Activity Report 2011

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

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]
Jean-Pierre Tillich [Junior Researcher (CR) Inria, HdR]
Ayoub Otmani [On leave from University of Caen, until August 2011]

External Collaborator

Matthieu Finiasz [Assistant Professor (MC) ENSTA, Paris]

PhD Students

Mamdouh Abbara [détachement du Corps des Mines]
Marion Bellard [Ministère de la défense, Univ. P. et M. Curie, since January 2011]
Céline Blondeau [INRIA grant, Univ. P. et M. Curie, until October 2011]
Christina Boura [CIFRE grant, Univ. P. et M. Curie]
Vincent Herbert [INRIA grant, Univ. P. et M. Curie]
Stéphane Jacob [AMX grant, Univ. P. et M. Curie]
Denise Maurice [AMN grant, Univ. P. et M. Curie]
Rafael Misoczki [INRIA grant, Univ. P. et M. Curie]
Grégory Landais [DGA grant, Univ. P. et M. Curie]
Jean-Christophe Sibel [INRIA grant, Univ. Cergy, since April 2011]
Valentin Suder [DGA grant, Univ. P. et M. Curie, since October 2011]

Post-Doctoral Fellow

Baudoin Collard [since February 2011]

Visiting Scientist

Gohar Kyureghyan [On leave from Otto-von-Guericke Universität Magdeburg, since October 2011]

Administrative Assistants

Christelle Guiziou [Secretary (TR) Inria]
Assia Saadi [Secretary Inria, until October 2011]

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

- **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, several candidates have been cryptanalyzed by some researchers of the project-team. More recently, we have provided a deep study of the algebraic properties of some of the finalists of the competition.
- **Discovery of a distinguishing property for the family of Goppa codes** which are used in the original McEliece cipher and the CFS signature scheme. Even if it does not lead to an attack, this property invalidates the previously known security proofs of these systems. Among the many families of linear codes which have been considered for code-based cryptography, Goppa codes seemed to be the only safe one. Now even Goppa codes seem to be questioned.
- **Organization of the WCC international conference**, which was held in Paris in April 2011. This was the seventh in the series of biannual workshops on *Coding and Cryptography*.

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.

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

5. New Results

5.1. Symmetric cryptosystems

Participants: Céline Blondeau, Christina Boura, Baudoin Collard, Anne Canteaut, Pascale Charpin, Stéphane Jacob, Gohar Kyureghyan.

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 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:

- study of the algebraic properties of the recent hash function proposals, including the SHA-3 candidates Keccak and Luffa. This work includes a theoretical study of the algebraic degree of iterated functions composed of parallel applications of a smaller function [24].
- 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 [31], [44].

5.1.2. Stream ciphers.

Our research work on stream ciphers is a long-term work which has been developed within the 4-year ANR RAPIDE project. It 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 [13].
- Cryptanalysis of the recent stream cipher proposal Armadillo [21].

5.1.3. 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.

Recent results:

- Differential cryptanalysis with multiple differentials, multiple differential cryptanalysis on the lightweight block cipher Present [23].
- Use of tools from error correcting theory in linear cryptanalysis [36].
- 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 [12].

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 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 [11].
- 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: [14].
- Study of the algebraic properties (e.g. the algebraic degree) of the inverses of APN power permutations [47].

5.2. Code-based cryptography

Participants: Matthieu Finiasz, Grégory Landais, 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.

Recent results:

- A distinguishing attack on high rate Goppa codes [25]. This results does not lead to an attack on any code based cryptosystem, but, in some particular cases, it invalidates the security reduction. It was conjectured that there was no such distinguishers.
- A new class of codes for McEliece type cryptosystems offering more versatility [22]
- A generic attack on one-time signature based on codes (KKS type) [27].
- A improvement of generic decoding techniques when addressing multiple targets [28].

5.3. Error-correcting codes and applications

Participants: Mamdouh Abbara, Matthieu Finiasz, Vincent Herbert, Denise Maurice, 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. Algebraic error-correcting codes.

