INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Secret

Security, Cryptology and Transmissions

Paris - Rocquencourt

THEME SYM

Table of contents

1. Team

Research Scientist

Anne Canteaut [Team Leader, Research Director (DR) Inria, HdR]
Nicolas Sendrier [Research Director (DR) Inria, HdR]
Daniel Augot [Research Associate (CR) Inria, HdR]
Pascale Charpin [Research Director (DR) Inria, HdR]
Jean-Pierre Tillich [Research Associate (CR) Inria]

External Collaborator

Matthieu Finiasz [Assistant Professor (MC) ENSTA, Paris]
Grigory Kabatiansky [Senior Researcher IPIT, Academy of Sciences of Moscow, Russia]
Ayoub Otmani [Assistant Professor (MC), University of Caen]

Technical Staff

Mathieu Cluzeau [R&D Engineer]

PhD Student

Bhaskar Biswas [INRIA grant, Ecole Polytechnique]
Céline Blondeau [INRIA grant, Univ. P. et M. Curie]
Christophe Chabot [DGA grant, Univ. Limoges]
Maxime Côte [CIFRE grant, Ecole Polytechnique]
Cédric Faure [AMN grant, Ecole Polytechnique]
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]
María Naya Plasencia [INRIA grant, Univ. P. et M. Curie]
Andrea Röck [INRIA grant, Ecole Polytechnique]

Post-Doctoral Fellow

Sumanta Sarkar [Since December 2008]

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 two stream ciphers designed by the project-team in the final eSTREAM portfolio of recommended ciphers[1].** eSTREAM is a multi-year project running from 2004 to 2008, launched by the European network of excellence ECRYPT, to identify new stream ciphers that might become suitable for widespread adoption[2]. The project-team was involved in the design of 3 new stream ciphers which have been submitted to eSTREAM (among 34 candidates): SOSEMANUK, DECIM and F-FCSR. These three proposals belong to the 18 Phase-3 ciphers. In April 2008, SOSEMANUK and F-FCSR have been chosen in the final selection, which consists of 8 recommended ciphers.
- **Design of two new hash functions which have been submitted 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[3]. 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. The deadline for submitting a candidate was October 31, 2008. Among the 64 proposed candidates, two of them, named FSB and Shabal, have been proposed by the project-team. Moreover, we have broken two of the submitted proposals, Ponic and MCSSHA-3.
- **Reference implementations of code-based cryptosystems.** The first open-source reference implementations of code-based cryptography, namely of two versions McEliece public-key cipher and of the FSB hash function, have been written within the project-team and have been made publicly available. The implementation of McEliece cryptosystem has been included in the benchmarking tool SUPERCOP (System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives) developed within the European network of excellence ECRYPT[4].

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

[1] **http://www.ecrypt.eu.org/stream/portfolio.pdf**
[2] http://www.ecrypt.eu.org/stream/
[3] http://csrc.nist.gov/groups/ST/hash/sha-3/
[4] http://bench.cr.yp.to/

We also investigate some cross-disciplinary domains, which require a scientific competence coming from other areas, mainly social aspects of cryptology and quantum error correcting codes for fault tolerant quantum computing and quantum communications.

4. Software

4.1. HyMES - Hybrid McEliece System

The authors of HyMES are B. Biswas and N. Sendrier. It is available at http://www-rocq.inria.fr/secret/CBCrypto/index.php?pg=hymes and it is the first free open-source implementation of McEliece public-key encryption scheme. The software is meant to demonstrate the feasibility and the performances of code-based cryptosystems. It cannot be used for actual data encryption in the present version.

4.2. Stream ciphers

The three stream ciphers which have been submitted to the eSTREAM project, SOSEMANUK, DECIM and F-FCSR, have been implemented in software and the corresponding implementations are available on http://www.ecrypt.eu.org/stream/.

5. New Results

5.1. Security analysis of symmetric cryptosystems

Keywords: *cryptanalysis*, *hash functions*, *stream ciphers*, *symmetric cryptography*.

