Activity Report 2012

Project-Team SECRET

Security, Cryptology and Transmissions

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithms, Certification, and Cryptography

Table of contents

Project-Team SECRET

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

Creation of the Project-Team: July 01, 2008 .

1. Members

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]
Anthony Leverrier [On leave from Corps des Mines, since November 2012]
María Naya-Plasencia [Junior Researcher (CR) Inria, since September 2012]
Jean-Pierre Tillich [Junior Researcher (CR) Inria, HdR]

PhD Students

Mamdouh Abbara [On leave from Corps des Mines, until September 2012]
Marion Bellard [Ministère de la défense, Univ. P. et M. Curie]
Christina Boura [CIFRE grant, Univ. P. et M. Curie]
Stéphane Jacob [AMX grant, Univ. P. et M. Curie, until March 2012]
Grégory Landais [DGA grant, Univ. P. et M. Curie]
Denise Maurice [AMN grant, Univ. P. et M. Curie]
Rafael Misoczki [Inria grant, Univ. P. et M. Curie]
Joëlle Roué [Inria grant, Univ. P. et M. Curie, since September 2012]
Jean-Christophe Sibel [Inria grant, Univ. Cergy, until August 2012]
Valentin Suder [DGA grant, Univ. P. et M. Curie]
Audrey Tixier [Ministère de la défense, Univ. P. et M. Curie, since October 2012]

Post-Doctoral Fellows

Baudoin Collard [until January 2012]
Dimitrios Simos [ERCIM, from March 2012]

Visiting Scientist

Gohar Kyureghyan [On leave from Otto-von-Guericke Universität Magdeburg, until June 2012]

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.

2.2. Highlights of the Year

- Extensive study of the hash function proposal Keccak, which has been chosen as the winner of the SHA-3 competition. The analysis of the algebraic properties of Keccak due to C. Boura and A. Canteaut is the best known result on the new hash function standard.
- Design of a variant of the McEliece public-key cipher based on a moderate density parity-check codes (MDPC). This family of codes leads to public keys with a reasonable size and does not weaken the underlying security proof.
- Construction of spatially coupled quantum LDPC codes which performs well under iterative decoding almost up to the coherent capacity of the quantum channel.

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 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.

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.

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: Christina Boura, Baudoin Collard, Anne Canteaut, Pascale Charpin, Gohar Kyureghyan, 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 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, 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 previous standards (SHA-0, SHA-1...) and some other SHA-3 candidates.
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 [12], [22], [9].
- Side-channel attacks on two SHA-3 candidates, Skein and Grøstl, when they are used with HMAC, and counter-measures [23], [50].
- Indifferentiability results for a broadened mode of operation including the modes based on block ciphers, and modes based on un-keyed functions [51].

5.1.2. Block ciphers.

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

- Algebraic analysis of some recent lightweight block ciphers, including LED and Piccolo [24].
- Analysis of the security of the lightweight block cipher mCRYPTON [56].
- Design of a new block cipher, named PRINCE, with a very low-latency, leading to instantaneous encryption (i.e., within one clock cycle) with a very competitive chip area [21], [49].
- Analysis of the differential properties of the AES Superbox [58].
- Study of the significance of the related-key and known-key models for block ciphers [48].

5.1.3. Stream ciphers.

The project-team has been involved in the international project eSTREAM, which aimed at recommending some secure stream ciphers.

Recent results:

- Generalisation of several improvements of the so-called correlation attacks against stream ciphers and study of their complexities [13].
- Study of the bias of parity-check relations for combination generators used in stream ciphers [14].

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, 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 [26].
- Study of the planarity of some mappings, including products of linearized polynomials [25], [16].
- Definition of a new criterion for Sboxes and link with some recent algebraic attacks on the hash functuion Hamsi [29], [9].
- Survey of PN and APN mappings [42].

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 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.