Finding lower bounds on the minimum distance of cyclic codes is an old and difficult problem. Cyclic codes with three zeroes correct at most three errors, that is have minimum distance at most 7. It is an interesting question to determine which cyclic codes with three zeroes have minimum distance 7. Vincent Herbert revisit this problem by using an algorithm due to Shaub. Some classification questions are addressed about three error correcting cyclic codes and some new results involving intensive computer search have been obtained [10], [26].

5.3.2. 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:

- a construction of a family of quantum turbo-codes with excellent error reducing performance under iterative decoding and this even for very noisy channels [29];
- a proof that this family has unbounded minimum distance [20].

5.3.3. 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[2], it would be dangerous to rely, even partially, on the fact that the adversary does not know those specifications. However, this fundamental rule does not mean that the specifications are known to the attacker. In practice, before mounting a cryptanalysis, it is necessary to strip off the data. This reverse engineering process is often subtle, even when the data formatting is not concealed on purpose. A typical case is interception; some raw data, not necessarily encrypted, 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.

6. Contracts and Grants with Industry

6.1. Grants with Industry

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

7. Partnerships and Cooperations

7.1. National Initiatives

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

- **ANR RAPIDE** ($01/07 \rightarrow 03/11$)
  Design and analysis of stream ciphers dedicated to constraint environments
  http://rapide-anr2006.gforge.inria.fr/index.html
  Partners: LORIA (project-team CACAO/CARAMEL), 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. The results of the project are practical as well as theoretical and concern both design and analysis of such stream ciphers.

- **ANR DEMOTIS** ($02/09 \rightarrow 02/12$)
  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.

- **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** ($01/09 \rightarrow 01/12$)
  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.
- **French Ministry of Defense** $(01/11 \rightarrow 12/13)$
  Funding for the supervision of Marion Bellard's PhD.
  30 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. Major European Organizations with which you have followed Collaborations

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 Initiatives

7.3.1. Visits of International Scientists

- Gohar Kyureghyan, Otto-von-Guericke Universität Magdeburg, Germany, from October 2011 to June 2012
- Kaisa Nyberg, Aalto University, Finland, November 6-8.
- Christiane Peters, Danmarks Tekniske Universitet, Copenhagen, Denmark, November 13-18.
- Stefan Heyse, Ruhr-Universität Bochum, Germany, November 13-18.

7.3.2. Visits to International Partners

- EPFL, Lausanne, Switzerland, September 1-30, invitation to the *Combinatorial, Algebraic and Algorithmic Aspects of Coding Theory* Program of the Centre interfacultaire Bernoulli, (N. Sendrier)
- EPFL, Lausanne, Switzerland, September 7-15, invitation to the *Combinatorial, Algebraic and Algorithmic Aspects of Coding Theory* Program of the Centre interfacultaire Bernoulli, (P. Charpin)
- EPFL, Lausanne, Switzerland, September 5-29, invitation to the *Combinatorial, Algebraic and Algorithmic Aspects of Coding Theory* Program of the Centre interfacultaire Bernoulli, (JP. Tillich)

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.
- *RAIRO - Theoretical Informatics and Applications*, associate editor: N. Sendrier.
- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, 2011, co-editor: P. Charpin.
- *WCC 2011*, April 11-15, 2011, Paris, Program co-chair: A. Canteaut.
- *FSE 2012 (Fast Software Encryption)*: March, 19-21, 2012, Washington DC, USA, Program chair: A. Canteaut
- 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. Organization of international conferences

We are involved in the organization of the *Workshop on Coding Theory and Cryptography (WCC)* which will be held in Paris in April 2011. This is the seventh in the series of biannual workshops on *Coding and Cryptography*. Pascale Charpin and Nicolas Sendrier were the general chairs of the workshop. Anne Canteaut was a program co-chair.

8.1.3. Program committees

- 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, program co-chair);
- Code-based Cryptography Workshop: May 11-12, 2011, Eindhoven, The Netherlands (N. Sendrier);
- WCCS'11 (2nd Workshop on Codes, Cryptography and Communication Systems), June 16-17, 2011, Rabat, Morocco (A. Otmani);
- 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);
- PQCrypto 2011: November 29 - December 2, Taipei, Taiwan (N. Sendrier, JP Tillich);
- Indocrypt 2011: December 11-15, 2011, Chennai, India (N. Sendrier);
- IMA International Conference on Cryptography and Coding: December 12-15, 2011, University of Oxford, UK (P. Charpin);
- FSE 2012: March 19-21, 2012, Washington DC, USA (A. Canteaut, program chair);
- PKC 2012: May 21-23, 2012, Darmstadt, Germany (N. Sendrier);
- SAC 2012: August 16-17, 2012, Windsor, Ontario, Canada (A. Canteaut).

