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 Scientist

Anne Canteaut [Team Leader, Research Director (DR) Inria, HdR]
Nicolas Sendrier [Research Director (DR) Inria, HdR]
Pascale Charpin [Research Director (DR) Inria, HdR]
Jean-Pierre Tillich [Research Associate (CR) Inria, HdR]
Ayoub Otmani [On leave from University of Caen since Sept. 2009]

External Collaborator

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

Technical Staff

Grégory Landais [R&D Engineer, since July 2009]

PhD Student

Mamdouh Abbara [détachement du Corps des Mines, since July 2009]
Bhaskar Biswas [INRIA grant, Ecole Polytechnique]
Céline Blondeau [INRIA grant, Univ. P. et M. Curie]
Christophe Chabot [DGA grant, Univ. Limoges, until Sept. 2009]
Maxime Côte [CIFRE grant, Ecole Polytechnique]
Cédric Faure [AMN grant, Ecole Polytechnique, until March 2009]
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]
Yann Laigle-Chapuy [Éducation Nationale, Univ. P. et M. Curie]
Stéphane Manuel [INRIA grant, Ecole Polytechnique]
Denise Maurice [Ecole Normale Supérieure, Paris, since Sept. 2009]
María Naya-Plasencia [INRIA grant, Univ. P. et M. Curie, until Nov. 2009]
Andrea Röck [INRIA grant, Ecole Polytechnique, until June 2009]
Alexander Zeh [Ulm University, Germany and Ecole Polytechnique, Palaiseau, France]

Post-Doctoral Fellow

Sumanta Sarkar [until Nov. 2009]

Administrative Assistant

Christelle Guiziou-Cloitre [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

- **Selection of *Shabal* to the second round of 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). The new hash algorithm, referred to as "SHA-3", will be developed through a public competition, much like the development of the AES. Among the 64 candidates which have been proposed in 2008, 14 have moved forward to the second round of the competition in July 2009. One of these 14 algorithms, named *Shabal*, has been designed by some researchers of the project-team.
- **Cryptanalysis of four SHA-3 candidates.** 51 hash function proposals have been selected for the first round of the SHA-3 competition. Among these 51 candidates, 3 have been cryptanalyzed by some researchers of the project-team, namely MCSSHA-3 and its variants proposed by M. Maslennikov from Korea, LANE proposed by Indesteege *et al.* from Leuven University (Belgium) and ESSENCE proposed by J.W. Martin from James Madison University (Virginia, USA). We have also mounted an attack against a candidate which has not been moved forward to the first round, Maraca proposed by R.J. Jenkins Jr. from Microsoft.
- **Code-based cryptography.** The project-team is strongly involved in code-based cryptography, a subject which attracts more and more attention with the raise of post-quantum cryptography. Two important works have been completed this year. One was presented at Asiacrypt 2009, and gives very tight security bounds for the security of code-based cryptosystems against message attack [37]. The other is a yet unpublished [70], key-recovery algebraic attack on some variants of McEliece cryptosystem. This is a key-work which opens the door to a new class of cryptanalysis.

3. Application Domains

3.1. Application domains

Our research work is mainly devoted to the design and analysis of cryptographic algorithms. However, 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. Our main application domains are therefore:

- cryptology,
- error-correcting codes
- 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 and quantum error correcting codes for fault tolerant quantum computing and quantum communications.

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

4. Software

4.1. Hash functions

The hash functions which have been submitted to the SHA-3 competition, *Shabal* and FSB, have been implemented in software and the corresponding implementations are available on http://csrc.nist.gov/groups/ST/hash/sha-3/.

5. New Results

5.1. Symmetric cryptosystems

Participants: Céline Blondeau, Anne Canteaut, Pascale Charpin, Benoît Gérard, Stéphane Jacob, Yann Laigle-Chapuy, Stéphane Manuel, María Naya-Plasencia, Andrea Röck, 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 EDHASH and Saphir-2 ANR Projects and with S. Manuel's and M. Naya-Plasencia's 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 *Shabal*: presentation of *Shabal* to the NIST candidate conference [50]; new proof of the mode of operation which takes into account the existence of related-key distinguishers on the round permutation [65], [23]; evaluation of the security of weakened versions of *Shabal* [12]. It is worth noticing that *Shabal* belongs to the 14 candidates (among 64) which have been moved forward to the second round of the SHA-3 competition;
- Cryptanalysis of the successive versions of the SHA-3 candidate MCSSHA-3 : [30];
- Semi-free start collisions on LANE, which is the SHA-3 candidate designed by the COSIC group from Leuven University. This attack is based on the recent rebound technique: [40];
- 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: [69], [48];
- 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: [51], [24];
- Security evaluation of the SHA-3 candidate CubeHash: [29];
- Classification of the disturbance vectors for collision attacks on SHA-1: [39], [56].

