of the ECRYPT II European network of excellence http://www.ecrypt.eu.org/.

7.3. International Initiatives

- Collaboration with Nanyang Technological University (Singapore): visit of Jean-Pierre Tillich at NTU (Feb. 19-27);
- Collaboration with DTU, Denmark: visit of Valérie Gauthier Umana at INRIA (Sept-Nov);
- Collaboration with ISI Calcutta (India), visit of R. Bhattacharyya at INRIA (Sept-Nov).

7.4. Exterior research visitors

- Grigory Kabatianskiy, Institute of Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia, March 13-21.
- Graham Norton, from April 30 to May 18.
- Rafael Misoczki, University of Sao Paulo, Brasil, from May 29 to June 13.
- Sugata Gangopadhyay, Indian Institute of Technology, Roorkee, from May 30 to July 19.
- Valérie Gauthier-Umana, Technical University of Denmark, from Sept. 1 to Nov. 30.
- Rishiraj Bhattacharyya, ISI Calcutta, India, from Sept. 14 to Nov. 13.
- Baudouin Collard, Université Catholique de Louvain-la-Neuve, Nov. 16-19.

8. Dissemination

8.1. Animation of the scientific community

8.1.1. Publishing activities.

- *IEEE Transactions on Information Theory*, associate editor: J.-P. Tillich for *Coding Theory*.
- *Designs, Codes and Cryptography*, associate editor: P. Charpin, since 2003.
- *PQCrypto 2010*, May 25-28, 2010, Darmstadt, Germany, Program chair: N. Sendrier [47].
- *ITW 2010 (IEEE Information Theory Workshop)*, August 30- Sept. 3, Dublin, Ireland, organizer of the session on Quantum information processing: J.P. Tillich.
- *Special issue in Coding and Cryptography*,
  Designs, Codes and Cryptography, Springer, In press.
  Editeurs : M.F. Parker, A. Kholosha, P. Charpin and E. Rosnes. [46].
- *WCC 2010*, April 11-15, 2011, Paris, Program co-chair: A. Canteaut.

8.1.2. Program committees

- 5th Conference on Theory of Quantum Computation, Communication and Cryptography (TQC 2010) : April 13-15, 2010, Leeds, United Kingdom (J.-P. Tillich);
- Eurocrypt 2010: May 30 - June 3, 2010, Nice, France (A. Canteaut);
- Africacrypt 2010: May 3-6, Cairo, Egypt (N. Sendrier);
- PQCrypto 2010: May 25-28, 2010, Darmstadt, Germany (N. Sendrier, program chair);
- SCC 2019: June 23-25, 2010, London, United Kingdom (A. Otmani);
- SAC 2010: August 12-13, 2010, Waterloo, Canada (A. Canteaut);
- SETA 2010: September 12-17, 2010, Paris, France (P. Charpin);
- YACC 2010: October 4-8, 2010, Porquerolles Island, France (A. Canteaut, P. Charpin, N. Sendrier);
- Indocrypt 2010: December 12-15, 2010, Hyderabad, India (A. Canteaut, N. Sendrier);

- FSE 2011: February, 14-16, 2011, Lyngby, Denmark (A. Canteaut);
- Skew 2011: February 16-17, 2011, Lyngby, Denmark (A. Canteaut);
- WCC 2011: April 11-15, 2011, Paris, France (A. Canteaut);
- Africacrypt 2011: July 4-8, 2011, Dakar, Senegal (A. Canteaut, A. Otmani);
- SCC 2011: June 24-25, 2011, Royal Holloway, University of London, UK (A. Otmani);
- SAC 2011: August 11-12, 2011, Ryerson University, Ontario, Canada (A. Canteaut);
- TQC 2011 (6th Conference on Theory of Quantum Computation, Communication and Cryptography): May 24-26, 2011, Universidad Complutense de Madrid Madrid, Spain (J.-P. Tillich);
- ITW 2011: October 16-20, 2011, Paraty, Brazil (N. Sendrier);
- IMA International Conference on Cryptography and Coding: December 12-15, 2011, University of Oxford, UK (P. Charpin).