8.1.4. Invited talks

- JP. Tillich, *Quantum turbo codes with unbounded minimum distance and excellent error-reducing performance*, Workshop on /Quantum/ Information: Codes, /Geometry/ and Random Structures, Centre de recherches mathématiques Université de Montréal, October 24-26, 2011.
- N. Sendrier, *Decoding One Out of Many*, Algebraic Coding Theory workshop, CI Bernouilli, EPFL, Lausanne, September 2011.

- N. Sendrier, *The Tightness of Security Reductions in Code-based Cryptography*, IEEE Information Theory Workshop - ITW 2011, Paraty, Brazil, October 2011.
- N. Sendrier, *A Survey of Code-based Cryptography*, The São Paulo Advanced School of Cryptography, University of Campinas, Brazil, October 2011.
- A. Canteaut, *De l'espérance de vie d'un algorithme symétrique (ou l'AES dix ans après)*, Journées CRYPTIS, Université de Limoges, November 25-26, 2011.

8.1.5. Other responsibilities in the national community.

- 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)**: Université de Versailles-St Quentin (A. Canteaut), Université Paris Diderot (A. Canteaut), INRIA Saclay-Ile de France (concours CR, N. Sendrier), INRIA (concours DR, N. Sendrier);
- A. Canteaut has been co-chair of the postdoc committee for the Paris-Rocquencourt center;
- JP Tillich is in charge of "Formation par la recherche" for the Paris-Rocquencourt center since October 2011.

8.2. Ph.D. committees

- P. Delaunay, *Attaques physiques sur des algorithmes de chiffrement par flot*, Université de Versailles-St Quentin, January 28, 2011, committee: A. Canteaut.
- Christiane Peters, *Curves, Codes, and Cryptography*, Technische Universiteit Eindhoven, The Netherlands, May 10, 2011. committee: N. Sendrier.
- R. Bhattacharyya, *On the blackbox reduction of some cryptographic constructions*, Indian Statistical Institute, October 1, 2011, committee: A. Canteaut (reviewer).
- T. Fuhr, *Conception, preuves et analyse de fonctions de hachage cryptographiques*, Telecom ParisTech, October 3, 2011, committee: A. Canteaut.
- C. Blondeau, *La cryptanalyse différentielle et ses généralisations*, Université Pierre et Marie Curie, November 7, 2011, committee: P. Charpin (supervisor), A. Canteaut, JP. Tillich.
- V. Gauthier-Umana, *Post-quantum cryptography*, Danmarks Tekniske Universitet, Danemark, November 30, 2011, committee: A. Canteaut (reviewer).
- Vincent Herbert, *Des codes correcteurs pour sécuriser l'information numérique*, Université Pierre et Marie Curie, December 5, 2011. committee: N. Sendrier (supervisor).
- Y. Guo, *Confidentialité et intégrité de bases de données embarquées*, Université de Versailles-St Quentin, December 6, 2011, committee: A. Canteaut.
- A. Bocquet, *Modèles de sécurité réalistes pour la distribution quantique de clés*, Telecom ParisTech, December 6, 2011, committee: JP. Tillich.
- J.-R. Reinhard, *Etude de primitives cryptographiques symétriques : chiffrements par flot et fonctions de hachage*, Université de Versailles-St Quentin, December 14, 2011, committee: A. Canteaut (reviewer).

8.3. Teaching

A. Canteaut, *Stream ciphers*, 6 hours, M2, Telecom ParisTech, France;

A. Canteaut, *Principles of programming languages*,40 hours, L3, Ecole Polytechnique, France;

N. Sendrier, *Error-correcting codes and applications to cryptography*, 3 h, M2, Master Parisien de Recherche en Informatique (MPRI), Université Paris Diderot, France;

J.-P. Tillich, *Introduction to Information Theory*, 32 h, M2, Ecole Polytechnique, France.