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. Some researchers from the project-team are actually co-authors of three stream cipher proposals which have been submitted to the eSTREAM project: SOSEMANUK, DECIM and F-FCSR. SOSEMANUK belongs to the 7 recommended ciphers which have been included in the current portfolio of eSTREAM[2] (among 34 submissions). Our work within the eSTREAM project also includes an important cryptanalytic effort on stream ciphers.

Recent results:

- Design and study of new cryptanalytic methods against general combination generators whose constituent devices generate periodic sequences (e.g., NLFSRS): [12]
- Evaluation of the bias of parity-check relations in the context of cryptanalysis of combination generators with constituent devices which generate period sequences: [33];
- Analysis of the security of the eSTREAM proposal DRAGON: [13];
- Study of the security and of the implementation properties of stream ciphers based of FCSRs (Feedback with Carry Shift registers): [13], [25];
- Design of a new attack against the combination generator with LFSRs. This attack applies when the combining function has good auto-correlation properties: [11], [66].

5.1.3. Random number generators.

Random number generators are non-deterministic algorithms which produce random-looking sequences from parameters that we cannot control. Thus, they differ from pseudo-random generators used in stream ciphers where the same sequence must be generated twice (once for enciphering, and once for deciphering). Random number generators are typically used to generate secret keys. However, many cryptographic schemes can be attacked if the underlying random generator does not meet some requirements, for instance if its output does not contain enough uncertainty/entropy.

[2] http://www.ecrypt.eu.org/stream/

Recent results:

- Analysis of the statistical properties of the HAVEGE random number generator [72]; HAVEGE is a high-speed random number generator which uses the uncertainties of the processor state coming from the use of optimization techniques, such as data or instruction caches or branch predictors: [13];
- Security analysis of the random number generator included in the Linux kernel, `/dev/random` and `/dev/urandom`: [57].

5.1.4. 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: [32], [49].
- Linear cryptanalysis with multiple approximations: following the work by C. Tavernier on list decoding of first-order Reed-Muller codes, B. Gérard and J.-P. Tillich have explored how to improve on Matsui's linear cryptanalysis by using all the approximations obtained by this list decoding algorithm. It turns out that recovering the key from these approximations is equivalent to decoding a linear code on the Gaussian channel. This relationship has been used in order to evaluate accurately the data complexity of this new attack and also to suggest an algorithm based on decoding techniques for recovering the secret key in a much more efficient way than what was known before: [38].

5.1.5. 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: [16];
- Construction and study of the properties of new families of permutation polynomials over the field with 2^m elements: [20], [52], [11];

- Determination of the second-order nonlinearity (*i.e.*, of the distance to the set of all quadratic functions) of some cubic bent functions: [53];
- Investigation of the cryptographic properties of negabent Boolean functions: [42].

5.1.6. 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; Cryptanalysis of a fast encryption scheme proposed by Ge and Zdonic [71] (this study is a joint work with the SMIS project-team): [54].

5.2. Code-based cryptography

Participants: Bhaskar Biswas, Cédric Faure, Matthieu Finiasz, Vincent Herbert, 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

- 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,
- trying new hard problems, like decoding Reed-Solomon codes above the list-decoding radius,
- address new functionalities, like hashing or symmetric encryption.

Recent results:

- PhD thesis of Cédric Faure: in this work, C. Faure studies various aspects of the use of rank metric codes in cryptography as well as the structural weakness of algebraic codes from curves of low genus when used in code-based cryptosystems [10].
- B. Biswas and V. Herbert have studied the root finding phase of the Goppa code decoding procedure. This work allows a speedup of the decryption in the McEliece and the Niederreiter public-key encryption schemes. This work was published in the proceedings of WEWoRC 2009 [31].
- M. Finiasz and N. Sendrier have proposed new tight lower bounds for the two best decoding techniques used in code-based cryptanalysis (Information Set Decoding and Generalized Birthday Algorithm). This work has been presented at Asiacrypt 2009 [37].
- Following [21], A. Otmani and J.-P. Tillich are working on key recovery techniques for McEliece like cryptosystems using structured codes. New interesting results have been obtained on existing cryptosystem.

5.3. Decoding techniques and applications

Participants: Mamdouh Abbara, Christophe Chabot, Maxime Côte, Matthieu Finiasz, Grégory Landais, Denise Maurice, Jean-Pierre Tillich, Alexander Zeh.

Many cryptanalyses of cryptosystems rely on approximations of these systems by simple, easier functions. For instance, one tries to approximate the system by low degree polynomials, be they in one variable over a huge finite field, or in several variables over the Boolean field. Once such an approximation has been found, the problem of finding the key or of inverting the system, which is normally intractable with a direct approach, is written into a system of simple equations, where each equation holds with some probability. The probability is as good as the approximation is close. 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 an LDPC[3] code, with iterative algorithms. Furthermore, the problem of finding such good approximations of ciphers leads also to a decoding problem. Here, finding good approximations by linear functions 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.