8.1.3. Other responsibilities in the national community.

- A. Canteaut is a member of the scientific committee of the "UFR de sciences" of the university of Versailles-St Quentin;
- N. Sendrier is a member of the "Commission d'Evaluation" at INRIA;
- **"Commission d'experts"(Committees for the selection of professors and assistant professors, or for the selection of researchers)**: University of Toulon (N. Sendrier), INRIA Grenoble - Rhône-Alpes (N. Sendrier), INRIA Lille - Nord Europe (N. Sendrier), INRIA - DR2 (N. Sendrier);
- A. Canteaut has been co-chair of the postdoc committee for the Paris-Rocquencourt center.

8.2. Ph.D. committees

- S. Kakakhail, *Prédiction et estimation de très faibles taux d?erreurs pour les chaînes de communications codées*, Université de Cergy-Pontoise, January 25, 2010, committee: J.P. Tillich (reviewer).
- M. Côte, *Reconnaissance de codes correcteurs d'erreurs*, Ecole Polytechnique, March 22, 2010, committee: N. Sendrier, J.P. Tillich (supervisors).
- M. Hermelin, *Multidimensional Linear Cryptanalysis*, Aalto University, Helsinki, Finland, June 11, 2010, committee: A. Canteaut (opponent).
- S. Khazaei, *Neutrality-Based Symmetric Cryptanalysis*, EPFL, Switzerland, June 15, committee: A. Canteaut (reviewer).
- L. Dallot *Sécurité de protocoles cryptographiques fondées sur les codes correcteurs d'erreurs*, Université de Caen Basse-Normandie, July 15, 2010, committee: A.Otmani (supervisor), N. Sendrier (reviewer).
- J. Etrog, *Cryptanalyse linéaire et conception de protocoles d'authentification à sécurité prouvée*, Université de Versailles-St Quentin, Sept. 29, committee: A. Canteaut (reviewer).
- G. Leurent, *Construction et analyse de fonctions de hachage*, Université Paris 7, Sept. 30, committee: A. Canteaut (reviewer).
- B. Biswas, *Aspects de mise en oeuvre de la cryptographie basée sur les codes*, Oct 1, 2010, committee: N. Sendrier (supervisor).
- S. Manuel, *Analyse et conception de fonctions de hachage cryptographiques*, Ecole Polytechnique, Nov. 23, 2010, committee: N. Sendrier (supervisor).
- B. Pousse, *Design et cryptanalyse de chiffrements à flot*, Université de Limoges, Dec. 2, 2010, committee: A. Canteaut (reviewer).

- B. Gérard, *Cryptanalyses statistiques des algorithmes de chiffrement à clef secrète*, Dec. 9, 2010, committee: A. Canteaut, J.P. Tillich (supervisor).
- Christophe Guyeux, *Les désordres des itérations chaotiques et leur utilité en sécurité informatique*, Université de Franche-Compté, 13 décembre 2010, committee: P. Charpin (reviewer).

8.3. Teaching

- A. Canteaut, *Symmetric cryptography*, M2, Télécom Paris, 6 h;
- A. Canteaut, *Principles of programming languages*, L3, Ecole Polytechnique, 40 h;
- N. Sendrier, *Error-correcting codes and applications to cryptography*, M2, Mastère MPRI, 32 h ETD;
- J.-P. Tillich, *Introduction to Information Theory*, Ecole Polytechnique, 32 h.
- J.-P. Tillich, *Programs and Algorithms : from sequential to distributed*, M1, Ecole Polytechnique, 32 h.

9. Bibliography

Major publications by the team in recent years

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

[2] A. CANTEAUT, M. VIDEAU. *Symmetric Boolean functions*, in "IEEE Transactions on Information Theory", 2005, vol. 51, n^{o} 8, p. 2791–2811.