Recent results:

- A new variant of McEliece using Moderate Density Parity Check (MDPC) codes [55];
- An optimized software implementation of the code-based digital signature scheme CFS [27];
- An attack on a homomorphic encryption scheme [53];
- An attack on a variant of the McEliece cryptosystem based on Reed-Solomon codes [54].

5.3. Error-correcting codes and applications

Participants: Mamdouh Abbara, Marion Bellard, Denise Maurice, Nicolas Sendrier, Jean-Christophe Sibel, Jean-Pierre Tillich, Audrey Tixier.

We mainly 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 obtained by transforming a quantum CSS LDPC code into a code over a larger alphabet which improves substantially the performances under iterative decoding [18];
- Construction of spatially coupled quantum LDPC codes which performs well under iterative decoding almost up to the coherent capacity of the quantum channel [19].

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 [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, 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 and the French Ministry for Defense.

Recent results:

- Recontruction of the constellation labeling (i.e. used in the modulator of a communication system) in presence of error and when the underlying code is convolutional [20].

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Grants with Industry

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

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- **ANR DEMOTIS** ($02/09 \rightarrow 02/12$)
  Collaborative Analysis, Evaluation and Modelling of Health Information Technology
  http://www.demotis.org/
  ANR program: ARPEGE (Systèmes Embarques 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). The aim is to understand how the intrication between the legal and technical domains affects the design of such data infrastructures.

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

- **ANR SAPHIR-2** ($03/09 \rightarrow 03/13$)
  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 COCQ** ($01/09 \rightarrow 07/12$)
  Codes correcteurs quantiques
  http://www-roc.inria.fr/secret/Jean-Pierre.Tillich/COCQ.html
  ANR program: Domaines emergents
  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.
- **ANR BLOC** ($10/11 \rightarrow 09/15$)
  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** ($12/11 \rightarrow 12/15$)
  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.

7.1.2. Others

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

7.2. European Initiatives

Associate member of the ECRYPT II European network of excellence ($08/08 \rightarrow 07/12$) http://www.ecrypt.eu.org/

7.2.1. Collaborations with Major European Organizations

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

Symmetric crytography and code-based cryptography

7.3. International Research Visitors

7.3.1. Visits of International Scientists

- Gohar Kyureghyan, Otto-von-Guericke Universität Magdeburg, Germany, from October 2011 to June 2012
- Davide Schipani, Universität Zurich, Switzerland, February 13-17
- Sergey Abrahamyan, Institute for Informatics and Automation Problems, Yerevan, Armenia, May 20-26
- Yves Edel, Gent University, Belgium, June 3-9
- Christiane Peters, DTU, Denmark, November 19-23
- Stefan Heyse, Ingo von Maurich and Ralf Zimmermann, Ruhr-Universität Bochum, Germany, November 19-23
- Grigory Kabatyanskiy, IPIT, Moscow, Russia, December 17-21 .

7.3.2. Visits to International Teams

- DTU-Mathematics, Denmark Technical University, Denmark, January-August, 8-month sabbatical stay funded by the DGA (A. Canteaut).
- School of Informatics, University of Edinburgh, Scotland, December 3-6, invitation to the *Quantum Security Meeting*, and visit of Elham Kashefi's group (A. Leverrier).

8. Dissemination

8.1. Scientific Animation

8.1.1. Editorial activities.

- *IEEE Transactions on Information Theory*, associate editor: J.-P. Tillich for *Coding Theory*.
- *Designs, Codes and Cryptography*, associate editor: P. Charpin, since 2003.
- *RAIRO - Theoretical Informatics and Applications*, associate editor: N. Sendrier.
- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, 2012, co-editor: A. Canteaut.
- *FSE 2012 (Fast Software Encryption)*: March, 19-21, 2012, Washington DC, USA, Program chair and editor of the proceedings: 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 is a member of the steering committee of *Fast Software Encryption (FSE)*;
- N. Sendrier is a member of the steering committee of *Post-quantum cryptography (PQCrypto)*.