[3] Low-density parity-check code

Recent results:

- Iterative decoding algorithms in the quantum setting: we have shown that iterative decoding algorithms can be generalized to the quantum setting and have come up with some quantum serial turbo-codes with rather good performances under iterative decoding [22].
- Quantum LDPC codes and quantum tornado codes: the previously mentioned work points out that, in order to have an iterative decoding which converges, we have to pay a price in terms of the minimum distance which is not allowed to grow with the blocklength. Interestingly enough, the quantum LDPC codes that have been proposed in the literature suffer from the same problem. Fortunately, in the case of LDPC codes, we have found out that contrarily to the turbo-code case (where we prove that the minimum distance is necessarily bounded in order to ensure convergence of iterative decoding), this is merely a consequence of the way the quantum LDPC codes have been constructed so far: in [44], we namely suggest a construction of quantum LDPC codes based on Cartesian products of Tanner graphs that has a minimum distance that grows like the square root of the blocklength. This opens the way for obtaining quantum LDPC codes with good iterative decoding performance. Right now, we are unable to analyze rigorously iterative decoding for this family. This is due to the presence of small cycles in the construction. This issue has been addressed and partly solved in [43]. In this article, inspired by classical Tornado codes, we suggest a modification of quantum LDPC codes schemes for which iterative decoding can be analyzed rigorously. This can be used to show that the construction proposed in [43] can attain the capacity of the quantum erasure channel under iterative decoding.

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[4], 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 two industrial contracts driven by the DGA.

Recent results:

- M. Côte and N. Sendrier have presented at ISIT 2009 a new algorithm for recovering convolutional codes from noisy data [35].

5.3.3. New decoding algorithm for error-correction.

We also investigate more traditional aspects of coding theory by improving some decoding algorithms for error-correction and by searching for codes with good decoding performance.

Recent results:

- Generalization of Roth and Ruckenstein's method: in 2000, a paper by Roth and Ruckenstein describes a very efficient method for implementing the Sudan decoding algorithm. He first derived an algorithm based on the FIA (Fundamental Iterative Algorithm) presented at the ITW 2009 workshop [45], and also remarked that this can done with Feng-Tzeng algorithm [46].
- Alexander Zeh and Daniel Augot have noticed a relation between the parameters of a Guruswami-Sudan algorithm with multiplicity s and $\binom{s+1}{2}$ times a simple Sudan algorithm (with multiplicity 1). The corresponding codes and codewords have to be found, so this is work in progress.

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

6. Contracts and Grants with Industry

6.1. Industrial contracts

- **I2E/AMESYS** (01/07 → 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.

- **Société IPSIS** (11/06 → 10/09)
  Recognition of a coding scheme
  60 kEuros.

  This other contract on codes reconstruction provides the funding for Maxime Côte's PhD scholarship. It is funded by the DGA ACETE call for offers.

7. Other Grants and Activities

7.1. Other external funding

7.1.1. National initiatives

- **ANR RAPIDE** (01/07 → 12/10)
  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 EDHASH** (01/07 → 12/09)
  Evaluation and Design of secure HASH functions
  http://www-rocq.inria.fr/secret/EDHASH/
  Partners: INRIA (project-team SECRET) and UVSQ/PRISM (Crypto team).
  123 kEuros.

  This project had two purposes: understanding the recent attacks on cryptographic hash functions and suggesting new constructions based on coding theory. The results obtained with this project include new developments on the cryptanalysis of SHA-0 and SHA-1, and new constructions of hash functions, in particular the FSB proposal which has been submitted to the SHA-3 competition.

- **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. Visibility

7.2.1. Publishing activities.

- *Cahiers droit, sciences et technologies*, editorial board: A. Canteaut.
- *IEEE Transactions on Information Theory*, associate editor: J.-P. Tillich for *Coding Theory*.
- *Designs, Codes and Cryptography*, associate editor: P. Charpin, since 2003.
- *Indocrypt 2009*, December 13-17, 2009, New Delhi, India, Program co-chair: N. Sendrier.
- *PQCrypto 2010*, May 25-28, 2010, Darmstadt, Germany, Program chair: N. Sendrier.

7.2.2. Program committees

- WCC 2009 (Workshop on coding and cryptography): May 10-15, 2009, Loftus, Norway (A. Canteaut, P. Charpin and N. Sendrier);
- AfricaCrypt 2009: June 21-25, 2009, Gammarth, Tunisia (A. Canteaut);

- WEWoRC 2009: July 7-9, 2009, Graz, Austria (N. Sendrier);
- SECRYPT 2009 (International Conference on Security and Cryptography), July 7-10, 2009, Milan, Italy (P. Charpin);
- Indocrypt 2009: December 13-17, 2009, New Delhi, India (J.-P. Tillich);
- 12th IMA conference on Cryptography and Coding : December 14-17, 2009, Cirencester, UK (P. Charpin);
- 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);
- SCC 2019: June 23-25, 2010, London, United Kingdom (A. Otmani);
- 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).