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. 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 and F-FCSR belong to the 8 recommended ciphers which have been included in the final portfolio of eSTREAM in April 2008 (among 34 submissions). Our work within the eSTREAM project also includes an important cryptanalytic effort on stream ciphers.
Recent results:

- Design of new stream ciphers: [46], [50], [49];
- Development of a new technique, which leads to a parallel implementation of sequences produced by feedback with carry shift register (FCSR); application to the eSTREAM candidate F-FCSR: [42], [41], [29];
- Estimation of the entropy loss of the internal state in some stream ciphers using a non-invertible next-state function: for a random next-state function [34] and for an FCSR in Galois representation [34];
- Evaluation of the bias of parity-check relations in the context of cryptanalysis of combination generators: [38], [17];
- Analysis of the vulnerability of the filter generator to an algebraic attack based on low-degree relations for the augmented function: [62];
- Design of a new attack against the combination generator: [39].

5.1.2. 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 ANR Project and with S. Manuel's PhD thesis. 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:

- Design of two new hash functions, submitted to the SHA-3 competition launched by the U.S. National Institute of Standards and Technology for defining a new standard: FSB [54] and Shabal [59];
- New cryptanalysis of SHA-0, the predecessor of the actual standard, SHA-1: [30];
- Cryptanalysis of a hash function family based on walks in LPS Ramanujan graphs recently introduced by Charles et al.: [35].
- Cryptanalysis of two hash functions submitted to SHA-3: Ponic [63] and MCSSHA-3 [56];
- Security evaluation of another SHA-3 candidate, CubeHash, which received the prize of the "most interesting CubeHash cryptanalysis" in November 2008[5]: [55].

5.1.3. 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.

[5] see http://cubehash.cr.yp.to/prizes.html

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 APN functions, which are the S-boxes ensuring an optimal resistance to differential cryptanalysis.

Recent results:

- Study of monomial bent functions: these functions are of interest since they lie as far as possible to the functions of degree 1 and they have a low implementation cost. Several classes of such functions of degree 3 have been exhibited and it has been proved that no other cubic exponent leads to a similar bent function: [12], [16];
- Study of the hyperbent criterion: this criterion, introduced in 1999, characterizes the functions which lie at the highest distance to all monomial permutations. Our recent work investigates the case of monomial hyperbent functions and their characterizations in terms of Kloosterman sums and Dickson polynomials [13], [23];
- Divisibility properties of Kloosterman sums: the values of the so-called classical Kloosterman sums over the finite field with 2^m elements is closely related to the Walsh spectra of some Boolean functions. Our new results on the divisibility of these values have also some impact for the determination of the weight distributions of the cosets of some BCH codes: [15], [14], [24];
- Study of APN power functions, *i.e.*, the functions which guarantee the best resistance to differential attacks: [27];
- Construction of a family of permutations over the field with 2^m elements from other mappings: [25];
- Resistance of S-boxes to truncated differential attacks: [57].

5.2. Code-based cryptography

Keywords: *McEliece cryptosystem*, *code-based cryptography*, *hash functions*, *postquantum cryptography*, *public-key cryptography*.

Participants: Daniel Augot, Biswas Bhaskar, Cédric Faure, Matthieu Finiasz, Stéphane Manuel, 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 Harald 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.

5.2.1. The class of McEliece-like cryptosystems.

The original McEliece cryptosystem remains unbroken. It has been proved by N. Sendrier [74], [73] that its security is provably reduced to two problems, conjectured to be hard, of coding theory:

- hardness of decoding in a random binary code, *in the average case*,
- pseudorandomness of Goppa codes.

This result also applies to Niederreiter's scheme and a similar result was already known for the digital signature scheme [71]. The reduction is not a guaranty of security, but we know that a significant improvement on one of the above problem must occur before the system is seriously threatened.