J.-P. Tillich, *Programs and Algorithms : from sequential to distributed*, 32 h, M1, Ecole Polytechnique, France.

8.4. General Audience Actions

- A. Canteaut gave a talks at Lycée Jean Renoir, Bondy (Feb. 2011) and to the professors of mathematics from Académie de Versailles (Dec. 2011)
- Talk to *Les rencontres des Tuileries*, June 2011.
- The whole team was in charge of one of the Inria animation during *Fête de la science* at the "Quartier des sciences" in Paris (Nov. 2011).

8.4.1. PhD defended in 2011.

- Céline Blondeau, *La cryptanalyse différentielle et ses généralisations*, Université Pierre et Marie Curie, November 7, 2011, supervisor: P. Charpin.
- Vincent Herbert, Université Pierre et Marie Curie, December 5, 2011, supervisor: N. Sendrier.

8.4.2. PhD in progress.

- Mamdouh Abbara, *Quantum turbo-codes*, August 2009, supervisor: JP. Tillich.
- Marion Bellard, *Influence du mapping pour la reconnaissance d'un système de communication*, January 2011, supervisors: N. Sendrier and J.-P. Tillich
- Christina Boura, *Sécurité et cryptanalyse des fonctions de hachage*, since January 2010, supervisor: A. Canteaut
- Stéphane Jacob, *Protection cryptographique des bases de données : conception et cryptanalyse*, since December 2008, defense scheduled in March 2012, supervisor: A. Canteaut
- 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
- Denise Maurice, *Quantum LDPC codes*, September 2010, supervisor : JP. Tillich.
- Rafael Misoczki, *Aspects of code-based cryptography*, November 2010, supervisor: N. Sendrier
- Jean-Christophe Sibel, *Decoding LDPC codes with many short cycles*, October 2009, supervisor : D. Declercq.
- Valentin Suder, *Les Permutations en Cryptographie Symétrique*, since October 2011, supervisor: P. Charpin.

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] 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. BLONDEAU. *La cryptanalyse différentielle et ses généralisations*, Université Pierre et Marie Curie, Paris, November 2011.

[10] V. HERBERT. *Des Codes Correcteurs pour Sécuriser l'Information Numérique*, Université Pierre et Marie Curie, Paris, December 2011.

Articles in International Peer-Reviewed Journal

[11] C. BLONDEAU, A. CANTEAUT, P. CHARPIN. *Differential Properties of $x \mapsto x^{2^t-1}$*, in "IEEE Transactions on Information Theory", 2011, to appear, http://hal.inria.fr/hal-00610099/en.

[12] C. BLONDEAU, B. GÉRARD, J.-P. TILLICH. *Accurate estimates of the data complexity and success probability for various cryptanalyses*, in "Designs Codes and Cryptography / Designs Codes and Cryptography An International Journal", 2011, vol. 59, n^{o} 1-3, p. 3-34, 36 pages, http://dx.doi.org/10.1007/s10623-010-9452-2.

[13] A. CANTEAUT, M. NAYA-PLASENCIA. *Parity-check relations on combination generators*, in "IEEE Transactions on Information Theory", 2011, to appear.

[14] P. CHARPIN, S. SARKAR. *Polynomials with Linear Structure and Maiorana-McFarland Construction*, in "IEEE Transactions on Information Theory", 2011, vol. 57, n^{o} 6, p. 3796–3804.

Invited Conferences

[15] A. CANTEAUT. *De l'espérance de vie d'un algorithme symétrique (ou l'AES dix ans après)*, in "Journées CRYPTIS", Limoges, France, November 2011, http://www.cryptis.fr/programme-25ans.html.

[16] N. SENDRIER. *A Survey of Code-based Cryptography*, in "The São Paulo Advanced School of Cryptography", University of Campinas, Brazil, October 2011.

[17] N. SENDRIER. *Decoding One Out of Many*, in "Algebraic Coding Theory", CI Bernouilli, EPFL, Lausanne, September 2011.