7.2.3. 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;
- **"Commission d'experts"(Committees for the selection of professors and assistant professors)**: University of Caen (A. Canteaut), University of Limoges (N. Sendrier), University of Bordeaux (J.P. Tillich), ENSEA (J.P. Tillich);
- A. Canteaut has been co-chair of the postdoc committee for the Paris-Rocquencourt center.

8. Dissemination

8.1. 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.

8.2. Ph.D. committees

- C. Chabot, *Reconnaissance de codes, structure des codes quasi-cycliques*, Université de Limoges, September 24, 2009, committee: P. Charpin, N. Sendrier (supervisor).
- C. Faure, *Etude de systèmes cryptographiques construits a l'aide de codes correcteurs, en métrique de Hamming et en métrique rang*, Ecole Polytechnique, March 17, 2009, committee: N. Sendrier (supervisor).
- Y. Laigle-Chapuy, *Polynômes de permutation et applications en cryptographie. Cryptanalyse des registres filtrés*, Université Pierre et Marie Curie, June 19, 2009, committee: A. Canteaut (president), P. Charpin (supervisor).
- A. Leverrier, *Theoretical study of continuous-variable quantum key distribution*, Ecole Nationale Supérieure des Télécommunications, November 20, 2009, committee: J.-P. Tillich (reviewer).

- M. Naya-Plasencia, *Chiffrements à flot et fonctions de hachage: conception et cryptanalyse*, Université Pierre et Marie Curie, November 16, 2009, committee: A. Canteaut (supervisor), P. Charpin.
- Diana Radkova, *Constacyclic codes as invariant subspaces*, Delft University of Technology, the Netherlands, January 2009, committee: P. Charpin.
- A. Röck, *Quantifying studies of (pseudo)random number generation for cryptography*, Ecole Polytechnique, May 18, 2009, committee: N. Sendrier (supervisor).
- Y. Seurin, *Primitives et protocoles cryptographiques à sécurité prouvéee*, July 1, 2009, committee: A. Canteaut (president).

8.3. Participation to workshops/conferences in 2009

- Quantum Information Processing - QIP 2009, Santa Fe, USA, January 11-16, participant: Jean-Pierre Tillich.
- Dagstuhl Seminar on Symmetric Cryptography, January 12-16, participants: María Naya-Plasencia, Andrea Röck.
- FSE 2009, Leuven, Belgium, February 22-28, participants: Anne Canteaut, Stéphane Jacob, Stéphane Manuel, María Naya-Plasencia, Andrea Röck, Pascale Charpin, Benoit Gérard, Céline Blondeau.
- First SHA-3 candidate conference , Leuven, Belgium, February 22-28, participants: Anne Canteaut, Stéphane Jacob, Stéphane Manuel, María Naya-Plasencia, Andrea Röck, Nicolas Sendrier.
- Seventh Bellairs' Crypto-Workshop on Quantum Crypto, March 9-13, Bridgetown, Barbados, participant: Nicolas Sendrier.
- EUROCRYPT 2009, Cologne, Germany, April 26-30, participants: Céline Blondeau, Benoit Gérard.
- ECRYPT II Hash research retreat, May 05-07, Graz, Austria, participant: María Naya-Plasencia.
- WCC 2009, Bergen, Norway, May 10-15, participants: Céline Blondeau, Anne Canteaut, Pascale Charpin, Benoit Gérard, Stéphane Manuel, Nicolas Sendrier.
- ISIT 2009, Seoul, Korea, June 28-July 3, participants: Maxime Côte, María Naya-Plasencia, Nicolas Sendrier, Jean-Pierre Tillich.
- WEWORC 2009, Graz, Austria, July 6-9, participants: Vincent Herbert, María Naya-Plasencia.
- Finite Fields and Applications - Fq9, Dublin, Ireland, July 12-17, participants: Anne Canteaut, Pascale Charpin, Sumanta Sarkar.
- Academy contact forum Coding Theory and Cryptography III, Bruxelles, Belgium, September 25, 2009, participants: Ayoub Otmani, Bimal Roy, Sumanta Sarkar, Nicolas Sendrier.
- Journées "Codage et Cryptographie" - C2, Fréjus, October 04-08, 2009, participants: Mamdouh Abbara, Céline Blondeau, Christina Boura, Anne Canteaut, Benoit Gérard, Vincent Herbert, Stéphane Jacob, Grégory Landais, Stéphane Manuel, Denise Maurice, María Naya-Plasencia, Nicolas Sendrier, Jean-Pierre Tillich.
- Workshop QuantumComm'09, Naples, Italy, October 25-27, participant: Nicolas Sendrier.
- ASIACRYPT 2009, Tokyo, Japan, December 6-10, participant: Ayoub Otmani, Nicolas Sendrier.
- INDOCRYPT 2009, New Delhi, India, December 13-16, participants: Anne Canteaut, Sumanta Sarkar, Nicolas Sendrier, Jean-Pierre Tillich.
- 12th Cryptography and Coding Conference, Cirencester, UK, December 14-17, participant: Benoit Gérard.