8.1.2. Program committees

- FSE 2012: March 19-21, 2012, Washington DC, USA (A. Canteaut, program chair);

- PKC 2012: May 21-23, 2012, Darmstadt, Germany (N. Sendrier);
- SETA 2012, June 4-8, 2012, Waterloo, Canada (P. Charpin);
- SAC 2012: August 16-17, 2012, Windsor, Ontario, Canada (A. Canteaut);
- *RICAM-Workshop on Finite Fields and Their Applications: Character Sums and Polynomials*, September 2-7, 2012, St. Wolfgang Federal Institute, Austria (P. Charpin);
- YACC 2012, September 24-28, 2012, Porquerolles, France (A. Canteaut);
- Journées Codage et Cryptographie du GDR-IM, October 7-12, 2012, Dinard, France (A. Canteaut);
- Indocrypt 2012: December 9-12, 2012, Calcutta, India (N. Sendrier);
- 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, Limoges, France (N. Sendrier, JP Tillich);
- Asiacrypt 2013: December 1-5, Bengaluru, India (A. Canteaut, N. Sendrier);

8.1.3. Invited talks

- N. Sendrier. *Code-based Cryptography: Theory and Practice.* ARES, MoCrySEn 2012, Prague, Czech Republic, September 2012.
- N. Sendrier. *Code-based Cryptography*. Post-Quantum Cryptography and Quantum Algorithms, Lorentz Center, Leiden, The Netherlands, November 2012.
- D.E. Simos. *Families of Block Ciphers from Combinatorial Designs*. In Cryptography and its Applications in the Armed Forces (CAIAF2012) , Hellenic Military Academy "Evelpidon", Vari, Greece, April 2012.

8.1.4. Other responsibilities in the national community.

- N. Sendrier is a vice-chair of the "Commission d'Evaluation" at Inria;
- A. Canteaut is a member of the "Comité de pilotage" of the Fondation Sciences Mathématiques de Paris;
- JP Tillich is in charge of "Formation par la recherche" for the Paris-Rocquencourt center.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- A. Canteaut, *Stream ciphers*, 6 hours, M2, Telecom ParisTech, France;
- A. Canteaut, *Mathematical aspects of symmetric cryptographŷ*, 3 hours, M2 (corps de Mines), Telecom ParisTech, France;
- A. Canteaut, *Advanced topics in symmetric cryptology*, 9 hours, M2, DTU, Denmark;
- J.-P. Tillich, *Algorithms and Programming*, 36 hours, M1, Ecole Polytechnique, France;
- J.-P. Tillich, *Introduction to Information Theory*, 32 hours, M2, Ecole Polytechnique, France.

8.2.2. Supervision

PhD: Christina Boura, *Sécurité et cryptanalyse des fonctions de hachage*, Université Pierre-et-Marie Curie, December 2012, supervisor: A. Canteaut

PhD: Stéphane Jacob, *Protection cryptographique des bases de données : conception et cryptanalyse*, Université Pierre-et-Marie Curie, March 2012, supervisor: A. Canteaut

PhD in progress: Mamdouh Abbara, *Quantum turbo-codes*, August 2009, supervisor: JP. Tillich.

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

PhD in progress: Grégory Landais, *Mise en oeuvre des cryptosystèmes basés sur les codes correcteurs d'erreurs et de leurs cryptanalyse*, October 2010, supervisors: M. Finiasz and N. Sendrier
PhD in progress: Denise Maurice, *Quantum LDPC codes*, September 2010, supervisor : JP. Tillich.
PhD in progress: Rafael Misoczki, *Aspects of code-based cryptography*, November 2010, supervisor: N. Sendrier
PhD in progress: Jean-Christophe Sibel, *Decoding LDPC codes with many short cycles*, October 2009, supervisor : D. Declercq.
PhD in progress: Valentin Suder, *Les Permutations en Cryptographie Symétrique*, October 2011, supervisor: P. Charpin.
PhD in progress: Audrey Tixier, *Reconstruction of LDPC codes*, October 2012, supervisor: JP. Tillich