Recent results:

- Cryptanalysis of some variants of McEliece cryptosystem with a shorter public-key: the main drawback of the McEliece cryptosystem is probably the large size of its public key. There have been several attempts to reduce it. Using quasi-cyclic codes as the secret code of the scheme and preserving this property in the public code has been proposed repeatedly for this purpose in the literature [72], [69]. A. Otmani, J.P. Tillich and L. Dalot have broken these schemes by providing a way for recovering the secret code in both cases: [31].
- Cryptanalysis of McEliece-like ciphers using algebraic geometry codes: the PhD thesis of C. Faure will be defended in February 2009. There are mainly two parts in this work, one on rank metric codes with results in 2007 and before, and the other on algebraic geometry codes. C. Faure, together with L. Minder, has demonstrated that using algebraic geometry codes based on curves of low genus is not safe for McEliece-like cryptosystems. This work breaks a cryptosystem proposal by Janwa and Moreno, and has a strong negative impact on the use of the above family of codes in cryptography: [28].
- Evaluation of the security of code-based authentication protocols for RFID tags: the lightweight authentication protocol HB+ and its variants may be vulnerable to some attacks using decoding algorithms. V. Herbert has studied these protocols and he has compared the complexities of different decoding techniques in this context: [61].
- Open-source implementation of McEliece encryption scheme: the first open-source full implementation of (a variant of) McEliece encryption scheme has been provided by N. Sendrier and B. Biswas. A related paper was published at PQCrypto 2008 [22] and also, in French, at the C2 meeting in Carcans [37]. In particular, this implementation includes of improvement of the constant weight word encoding algorithm by N. Sendrier, a preliminary presentation of this work was made in [45] and a paper is in preparation. Using the opportunity of the above implementation and of the SHA3 FSB submission, we have created a coded-based crypto web portal at http://www-rocq.inria.fr/secret/CBCrypto/ which contains both HyMES and FSB and hopefully more in the future.
- N. Sendrier is coauthor, with R. Overbeck, of a 50-page chapter on *Code-based cryptography* in a book, entitled *PQCrypto*, to appear at the end of 2008: [51].

5.2.2. Cryptographic hash function with codes.

A new collision resistant hash-function has been proposed by the project-team for a few years based on the problem of decoding general binary linear codes [68]. It has the advantage of being fast and of having a *security reduction*, on the opposite of classical designs, based on MD5 and relatives, which have been broken recently.

The one-wayness of syndrome computation can be exploited in conjunction with quasi-cyclic codes. The purpose is to reduce the size of the constants (a big binary matrix). We have made several new propositions based on this principle: an evolution of the syndrome-based hash function and a stream cipher. The last of those contributions is the submission of a hash function by M. Finiasz, P. Gaborit, S. Manuel and N. Sendrier, to the SHA-3 NIST competition. The security of the proposed hash function, called FSB (for Fast Syndrome Based) is provably reduced to hard problems of algorithmic coding theory. The proposal description and its reference implementation are available online at http://www-rocq.inria.fr/secret/CBCrypto/index.php?pg=fsb: [54].

5.3. Decoding techniques, algebraic systems solving and applications

Keywords: *BCH codes*, *Groebner bases*, *LDPC codes*, *algebraic attack*, *code reconstruction*, *decoding algorithms*, *linear cryptanalysis*, *quantum codes*, *reverse engineering*.

Participants: Daniel Augot, Christophe Chabot, Mathieu Cluzeau, Maxime Cote, Cédric Faure, Matthieu Finiasz, Benoît Gérard, Jean-Pierre Tillich.

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[6] 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. Linear cryptanalysis and decoding Reed-Muller codes.

The first family of codes that we have studied in detail is the family of Reed-Muller codes. Being able to decode efficiently members of this family on various channels is very helpful for cryptanalysis: the decoding of first order Reed-Muller codes on the binary symmetric channel is a useful task for linear cryptanalysis whereas decoding general Reed-Muller codes on the erasure channel can be used in algebraic attacks of ciphers. In particular in his thesis [75], Cédric Tavernier found new (local) decoding algorithms for first order Reed-Muller codes over the binary symmetric channel, which improves upon the Goldreich-Rubinfeld-Sudan algorithm. This algorithm enables him to find new linear approximations of several rounds of the DES with biases of the same order as Matsui's approximations.

[6] Low-density parity-check code

Recent results:

- Linear cryptanalysis of block ciphers: following the work by C. Tavernier, B. Gérard has explored how to improve on Matsui's linear cryptanalysis by using all these new equations. 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 how many pairs of plaintext-ciphertext we need in 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: [40].
- Generalization of the Guruswami-Sudan list decoding algorithm to Reed-Muller codes: [48].