8.4. Visiting researchers

- Petr Lisonek, Simon Fraser University, Burnaby, Canada, April 1-30;

- Grigory Kabatianskiy, Institute of Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia, March 23 - April 4;
- Santanu Sarkar, Indian Statistical Institute, Kolkata, India, May 17-30;
- Jennifer Key, University of the Western Cape, South Africa, May 25 - June 2;
- Gohar Kyureghan, Otto-von-Guencke-University, Magdeburg, Germany, June 15-20;
- Xavier Dahan, Kyushu university Faculty of Mathematics, Fukuoka, Japan, June 16-27;
- Bimal Roy, Indian Statistical Institute, Kolkata, September 16-30;
- Mathieu Legeay, Rennes University, France, November 23-27.

8.5. Visit to other laboratories

- Bordeaux University, France, Jean-Pierre Tillich, March 31-April 2.
- Indian Statistical Institue, Kolkata, India, Anne Canteaut, December 17-23.

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", vol. 51, n^{o} 8, 2005, p. 2791–2811.

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

[4] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *Divisibility properties of classical binary Kloosterman sums*, in "Discrete Mathematics", vol. 309, n^{o} 12, June 2009, 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, n^{o} 2248, Springer-Verlag, 2001, p. 157–174.

[6] F. DIDIER, J.-P. TILLICH. *Computing the algebraic immunity efficiently*, in "Fast Software Encryption - FSE 2006", LNCS, vol. 4047, Springer, 2006, 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, n^{o} 4965, Springer, 2008, p. 254–269.

Year Publications

Doctoral Dissertations and Habilitation Theses

[9] C. CHABOT. *Reconnaissance de codes, structure des codes quasi-cycliques*, Université de Limoges, September 2009, Thèse de doctorat.

[10] C. FAURE. *Etude de systèmes cryptographiques construits à l'aide de codes correcteurs, en métrique de Hamming et en métrique rang*, École Polytechnique, Palaiseau, March 2009, http://pastel.paristech.org/5288/, Thèse de doctorat.

[11] Y. LAIGLE-CHAPUY. *Polynômes de permutation et applications en cryptographie. Cryptanalyse des registres filtrés*, Université Paris 6, Juin 2009, http://tel.archives-ouvertes.fr/tel-00438765/fr/, Thèse de doctorat.

[12] M. NAYA-PLASENCIA. *Chiffrements à flot et fonctions de hachage: conception et cryptanalyse*, Université Paris 6, Novembre 2009, Thèse de doctorat.

[13] A. RÖCK. *Quantifying studies of (pseudo)random number generation for cryptography*, École Polytechnique, Palaiseau, May 2009, http://tel.archives-ouvertes.fr/tel-00428553/en/, Thèse de doctorat.

[14] J.-P. TILLICH. *Contributions aux codes correcteurs d'erreurs, à la cryptologie et à la théorie des graphes*, Université Paris 6, May 2009, Habilitation à Diriger des Recherches.

Articles in International Peer-Reviewed Journal

[15] D. AUGOT, M. BARDET, J.-C. FAUGÈRE. *On the decoding of cyclic codes with the Newton's identities*, in "Journal of Symbolic Computation, Special Issue on Gröbner Bases Techniques in Cryptography and Coding Theory", vol. 44, n^{o} 12, December 2009, p. 1608-1625, http://www-rocq.inria.fr/~augot/gbdecode.pdf.

[16] C. BLONDEAU, A. CANTEAUT, P. CHARPIN. *Differential Properties of Power Functions*, in "International Journal of Information and Coding Theory", 2009, to appear, invited paper.

[17] C. BLONDEAU, B. GÉRARD, J.-P. TILLICH. *Accurate Estimates of the Data Complexity and Success Probability for Various Cryptanalyses*, in "Designs, Codes and Cryptography", 2009, to appear.

[18] P.-L. CAYREL, C. CHABOT, A. NECER. *Quasi-cyclic codes over ring of matrices*, in "Finite Fields and Their Applications", 2009, to appear.

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

[20] P. CHARPIN, G. KYUREGHYAN. *When does $G(x) + \gamma Tr(H(x))$ permute $GF(p^n)$?*, in "Finite Fields and Their Applications", vol. 15, n^{o} 5, October 2009, p. 615-632, http://www-rocq.inria.fr/secret/Pascale.Charpin/ffa-ChaKyu-09.pdfDE.

[21] A. OTMANI, J.-P. TILLICH, L. DALLOT. *Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes*, in "Mathematics in Computer Science", 2009, http://arxiv.org/abs/0804.0409, to appear.