[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, p. 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, p. 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, p. 157–174.

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

[7] R. OVERBECK, N. SENDRIER. *Code-based cryptography*, in "Post-Quantum Cryptography", D. BERNSTEIN, J. BUCHMANN, E. DAHMEN (editors), Springer, 2009, p. 95-145.

[8] J.-P. TILLICH, G. ZÉMOR. *Collisions for the LPS expander graph hash function*, in "Advances in Cryptology - EUROCRYPT 2008", LNCS, Springer, 2008, n^{o} 4965, p. 254–269.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[9] B. BISWAS. *Aspects de mise en oeuvre de la cryptographie basée sur les codes*, Ecole Polytechnique, Oct 2010, http://pastel.archives-ouvertes.fr/pastel-00523007/fr/.

[10] M. CÔTE. *Reconnaissance de codes correcteurs d'erreurs*, Ecole Polytechnique, Mar 2010, http://pastel.archives-ouvertes.fr/pastel-00006125/fr/.

[11] B. GÉRARD. *Cryptanalyses statistiques des algorithmes de chiffrement à clef secrète*, Université Pierre et Marie Curie, December 2010.

[12] S. MANUEL. *Analyse et conception de fonctions de hachage cryptographiques*, École Polytechnique, Palaiseau, November 2010.

Articles in International Peer-Reviewed Journal

[13] C. BLONDEAU, A. CANTEAUT, P. CHARPIN. *Differential Properties of Power Functions*, in "International Journal of Information and Coding Theory", 2010, vol. 1, n^{o} 2, p. 149-170, Special Issue in honor of Vera Pless. Invited paper., http://dx.doi.org/10.1504/IJICOT.2010.032132.

[14] C. BLONDEAU, B. GÉRARD, J.-P. TILLICH. *Accurate Estimates of the Data Complexity and Success Probability for Various Cryptanalyses*, in "Designs, Codes and Cryptography", 2010, In press, http://dx.doi.org/10.1007/s10623-010-9452-2.

[15] P.-L. CAYREL, C. CHABOT, A. NECER. *Quasi-cyclic codes over ring of matrices*, in "Finite Fields and Their Applications", March 2010, vol. 16, n^{o} 2, p. 100-115, http://dx.doi.org/10.1016/j.ffa.2010.01.001.

[16] P. CHARPIN, S. SARKAR. *Polynomials with Linear Structure and Maiorana-McFarland Construction*, in "IEEE Transactions on Information Theory", 2010, To appear.

[17] S. MANUEL. *Classification and Generation of Disturbances Vectors for Collision Attacks against SHA-1*, in "Designs, Codes and Cryptography", 2010, In press.

[18] A. OTMANI, J.-P. TILLICH, L. DALLOT. *Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes*, in "Mathematics in Computer Science", 2010, vol. 3, n^{o} 2, p. 129-140, http://dx.doi.org/10.1007/s11786-009-0015-8.

[19] E. PASALIC, P. CHARPIN. *Some results concerning cryptographically significant mappings over $GF(2^n)$*, in "Designs, Codes and Cryptography", 2010, vol. 57, n^{o} 3, p. 257-269, http://dx.doi.org/10.1007/s10623-010-9365-0.

Invited Conferences

[20] A. CANTEAUT. *Capturing the existence of distinguishers into indifferentiability proofs for hash functions*, in "Early Symmetric Crypto (ESC) seminar", Remich, Luxemburg, January 2010, https://cryptolux.org/ESC/Anne_Canteaut.

[21] P. CHARPIN. *On permutation polynomials of the shape* $G(X) + \lambda Tr(H(X))$, in "Algebraic and Combinatorial Coding Theory - ACCT 10", Akademgorodok, Russia, September 2010.

[22] P. CHARPIN. *Permutations with small differential uniformity*, in "Antalya Algebra Days XII", Antalya, Turkey, May 2010.