8.2.3. Juries

- Jean-Claude Carlach, *Contribution à la construction et au décodage à décision douce des codes correcteurs d'erreurs auto-duaux extrémaux*, Institut National des Sciences Appliquées de Rennes, February 2, 2012, committee: JP. Tillich.
- Stéphane Jacob, *Protection cryptographique des bases de données : conception et cryptanalyse*, Université Pierre-et-Marie Curie, March 8, 2012, committee: A. Canteaut (supervisor).
- Marine Minier, *Quelques résultats en cryptographie symétrique, pour les modèles de confiance dans les réseaux ambiants et la sécurité dans les réseaux de capteurs sans fil*, HDR, Université Lyon 1, May 31, 2012, committee: A. Canteaut.
- Pouyan Sepehrdad, *Statistical and Algebraic Cryptanalysis of Lightweight and Ultra-Lightweight Symmetric Primitives*, Ecole Polytechnique Fédérale de Lausanne, Suisse, June 11, 2012, committee: A. Canteaut (reviewer).
- Matteo Gorgoglione, *Analyse et construction de codes LDPC non-binaires pour des canaux à évanouissement*, Université de Cergy-Pontoise, October 25, 2012, committee: JP. Tillich (reviewer).
- Anja Becker, *The representation technique – Applications to hard problems in cryptography*, UVSQ, Octobre 26, 2012, committee: N. Sendrier (reviewer).
- Matthieu Legeay, *Utilisation du groupe de permutations d'un code correcteur pour améliorer l'efficacité du décodage*, Université de Rennes 1, November 20, 2012, committee: N. Sendrier (reviewer).
- Christina Boura, *Sécurité et cryptanalyse des fonctions de hachage*, Université Pierre-et-Marie Curie, December 7, 2012, committee: A. Canteaut (supervisor).
- Sihem Mesnager, *Contributions aux fonctions booléennes pour la cryptographie symétrique et aux codes correcteurs d'erreurs*, HDR, Université Paris 8, December 10, 2012, committee: P. Charpin (reviewer), A. Canteaut.
- N. Delfosse, *Constructions et performances de codes LDPC quantiques*, Université Bordeaux I, December 12, 2012, committee: JP. Tillich (reviewer).

8.3. Popularization

- Anne Canteaut is a co-author of a paper on the state-of-the-art on the AES standard in the large-audience journal *MISC* [17].
- Lecture on cryptography at the *Journées Filles et Maths*, organized by Animath and Femmes et Sciences, for students in "Première" and "Terminale", IHP, Paris, December 21, 2012, A. Canteaut.
- Lectures (6h in total) to an audience of professors in "classes preparatoires" on quantum algorithms, Luminy, May 9, 2012, 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, p. 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, 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] 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.

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

Publications of the year

Doctoral Dissertations and Habilitation Theses

[9] C. BOURA. *Analyse de fonctions de hachage cryptographiques*, Université Pierre et Marie Curie - Paris VI, December 2012, http://tel.archives-ouvertes.fr/tel-00767028.

[10] S. JACOB. *Protection cryptographique des bases de données : conception et cryptanalyse*, Université Pierre et Marie Curie - Paris VI, March 2012, http://hal.inria.fr/tel-00738272.

Articles in International Peer-Reviewed Journals

[11] I. ANDRIYANOVA, J.-P. TILLICH. *Designing a Good Low-Rate Sparse-Graph Code*, in "IEEE Transactions on Communications", 2012, vol. 60, n^{o} 11, p. 3181-3190.

[12] 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", 2012, p. 1-12, To appear, http://hal.inria.fr/hal-00738398.