[22] D. POULIN, J.-P. TILLICH, H. OLLIVIER. *Quantum serial turbo-codes*, in "IEEE Transactions on Information Theory", vol. 55, n^{o} 6, June 2009, p. 2776–2798, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4957637&isnumber=4957623US.

Invited Conferences

[23] A. CANTEAUT. *Shabal, a submission to NIST for their cryptographic hash algorithm competition*, in "Fundamentals of Communications and Networking - INRIA - Bell Labs Workshop II, Rocquencourt, France", October 2009.

[24] A. CANTEAUT, M. NAYA-PLASENCIA. *Internal collision attack on Maraca*, in "Dagstuhl Seminar Proceedings 09031 - Symmetric Cryptography, Schloss Dagstuhl, Germany", January 2009, http://drops.dagstuhl.de/opus/volltexte/2009/1953/pdf/09031.NayaPlasenciaMaria.Paper.1953.pdf.

[25] C. LAURADOUX, A. RÖCK. *Parallel Generation of ℓ-Sequences*, in "Dagstuhl Seminar Proceedings 09031 - Symmetric Cryptography, Schloss Dagstuhl, Germany", January 2009, http://drops.dagstuhl.de/opus/volltexte/2009/1956/pdf/09031.RoeckAndrea.ExtAbstract.1956.pdf.

[26] N. SENDRIER. *A Fly over Code-Based Cryptography*, in "International Conference on Quantum Communication and Quantum Networking - QuantumComm 2009, Vico Equense, Italy", October 2009.

[27] N. SENDRIER. *Code-based cryptology*, in "Academy Contact Forum "Coding theory and cryptography III", Brussels, Belgium", September 2009.

International Peer-Reviewed Conference/Proceedings

[28] I. ANDRIYANOVA, V. RATHI, J.-P. TILLICH. *Binary Weight Distribution of Non-Binary LDPC Codes*, in "IEEE International Symposium on Information Theory - ISIT 2009, Seoul, Korea", IEEE Press, June 2009, p. 65-69, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5205662&isnumber=5205248SE.

[29] J.-P. AUMASSON, E. BRIER, W. MEIER, M. NAYA-PLASENCIA, T. PEYRIN. *Inside the hypercube*, in "Information Security and Privacy - ACISP 2009, Brisbane, Australia", LNCS, vol. 5594, Springer, 2009, p. 202-213, http://www.springerlink.com/content/g7284t3750527264/?p=95f8fb321122422bab4180ba7e979ff6&pi=3CH.

[30] 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, July 2009, to appear CH .

[31] 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, July 2009, to appear.

[32] C. BLONDEAU, B. GÉRARD. *On the data complexity of statistical attacks against block ciphers*, in "Workshop on Coding and Cryptography - WCC 09, Lofthus, Norway", May 2009, p. 469-488.

[33] A. CANTEAUT, M. NAYA-PLASENCIA. *Computing the bias of parity-check relations*, in "IEEE International Symposium on Information Theory - ISIT 2009, Seoul, Korea", IEEE Press, June 2009, p. 290-294, http://arxiv.org/abs/0904.4412.

[34] C. CHABOT. *Reconstruction of families of codes, application to cyclic code*, in "Workshop on Coding and Cryptography - WCC 09, Lofthus, Norway", May 2009, p. 311-325.

[35] M. CÔTE, N. SENDRIER. *Reconstruction of Convolutional Codes from Noisy Observation*, in "IEEE International Symposium on Information Theory - ISIT 2009, Seoul, Korea", IEEE Press, June 2009, p. 546-550, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5205729&isnumber=5205248.

[36] X. DAHAN, J.-P. TILLICH. *Ramanujan graphs of larger girth*, in "Joint Conference of ASCM2009 and MACIS2009, Fukuoka, Japan", December 2009 JP .

[37] M. FINIASZ, N. SENDRIER. *Security Bounds for the Design of Code-based Cryptosystems*, in "Advances in Cryptology - ASIACRYPT 2009, Tokyo, Japan", LNCS, vol. 5912, Springer, December 2009, p. 88-105, http://www.springerlink.com/content/p3708n2h21786861/?p=daee5ed05d974a88a22eba7ad5b40fd8&pi=0.

[38] B. GÉRARD, J.-P. TILLICH. *On Linear Cryptanalysis with Many Linear Approximations*, in "Twelfth IMA International Conference on Cryptography and Coding 2009, Cirencester, UK", LNCS, vol. 5921, Springer, December 2009, p. 112-132, http://www.springerlink.com/content/m6037r2881525451/?p=aa11c629e3454026a6ac04d2241c052b&pi=7.

[39] S. MANUEL. *Classification and generation of disturbance vectors for collision attacks against SHA-1*, in "Workshop on Coding and Cryptography - WCC 09, Lofthus, Norway", May 2009, p. 224-233.