[23] N. SENDRIER. *On the Key Security of Code-based Public-key Cryptosystems*, in "Workshop on Post-Quantum Security Models", Télécom ParisTech, Paris, October 2010, http://iq.enst.fr/workshop/docs/PQSM_NicolasSendrier.pdf.

[24] N. SENDRIER. *On the Use of Structured Codes in Code Based Cryptography*, in "Coding Theory and Cryptography III", The Royal Flemish Academy of Belgium for Science and the Arts, 2010.

International Peer-Reviewed Conference/Proceedings

[25] J.-P. AUMASSON, M. NAYA-PLASENCIA. *Second preimages on MCSSHA-3*, in "Western European Workshop on Research in Cryptology - WEWoRC 2009", Graz, Austria, LNCS, Springer, 2010, vol. 6429, to appear.

[26] B. BISWAS, V. HERBERT. *Efficient root finding of polynomials over fields of characteristic 2*, in "Western European Workshop on Research in Cryptology - WEWoRC 2009", Graz, Austria, LNCS, Springer, 2010, vol. 6429, to appear.

[27] C. BLONDEAU, A. CANTEAUT, P. CHARPIN. *Differential properties of power functions*, in "IEEE International Symposium on Information Theory - ISIT 2010", Austin, USA, IEEE Press, June 2010, p. 2478-2482, http://dx.doi.org/10.1109/ISIT.2010.5513437.

[28] C. BOURA, A. CANTEAUT. *A Zero-Sum property for the Keccak-f Permutation with 18 Rounds*, in "IEEE International Symposium on Information Theory - ISIT 2010", Austin, USA, IEEE Press, June 2010, p. 2488-2492, http://dx.doi.org/10.1109/ISIT.2010.5513442.

[29] C. BOURA, A. CANTEAUT. *Zero-sum Distinguishers for Iterated Permutations and Application to Keccak-f and Hamsi-256*, in "Selected Areas in Cryptography - SAC 2010", LNCS, Springer-Verlag, 2010, to appear.

[30] E. BRESSON, A. CANTEAUT, T. FUHR, T. ICART, M. NAYA-PLASENCIA, P. PAILLIER, J.-R. REINHARD, M. VIDEAU. *Internal Distinguishers in Indifferentiable Hashing: The Shabal Case*, in "The second SHA-3 Candidate Conference", Santa Barbara, USA, August 2010, http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/documents/papers/Canteaut_extended_abstract.pdf.

[31] A. CANTEAUT, M. NAYA-PLASENCIA. *Structural weaknesses of permutations with a low differential uniformility and generalized crooked functions*, in "Finite Fields: Theory and Applications - FQ9", Contemporary Mathematics, AMS, 2010, vol. 518, p. 55-71.

[32] P. CHARPIN, G. KYUREGHYAN. *Monomial functions with linear structure and permutation polynomials*, in "Finite Fields: Theory and Applications - FQ9", Contemporary Mathematics, AMS, 2010, vol. 518, p. 99-111.

[33] P. CHARPIN, S. SARKAR. *Polynomials with Linear Structure and Maiorana-McFarland Construction*, in "IEEE International Symposium on Information Theory - ISIT 2010", Austin, USA, IEEE Press, June 2010, p. 2737-2741, http://dx.doi.org/10.1109/ISIT.2010.5513680.

[34] M. CLUZEAU, M. FINIASZ, J.-P. TILLICH. *Methods for the Reconstruction of Parallel Turbo Codes*, in "IEEE International Symposium on Information Theory - ISIT 2010", Austin, USA, IEEE Press, June 2010, p. 2008-2012, http://dx.doi.org/10.1109/ISIT.2010.5513365.

[35] M. CÔTE, N. SENDRIER. *Reconstruction of a turbo-code interleaver from noisy observation*, in "IEEE International Symposium on Information Theory - ISIT 2010", Austin, USA, IEEE Press, June 2010, p. 2003-2007, http://dx.doi.org/10.1109/ISIT.2010.5513364.