[13] A. CANTEAUT, M. NAYA-PLASENCIA. *Correlation attacks on combination generators*, in "Cryptography and Communications", 2012, vol. 4, n^{o} 3-4, p. 147–171.

[14] A. CANTEAUT, M. NAYA-PLASENCIA. *Parity-Check Relations on Combination Generators*, in "IEEE Transactions on Information Theory", 2012, vol. 58, n^{o} 6, p. 3900–3911.

[15] C. KOUKOUVINOS, D. E. SIMOS. *Encryption Schemes from Williamson Matrices*, in "Journal of Information Assurance and Security", 2012, vol. 7, n^{o} 6, p. 252-258.

[16] G. M. KYUREGHYAN, F. ÖZBUDAK. *Planarity of products of linearized polynomials*, in "Finite Fields and Applications", 2012, vol. 18, n^{o} 6, p. 87–114.

Articles in Non Peer-Reviewed Journals

[17] A. CANTEAUT, M. MINIER. *De l'espérance de vie d'un algorithme symétrique (ou l'AES dix ans après)*, in "MISC", April-May 2012, n^{o} HS 5, p. 12-19.

International Conferences with Proceedings

[18] I. ANDRIYANOVA, D. MAURICE, J.-P. TILLICH. *Quantum LDPC codes obtained by non-binary constructions*, in "IEEE International Symposium on Information Theory - ISIT 2012", Boston, USA, July 2012, p. 343-347.

[19] I. ANDRIYANOVA, D. MAURICE, J.-P. TILLICH. *Spatially coupled quantum LDPC codes*, in "IEEE Information Theory worksop - ITW2012", Lausanne, Switzerland, 2012, p. 327–331.

[20] M. BELLARD, N. SENDRIER. *Recognition of constellation labeling with convolutional coded data*, in "2012 International Symposium on Information Theory and its Applications - ISITA 2012", Honolulu, Hawaii, USA, IEEE, October 2012, p. 653-657.

[21] J. BORGHOFF, A. CANTEAUT, T. GÜNEYSU, E. B. KAVUN, M. KNEZEVIC, L. R. KNUDSEN, G. LEANDER, V. NIKOV, C. PAAR, C. RECHBERGER, P. ROMBOUTS, S. S. THOMSEN, T. YALÇIN. *PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications*, in "Advances in Cryptology - ASIACRYPT 2012", Beijing, China, Lecture Notes in Computer Science, Springer, December 2012, vol. 7658, p. 208-225.

[22] C. BOURA, A. CANTEAUT. *On the Algebraic Degree of some SHA-3 Candidates*, in "The third SHA-3 candidate conference", Washington DC, USA, March 2012, http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/March2012/documents/papers/BOURA_CANTEAUT_paper.pdf.

[23] C. BOURA, S. LÉVÊQUE, D. VIGILANT. *Side-channel Analysis of Grøstl and Skein*, in "Security and Privacy Workshops (SPW), 2012", San Francisco, United States, IEEE, 2012, p. 16-26, http://hal.inria.fr/hal-00738410.

[24] V. GROSSO, C. BOURA, B. GÉRARD, F.-X. STANDAERT. *A Note on the Empirical Evaluation of Security Margins against Algebraic Attacks (with Application to Low Cost Ciphers LED and Piccolo)*, in "The 33rd WIC Symposium on Information Theory in the Benelux", Boekelo, The Netherlands, May 2012, p. 52-59.

[25] G. M. KYUREGHYAN, F. ÖZBUDAK, A. POTT. *Some planar maps and related function fields*, in "Arithmetic, Geometry, Cryptography and Coding Theory", Contemporary Mathematics, 2012, vol. 574, p. 87-114.

[26] G. M. KYUREGHYAN, V. SUDER. *On inverses of APN exponents*, in "IEEE International Symposium on Information Theory - ISIT 2012", Boston, USA, July 2012, p. 1207-1211.