[40] K. MATUSIEWICZ, M. NAYA-PLASENCIA, I. NIKOLIC, Y. SASAKI, M. SCHLAFFER. *Rebound Attack on the full LANE Compression Function*, in "Advances in Cryptology - ASIACRYPT 2009, Tokyo, Japan", LNCS, vol. 5912, Springer, 2009, p. 106-125, http://www.springerlink.com/content/q1867gk784v2mp8q/?p=95f8fb321122422bab4180ba7e979ff6&pi=2DKLUJPAT.

[41] C. PETIT, J.-J. QUISQUATER, J.-P. TILLICH, G. ZÉMOR. *Hard and Easy Components of Collision Search in the Zémor-Tillich Hash Function: New Attacks and Reduced Variants with Equivalent Security*, in "Topics in cryptology - CT-RSA 2009, San Francisco, USA", LNCS, vol. 5473, Springer, April 2009, p. 182-194, http://hal.archives-ouvertes.fr/hal-00386479/en/BE.

[42] S. SARKAR. *On the Symmetric Negabent Boolean Functions*, in "Progress in Cryptology - INDOCRYPT 2009, New Delhi, India", LNCS, vol. 5922, Springer, December 2009, p. 136-143, http://www.springerlink.com/content/740l671114u12nm3/?p=adbba8d0f0ff438b94f9c3649ad40e29&pi=8.

[43] J.-P. TILLICH. *Quantum tornado codes*, in "Workshop on Quantum Information Processing - QIP 2009, Santa Fe, USA", January 2009, p. 12-13.

[44] J.-P. TILLICH, G. ZÉMOR. *Quantum LDPC Codes with Positive Rate and Minimum Distance Proportional to $n^{1/2}$*, in "IEEE International Symposium on Information Theory - ISIT 2009, Seoul, Korea", IEEE Press, June 2009, p. 799-803, http://arxiv.org/abs/0903.0566.

[45] A. ZEH, C. GENTNER, M. BOSSERT. *Efficient List-Decoding of Reed-Solomon codes with the Fundamental Iterative Algorithm*, in "IEEE Information Theory Workshop - ITW 2009, Taormina, Italy", October 2009, 77 DE .

[46] A. ZEH. *A Feng-Tzeng Approach for the Guruswami-Sudan Algorithm*, in "IEEE Information Theory Winter School, Loen, Norway", April 2009, 77, http://www.iet.ntnu.no/~demiguel/WinterSchool/Papers/Zeh.pdf DE .

Workshops without Proceedings

[47] C. AGUILAR, P. GABORIT, F. LAGUILLAUMIE, A. OTMANI. *Amélioration de la probabilité de tricher de $2/3$ à $1/2$ pour le schéma d'authentification de Stern*, in "Journées "Codage et Cryptographie" - C2 2009, Fréjus, Var", October 2009, http://www-salsa.lip6.fr/~bettale/C2/.

[48] J.-P. AUMASSON, Y. LAIGLE-CHAPUY, G. LEURENT, W. MEIER, M. NAYA-PLASENCIA, T. PEYRIN, A. RÖCK. *Cryptanalyse de la fonction de hachage ESSENCE*, in "Journées "Codage et Cryptographie" 2009, Fréjus, Var", October 2009, http://www-salsa.lip6.fr/~bettale/C2/ CH .

[49] C. BLONDEAU, B. GÉRARD, J.-P. TILLICH. *Complexité en données et probabilité de succès des cryptanalyses statistiques.*, in "Journées "Codage et Cryptographie" 2009, Fréjus, Var", October 2009, http://www-salsa.lip6.fr/~bettale/C2/.

[50] E. BRESSON, A. CANTEAUT, B. CHEVALLIER-MAMES, C. CLAVIER, T. FUHR, A. GOUGET, T. ICART, J.-F. MISARSKY, M. NAYA-PLASENCIA, P. PAILLIER, T. PORNIN, J.-R. REINHARD, C. THUILLET, M. VIDEAU. *Shabal*, in "The first SHA-3 candidate conference, Leuven, Belgium", February 2009, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/documents/shabal.pdf.

[51] A. CANTEAUT, M. NAYA-PLASENCIA. *Structural weaknesses of differentially uniform mappings*, in "Finite Fields and Applications - Fq9, Dublin, Ireland", July 2009.

[52] P. CHARPIN, G. KYUREGHYAN. *On a class of permutation polynomials*, in "Finite Fields and Applications - Fq9, Dublin, Ireland", July 2009 DE .

[53] S. GANGOPADHYAY, S. SARKAR. *On the second order nonlinearity of a cubic Maiorana-McFarland bent function*, in "Finite Fields and Applications - Fq9, Dublin, Ireland", July 2009 IN .

[54] Y. GUO, S. JACOB. *Confidentialité et intgrité des grandes bases de données*, in "Journées "Codage et Cryptographie" 2009, Fréjus, France", October 2009, http://www-salsa.lip6.fr/~bettale/C2/.