5.3.2. Solving algebraic systems and applications to coding.

Gröbner bases algorithms for solving algebraic systems is an important tool which can be applied both for error-correction and in cryptography, in the context of algebraic attacks.
Recent results:

- Decoding algorithms for cyclic codes with Gröbner bases: it was demonstrated that it is possible to find decoding formulas for all cyclic codes, by a Gröbner basis off-line computation. But, from the efficiency point of view, it was found that it is better to perform an on-line Gröbner bases computation, whose cost is reasonable. This enables to decode any cyclic code, up to their true minimum distance [67], [70]. An improved paper has been accepted for publication in the Journal of Symbolic Computation, with computational timings for non-trivial codes, of considerable length: [11].
- D. Augot is co-author, with E. Betti and E. Orsini of a chapter introducing cyclic codes, with their decoding algorithms, in a book devoted to Gröbner bases, coding and cryptography, in the RISC Book series: [47].
- Algebraic attacks: we have investigated some variants recent techniques for algebraic attacks, especially for stream cipher cryptanalysis: [62], [58], [60].

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. During his internship, A. Zeh has successfully generalized this method to the Guruswami-Sudan list decoding algorithm, where multiplicities are involved: [21], [36], [66].
- families of codes with good iterative decoding algorithms: this kind of codes has by now probably become the most popular coding scheme due to their exceptional performances at a reasonable algorithmic cost. We have in particular studied families of codes defined over large alphabets which are in a sense intermediate between turbo-codes and LDPC codes, and have found several instances of this family whose performance are quite close to the Shannon limit [65]. This work has been supported by France Telecom: [65].

5.3.4. Quantum codes.

The knowledge we have acquired in iterative decoding techniques has also lead 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. Notice 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. We have shown that the classical iterative decoding algorithms can be generalized to the quantum setting and have come up with some families of quantum LDPC codes and quantum serial turbo-codes with rather good performances under iterative decoding [32], [19], [64], [20].

5.3.5. 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[7], 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. Cluzeau and J.P. Tillich have found a lower bound on the number of codewords which have to be intercepted in order to recover the code. This lower bound turns out to be tight for several interesting code families such as LDPC codes for instance: [26].

6. Contracts and Grants with Industry

6.1. Industrial contracts

- **France Telecom R&D** $(02/06 \rightarrow 02/08)$
  Application of treillis/turbo/LDPC codes to modulations with a large number of states
  52 kEuros.

  This is a follow-up of a previous contract, aiming at constructing new families of binary codes with very good iterative decoding performances for a large range of rates and target error probabilities after decoding. The purpose is now to explore non-binary codes and completing the range of rates left by the previous contract.
- **I2E/AMESYS** $(01/07 \rightarrow 06/10)$
  Recognition of a coding scheme
  Partners: ENSTA, LIX, XLIM, INRIA projet-team SECRET.
  221 kEuros.

  This contract is funded by the DGA AINTERCOM call for offers. The context of this work is the analysis of a binary string in a non cooperative environment. The purpose is an academic research on related reconstruction problems, with a focus on error-correcting codes.
- **Société IPSIS** $(11/06 \rightarrow 10/09)$
  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] Kerckhoffs stated that principle in a paper entitled *La Cryptographie militaire*, published in 1883.

7. Other Grants and Activities

7.1. Other external funding

7.1.1. European initiatives

- **ECRYPT – European Network of Excellence** (02/04 → 08/08)
  http://www.ecrypt.eu.org/
  Partners: 33 European partners, both academic and industry.
  176 kEuros.

  This is a Network of Excellence in research in all the aspects of cryptology. It has been structured in "virtual labs". Our project-team is leading a working group within the virtual lab on symmetric techniques and it is in charge of the yearly deliverable *Open Research Areas in Symmetric Cryptography and Technical Trends in Lightweight Cryptography* [58]. The project-team is also involved in the AZTEC virtual lab (new primitives for public key cryptography).

7.1.2. 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 expected 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 has two purposes: understanding the recent attacks on cryptographic hash functions and suggesting new constructions based on coding theory.