[27] G. LANDAIS, N. SENDRIER. *Implementing CFS*, in "Progress in Cryptology - INDOCRYPT 2012", Lecture Notes in Computer Science, Springer-Verlag, 2012, vol. 7668, p. 474-488.

Conferences without Proceedings

[28] M. BELLARD. *Reconstruction du "mapping" en présence d'un codage convolutif*, in "Journées "Codage et Cryptographie 2012"", Dinard, Bretagne, October 2012, http://webmath.univ-rennes1.fr/c2/.

[29] C. BOURA. *Sur la propagation de relations linéaires au travers d'une S-box*, in "Journées "Codage et Cryptographie 2012"", Dinard, Bretagne, October 2012, http://webmath.univ-rennes1.fr/c2/.

[30] A. CANTEAUT. *Promenade mathématique : Comment concevoir un chiffrement rapide et solide*, in "Journées "Filles et Maths"", IHP, Paris, December 2012, http://www.animath.fr/spip.php?article447.

[31] G. LANDAIS. *CFS Software Implementation*, in "CBC 2012", DTU, Lyngby, Denmark, May 2012.

[32] G. LANDAIS. *Implementation de CFS*, in "Journées "Codage et Cryptographie 2012"", Dinard, Bretagne, October 2012, http://webmath.univ-rennes1.fr/c2/.

[33] D. MAURICE. *Codes LDPC quantiques non binaires*, in "Journées "Codage et Cryptographie 2012"", Dinard, Bretagne, October 2012, http://webmath.univ-rennes1.fr/c2/.

[34] R. MISOCZKI. *Improved LDPC and QC-LDPC McEliece variants*, in "CBC 2012", DTU, Lyngby, Denmark, May 2012.

[35] R. MISOCZKI. *Nouvelles variantes de McEliece à partir de codes de parité à densité modérée*, in "Journées "Codage et Cryptographie 2012"", Dinard, Bretagne, October 2012, http://webmath.univ-rennes1.fr/c2/.

[36] N. SENDRIER. *Code-based Cryptography*, in "Post-Quantum Cryptography and Quantum Algorithms", Lorentz Center, Leiden, The Netherlands, November 2012, Invited lecture.

[37] N. SENDRIER. *Code-based Cryptography: Theory and Practice*, in "ARES, MoCrySEn 2012", Prague, Czech Republic, September 2012, Invited lecture.

[38] D. E. SIMOS. *Families of Block Ciphers from Combinatorial Designs*, in "Cryptography and its Applications in the Armed Forces (CAIAF2012)", Hellenic Military Academy "Evelpidon", Vari, Greece, April 2012, Invited talk.

[39] D. E. SIMOS. *Quelle est la difficulté de l'équivalence de codes sur $GF(q)$?*, in "Journées "Codage et Cryptographie 2012"", Dinard, Bretagne, October 2012, http://webmath.univ-rennes1.fr/c2/.

[40] D. E. SIMOS. *The Support Splitting Algorithm and its application to Code-based Cryptography*, in "CBC 2012", DTU, Lyngby, Denmark, May 2012.

[41] V. SUDER. *Sur les inverses d'exposants APN*, in "Journées "Codage et Cryptographie 2012"", Dinard, Bretagne, October 2012, http://webmath.univ-rennes1.fr/c2/.

Scientific Books (or Scientific Book chapters)

[42] P. CHARPIN. *PN and APN functions*, in "Handbook of Finite Fields", G. L. MULLEN, D. PANARIO (editors), 2012, chap. Special functions over finite fields, To appear.

[43] G. M. KYUREGHYAN. *Special mappings of finite fields*, in "Finite Fields and Their Applications. Character Sums and Polynomials", Radon Series on Computational and Applied Mathematics, De Gruyter, 2012, To appear.