[55] V. HERBERT. *Recherche efficace de racines de polynômes dans les corps de caractéristique 2*, in "Journées "Codage et Cryptographie" 2009, Fréjus, France", October 2009, http://www-salsa.lip6.fr/~bettale/C2/.

[56] S. MANUEL. *Attaques par Collision contre SHA-1*, in "Journées "Codage et Cryptographie" 2009, Fréjus, Var", October 2009, http://www-salsa.lip6.fr/~bettale/C2/.

[57] A. RÖCK, V. STRUBELY, M. VIDEAU. *Étude du générateur d'aléa du noyau Linux.*, in "Journées "Codage et Cryptographie" 2009, Fréjus, Var", October 2009, http://www-salsa.lip6.fr/~bettale/C2/.

Scientific Books (or Scientific Book chapters)

[58] D. AUGOT, J.-C. FAUGÈRE, L. PERRET (editors). *Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics*, vol. 44, n^{o} 12, Elsevier, 2009, http://www.sciencedirect.com/science/article/B6WM7-4V3541X-1/2/ed04f9b0eb7a5eca5f3f9db3dde16873, Special issue of Journal of Symbolic Computation.

[59] D. AUGOT, E. BETTI, E. ORSINI. *An introduction to linear and cyclic codes*, in "Gröbner Bases, Coding, and Cryptography", RISC Book Series, Springer, Heidelberg, 2009, p. 47-68.

[60] D. AUGOT, M. STEPANOV. *A note on the generalisation of the Guruswami-Sudan list decoding algorithm to Reed-Muller codes*, in "Gröbner Bases, Coding, and Cryptography", RISC Book Series, Springer, Heidelberg, 2009, p. 47-68.

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

Books or Proceedings Editing

[62] B. ROY, N. SENDRIER (editors). *Progress in Cryptology - INDOCRYPT 2009*, LNCS, vol. 5922, Springer, New Delhi, India, December 2009, http://www.springerlink.com/content/l770g2h44j82/?p=09648f6d7d534476b9befc273cafb092&pi=4.

Scientific Popularization

[63] A. CANTEAUT. *La cryptographie symétrique*, in "Journés Nationales de l'Association des Professeurs de Mathématiques de l'enseignement public, Rouen, France", October 2009, http://ctug48.univ-fcomte.fr/APMEP2009/conferences/Conferences.php.

[64] A. CANTEAUT. *La Revanche de la Cryptographie Symétrique*, in "Exposé en classes préparatoires au lycé Faidherbe, Lille", February 2009.

Other Publications

[65] E. BRESSON, A. CANTEAUT, B. CHEVALLIER-MAMES, C. CLAVIER, T. FUHR, A. GOUGET, T. ICART, J.-F. MISARSKY, M. NAYA-PLASENCIA, P. PAILLIER, T. PORNIN, J.-R. REINHARD, C. THUILLET, M. VIDEAU. *Indifferentiability with Distinguishers: Why Shabal Does Not Require Ideal Ciphers*, 2009, http://eprint.iacr.org/2009/199.pdf, Cryptology ePrint Archive, Report 2009/199.

[66] F. DIDIER, Y. LAIGLE-CHAPUY. *Attacking the combination generator*, 2009, http://hal.archives-ouvertes.fr/hal-00401908/en/CH.

[67] A. MARIN. *Borne inférieure sur la capacité d'un canal quantique*, Université de Bordeaux, September 2009, Supervisor: Jean-Pierre Tillich, Mastère Cryptologie et Sécurité Informatique.

[68] D. MAURICE. *Borne supérieure sur la capacité de correction des codes stabilisateurs*, Ecole Normale Supérieure, Paris, August 2009, Supervisor: Jean-Pierre Tillich, Mastère Parisien de Recherche en Informatique.

[69] M. NAYA-PLASENCIA, A. RÖCK, J.-P. AUMASSON, Y. LAIGLE-CHAPUY, G. LEURENT, W. MEIER, T. PEYRIN. *Cryptanalysis of ESSENCE*, 2009, http://www.131002.net/data/papers/NRALLMP09.pdf, Disponible sur le SHA-3 Zoo CH .

References in notes

[70] J.-C. FAUGÈRE, A. OTMANI, L. PERRET, J.-P. TILLICH. *Algebraic Cryptanalysis of McEliece Variants with Compact Keys*, 2009.

[71] T. GE, S. ZDONIK. *Fast, Secure Encryption for Indexing in a Column-Oriented DBMS*, in "Proceedings of the 23rd International Conference on Data Engineering, ICDE 2007", IEEE, 2007, p. 676-685.

[72] A. SEZNEC, N. SENDRIER. *HAVEGE: A user-level software heuristic for generating empirically strong random numbers*, in "ACM Trans. Model. Comput. Simul.", vol. 13, n^{o} 4, 2003, p. 334-346.