[36] 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, p. 279-298, http://dx.doi.org/10.1007/978-3-642-13190-5_14.

[37] S. JACOB. *Cryptanalysis of a Fast Encryption Scheme for Databases*, in "IEEE International Symposium on Information Theory - ISIT 2010", Austin, USA, IEEE Press, June 2010, p. 2468-2472, http://dx.doi.org/10.1109/ISIT.2010.5513546.

[38] M. NAYA-PLASENCIA, A. RÖCK, J.-P. AUMASSON, Y. LAIGLE-CHAPUY, G. LEURENT, W. MEIER, T. PEYRIN. *Cryptanalysis of ESSENCE*, in "Fast Software Encryption - FSE 2010", LNCS, Springer, 2010, vol. 6147, http://dx.doi.org/10.1007/978-3-642-13858-4_8.

Workshops without Proceedings

[39] C. BLONDEAU, B. GÉRARD. *Links Between Theoretical and Effective Differential Probabilities: Experiments on PRESENT*, in "Workshop on Tools for Cryptanalysis 2010", June 2010, http://eprint.iacr.org/2010/261.

[40] C. BOURA, A. CANTEAUT, C. DE CANNIÈRE. *Beware of optimistic weather forecast*, in "Crypto 2010", Santa Barbara, USA, August 2010, rump session.

[41] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *Algebraic cryptanalysis of McEliece variants with compact keys - Towards a Complexity Analysis*, in "Yet Another Conference on Cryptography - YACC 2010", Porquerolles Island, France, October 2010.

[42] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *Algebraic cryptanalysis of McEliece variants with compact keys - Towards a Complexity Analysis*, in "International Conference on Symbolic Computation and Cryptography - SCC 2010", Royal Holloway, University of London, Egham, UK, C. CID, J.-C. FAUGÈRE (editors), June 2010, p. 45-55.

[43] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *Distinguisher for High Rate McEliece Cryptosystem*, in "Yet Another Conference on Cryptography - YACC 2010", Porquerolles Island, France, October 2010.

[44] S. GANGOPADHYAY, B. K. SINGH. *On second-order nonlinearities of some D_0 type bent functions*, in "10th Central European Conference on Cryptology", Bedlewo, Poland, June 2010.

[45] C. SAUVAGET, S. MANUEL, J. VITTAUT, J. SUAREZ, V. BOYER. *Segmented Images Colorization Using Harmony*, in "6th International Conference on Signal Image Technology and Internet Based Systems – SITIS 2010", Kuala Lumpur, Malaysia, December 2010.

Books or Proceedings Editing

[46] P. CHARPIN, A. KHOLOSHA, M. PARKER, E. ROSNES (editors). *Special issue in Coding and Cryptography*, Designs, Codes and Cryptography, Springer-Verlag, 2010, In press.

[47] N. SENDRIER (editor). *Post-Quantum Cryptography - PQCrypto 2010*, LNCS, Springer, Darmstadt, Germany, May 2010, vol. 6061, http://dx.doi.org/10.1007/978-3-642-12929-2.

Other Publications

[48] M. ABBARA, J.-P. TILLICH. *An excellent error-reducing code*, January 2011, Quantum Information Processing - QIP 2011, poster session.

[49] I. ANDRIYANOVA, J.-P. TILLICH. *On a Low-Rate TLDPC Code Ensemble and the Necessary Condition on the Linear Minimum Distance for Sparse-Graph Codes*, 2010, CoRR abs/1010.1911, http://arxiv.org/abs/1010.1911.

[50] S. JACOB. *Cryptanalysis of a Fast Encryption Scheme for Databases and of its Variant*, 2010, Report, http://hal.inria.fr/inria-00530733.

[51] C. MAVROMATI. *Mise en oeuvre d'un algorithme de reconnaissance d'un turbo-code*, Université Paris 7, September 2010, Supervisor: Nicolas Sendrier.