Books or Proceedings Editing

[44] D. AUGOT, A. CANTEAUT, G. M. KYUREGHYAN, F. SOLOV'EVA, Ø. YTREHUS (editors). *Special issue in Coding and Cryptography*, Designs, Codes and Cryptography, Springer, 2012, To appear [*DOI :* 10.1007/s10623-012-9731-1], http://hal.inria.fr/hal-00741923.

[45] A. CANTEAUT (editor). *Fast Software Encryption - 19th International Workshop, FSE 2012. Revised Selected Papers*, Lecture Notes in Computer Science, Springer, Washington, DC, USA, March 2012, vol. 7549.

[46] D. E. SIMOS (editor). *Workshop on Modern Cryptography and Security Engineering – MocrySen 2012*, IEEE CPS, Prague, Czech Republic, August 20-24, 2012.

Other Publications

[47] I. ANDRIYANOVA, D. MAURICE, J.-P. TILLICH. *New constructions of CSS codes obtained by moving to higher alphabets*, 2012, full version of a paper submitted to the IEEE Symposium on Information Theory, http://hal.inria.fr/hal-00671659.

[48] T. BAIGNÈRES, A. CANTEAUT, Y. SEURIN, T. FUHR, M. FINIASZ, M. MINIER. *Security Models*, November 2012, Delivrable 1 (Subtask 2.1) - Deliverable for the ANR project BLOC.

[49] J. BORGHOFF, A. CANTEAUT, T. GÜNEYSU, E. B. KAVUN, M. KNEZEVIC, L. R. KNUDSEN, G. LEANDER, V. NIKOV, C. PAAR, C. RECHBERGER, P. ROMBOUTS, S. S. THOMSEN, T. YALÇIN. *PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications (Full version)*, 2012, Cryptology ePrint Archive, Report 2012/529, http://eprint.iacr.org/2012/529.

[50] C. BOURA. *Intermediate results on physical analysis of phase-2 candidates*, March 2012, Delivrable D2.1 - Deliverable for the ANR Project Saphir 2.

[51] A. CANTEAUT, T. FUHR, M. NAYA-PLASENCIA, P. PAILLIER, J.-R. REINHARD, M. VIDEAU. *A Unified Indifferentiability Proof for Permutation- or Block Cipher-Based Hash Functions*, 2012, Cryptology ePrint Archive, Report 2012/363, http://eprint.iacr.org/2012/363.

[52] T. FRITZ, A. LEVERRIER, A. BELÉN SAINZ. *A Combinatorial Approach to Nonlocality and Contextuality*, December 2012, arXiv:1212.4084, http://arxiv.org/abs/1212.4084.

[53] V. GAUTHIER, A. OTMANI, J.-P. TILLICH. *A Distinguisher-Based Attack of a Homomorphic Encryption Scheme Relying on Reed-Solomon Codes*, 2012, IACR Cryptology ePrint Archive, Report 2012/168, http://eprint.iacr.org/2012/168.

[54] V. GAUTHIER, A. OTMANI, J.-P. TILLICH. *A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes*, April 2012, arXiv:1204.6459, http://arxiv.org/abs/1204.6459.

[55] R. MISOCZKI, J.-P. TILLICH, N. SENDRIER, P. S. L. M. BARRETO. *MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes*, 2012, IACR Cryptology ePrint Archive, Report 2012/409, http://eprint.iacr.org/2012/409.

[56] C. PELLE. *Chiffrement par blocs à bas coût*, Ecole Centrale de Lille, September 2012, Master's thesis, Co-direction: Anne Canteaut et María Naya-Plasencia.

[57] S. PIRONIO, L. MASANES, A. LEVERRIER, A. ACIN. *Device-independent quantum key distribution secure against adversaries with no long-term quantum memory*, 2012, arXiv:1211.1402, http://arxiv.org/abs/1211.1402.

[58] J. ROUÉ. *Super Boites-S*, Université de Versailles, sept 2012, Master's thesis, Co-direction: Anne Canteaut et Pascale Charpin.