[18] N. SENDRIER. *The Tightness of Security Reductions in Code-based Cryptography*, in "IEEE Information Theory Workshop - ITW 2011", Paraty, Brazil, October 2011, p. 415-419.

[19] J.-P. TILLICH. *Quantum turbo codes with unbounded minimum distance and excellent error-reducing performance*, in "Workshop on Quantum Information: Codes, Geometry and Random Structures", CRM, Université de Montréal, Québec, October 2011.

International Conferences with Proceedings

[20] M. ABBARA, J.-P. TILLICH. *Quantum turbo codes with unbounded minimum distance and excellent error-reducing performance*, in "IEEE Information Theory Workshop - ITW 2011", Paraty, Brazil, October 2011.

[21] M. A. ABDELRAHEEM, C. BLONDEAU, M. NAYA-PLASENCIA, M. VIDEAU, E. ZENNER. *Cryptanalysis of ARMADILLO2*, in "Advances in cryptology - ASIACRYPT 2011", Séoul, Korea, Republic Of, LNCS, Springer, 2011, vol. 7073, p. 308-326, http://hal.inria.fr/inria-00619236/en.

[22] P. S. BARRETO, R. LINDNER, R. MISOCZKI. *Monoidic Codes in Cryptography*, in "Post-Quantum Cryptography - PQCrypto 2011", LNCS, Springer, 2011, vol. 7071, p. 179-199.

[23] C. BLONDEAU, B. GÉRARD. *Multiple Differential Cryptanalysis: Theory and Practice*, in "Fast Software Encryption - FSE 2011", Lyngby, Denmark, LNCS, Springer, 2011, vol. 6733, p. 35-54, http://hal.inria.fr/hal-00610107/en.

[24] C. BOURA, A. CANTEAUT, C. DE CANNIÈRE. *Higher-order differential properties of Keccak and Luffa*, in "Fast Software Encryption - FSE 2011", Lyngby, Denmark, LNCS, Springer, 2011, vol. 6733, p. 252–269.

[25] J.-C. FAUGÈRE, V. GAUTHIER-UMANA, A. OTMANI, L. PERRET, J.-P. TILLICH. *A Distinguisher for High Rate McEliece Cryptosystems*, in "IEEE Information Theory Workshop - ITW 2011", Paraty, Brazil, October 2011.

[26] V. HERBERT, S. SARKAR. *On the Triple-Error-Correcting Cyclic Codes with Zero Set* $\{1, 2^i + 1, 2^j + 1\}$, in "Cryptography and Coding - IMACC 2011", Oxford, UK, LNCS, Springer, 2011, vol. 7089, p. 79-96, http://dx.doi.org/10.1007/978-3-642-25516-8_6.

[27] A. OTMANI, J.-P. TILLICH. *An Efficient Attack on All Concrete KKS Proposals*, in "Post-Quantum Cryptography - PQCrypto 2011", LNCS, Springer, 2011, vol. 7071, p. 98-116.

[28] N. SENDRIER. *Decoding One out of Many*, in "Post-Quantum Cryptography - PQCrypto 2011", LNCS, Springer, 2011, vol. 7071, p. 51-67.

Conferences without Proceedings

[29] M. ABBARA, J.-P. TILLICH. *Quantum serial turbo-like codes with minimum distance growing polynomially in the code length*, in "14th Workshop on Quantum Information Processing (QIP 2011)", The Capella, Santosa Singapore, January 2011, Poster.

[30] C. BLONDEAU, A. CANTEAUT, P. CHARPIN. *Differential properties of $x \mapsto x^{2^t-1}$*, in "Finite Fields and Applications - Fq10", Gent, Belgium, July 2011.

[31] C. BOURA, A. CANTEAUT. *On the algebraic degree of iterated permutations*, in "Finite Fields and Applications - Fq10", Gent, Belgium, July 2011.

Scientific Books (or Scientific Book chapters)

[32] A. CANTEAUT. *Articles: A5/1, Berlekamp-Massey algorithm, Combination generator, Correlation attack, Fast correlation attack, Filter generator, Inversion attack, Linear complexity, Linear consistency attack, Linear cryptanalysis for stream ciphers, Linear feedback shift register, Linear syndrome attack, Minimal polynomial, Running-key, Stream cipher*, in "Encyclopedia of cryptography and security - 2nd edition", H. VAN TILBORG, S. JAJODIA (editors), Springer, 2011, http://dx.doi.org/10.1007/978-1-4419-5906-5.

[33] P. CHARPIN. *Articles: Cyclic codes, Reed-Muller codes*, in "Encyclopedia of cryptography and security - 2nd edition", H. VAN TILBORG, S. JAJODIA (editors), Springer, 2011, http://dx.doi.org/10.1007/978-1-4419-5906-5.

[34] M. FINIASZ, N. SENDRIER. *Article: Digital Signature Scheme Based on McEliece*, in "Encyclopedia of Cryptography and Security – Second Edition", H. VAN TILBORG, S. JAJODIA (editors), Springer, 2011, http://dx.doi.org/10.1007/978-1-4419-5906-5.

[35] P. GABORIT, N. SENDRIER. *Article: Code-based Signature Schemes*, in "Encyclopedia of Cryptography and Security – Second Edition", H. VAN TILBORG, S. JAJODIA (editors), Springer, 2011, http://dx.doi.org/10.1007/978-1-4419-5906-5.

[36] B. GÉRARD, J.-P. TILLICH. *Using Tools from Error Correcting Theory in Linear Cryptanalysis*, in "Advanced Linear Cryptanalysis of Block and Stream Ciphers", P. JUNOD, A. CANTEAUT (editors), Cryptology and Information Security Series, IOS Press, October 2011, vol. 7, p. 87-114, http://dx.doi.org/10.1007/978-1-4419-5906-5.

[37] N. SENDRIER. *Articles: Code-based Cryptography; McEliece Public Key Cryptosystem; Niederreiter Encryption Scheme*, in "Encyclopedia of cryptography and security - 2nd edition", H. VAN TILBORG, S. JAJODIA (editors), Springer, 2011, http://dx.doi.org/10.1007/978-1-4419-5906-5.

Books or Proceedings Editing

[38] D. AUGOT, A. CANTEAUT (editors). *Workshop on Coding and Cryptography - WCC 2011*, INRIA, 2011, Proceedings of WCC 2011, April 11-15, Paris.

[39] P. CHARPIN, A. KHOLOSHA, E. ROSNES, M. G. PARKER (editors). *Special issue in Coding and Cryptography*, Designs, Codes and Cryptography, Springer-Verlag, 2011, vol. 59 (1–3), http://www.springerlink.com/content/0925-1022/59/1-3/.

[40] P. JUNOD, A. CANTEAUT (editors). *Advanced Linear Cryptanalysis of Block and Stream Ciphers*, Cryptology and Information Security Series, IOS Press, October 2011, vol. 7.

Research Reports

[41] M. ABBARA, J.-P. TILLICH. *The minimum distance of classical and quantum turbo-codes*, INRIA, 2011, http://arxiv.org/abs/1109.0215v1.

[42] P. S. BARRETO, R. LINDNER, R. MISOCZKI. *Monoidic Codes in Cryptography*, IACR, 2011, http://eprint.iacr.org/2011/371.

[43] C. BLONDEAU, A. CANTEAUT, P. CHARPIN. *Differential properties of functions $x \mapsto x^{2^t-1}$ – extended version*, INRIA, August 2011, http://hal.inria.fr/inria-00616674/en.

[44] C. BOURA, A. CANTEAUT. *On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$*, IACR, September 2011, http://eprint.iacr.org/2011/503.

[45] V. HERBERT, S. SARKAR. *On the Triple-Error-Correcting Cyclic Codes with Zero Set $\{1, 2^i + 1, 2^j + 1\}$*, INRIA, 2011, http://hal.inria.fr/hal-00627007/en.

Other Publications

[46] C. PENNARUM. *Fonctions booléennes et applications en cryptographie: un tour de piste*, Université de Bordeaux, June 2011, Direction: Pascale Charpin.

[47] V. SUDER. *Les permutations et leurs inverses en cryptographie symétrique*, Université de Limoges, September 2011, 37 pages. Direction: Pascale Charpin.