- **Asphales** (05/04 → 01/08)
  Interactions between computer security and legal security for the progress of regulations in the Information Society.
  http://www.asphales.cnrs.fr/
  Partners: CNRS (labo. CECOJI), Univ. Versailles, Univ. Montpellier, INT, Univ. Lille 2, INRIA (project-team SECRET).
  20.2 kEuros.

  The aim of this multi-disciplinary project is to have a scientific reading of the French legal texts related to computer and network security. One main concern is to discuss the laws regarding the notion of proof, probative value and also the conservation of digital documents. Anne Canteaut and Marion Videau have provided a scientific view of many laws on these topics.

7.2. Visibility

7.2.1. Publishing activities.

- *Cahiers droit, sciences et technologies*, editorial board: A. Canteaut.
- *IEEE Transactions on Information Theory*, associate editor: A. Canteaut for *Cryptography and Complexity* 2005-2008.
- *Designs, Codes and Cryptography*, associate editor: P. Charpin, since 2003.
- Special issue of *Designs, Codes and Cryptography* dedicated to the WCC workshop, editors: D. Augot, P. Charpin and N. Sendrier.
- *Journal of Symbolic Computation*, Special Issue on *Gröbner Bases Techniques in Cryptography and Coding Theory* (2007), guest editor: D. Augot.

7.2.2. Program committees in 2008

- WCC 2009 (Workshop on coding and cryptography): May 10-15, 2009, Loftus, Norway (D. Augot, A. Canteaut, P. Charpin and N. Sendrier);
- AfricaCrypt 2009: June 21-25, 2009, Gammarth, Tunisia (A. Canteaut);
- Indocrypt 2008: December 14-17, 2008, Kharagpur, India (A. Canteaut);
- PQCrypto 2008: October 17-19, 2008, Cincinnati, USA (N. Sendrier);
- ITSL'08 (Conference on Information Theory and Statistical Learning: July 14-15, 2008, Las Vegas, USA (J.P. Tillich);
- Waifi 2008 (International Workshop on the Arithmetic of Finite Fields): July 6-9, 2008, Siena, Italy. July 6-9, (D. Augot);
- AfricaCrypt 2008: June 11-14, 2008, Casablanca, Marocco (A. Canteaut);
- SCC 2008 (First International Conference on Symbolic Computation and Cryptography): April 28-30, 2008, Beijing, China (A. Canteaut)
- Journées C2 "Codage et Cryptographie": March 17-21, 2008, Carcans, France (D. Augot and J.P. Tillich);
- FSE 2008, (Fast Software Encryption): Feb. 10-13, 2008, Lausanne, Switzerland (A. Canteaut);
- SASC 2008 (State of the Art of Stream Ciphers), Feb. 13-14, 2008, Lausanne, Switzerland (A. Canteaut);

7.2.3. Other responsibilities in the national community.

- P. Charpin is an external expert for the Délégation Générale pour l'Armement (DGA);
- A. Canteaut is a member of the scientific committee of the "UFR de sciences" of the university of Versailles-St Quentin;
- **"Commission de spécialistes"(Committees for the selection of professors and assistant professors)**: University Paris 8 (J-P. Tillich), University of Limoges (A. Canteaut), École Normale Supérieure Paris (J-P. Tillich), University of Caen (J.P. Tillich);
- A. Canteaut was in the charge of "training-through-research" for the Paris-Rocquencourt center from January 2008 to September 2008;
- A. Canteaut has been co-chair of the postdoc committee for the Paris-Rocquencourt center since September 2008.

7.2.4. Other responsibilities in the international community.

Anne Canteaut is a member of the steering committee of the eSTREAM project http://www.ecrypt.eu.org/stream/ and is in charge of the working group "Open research areas in symmetric cryptography" of the ECRYPT European network of excellence.

8. Dissemination

8.1. Teaching

- D. Augot, *Error-correcting codes*, M2, Univ. Paris 7, 12 h;
- D. Augot, *Cryptography*, M2, Univ. Marne-la-Vallée, 9 h;
- D. Augot, *Cryptography* M1, École Polytechnique, as an assistant : 15 h;
- D. Augot, *Information theory*, M1, Ecole Polytechnique, 36 h;
- D. Augot, *Cryptography*, lectures to Tunisian officers, Thales Group, 6 h;
- A. Canteaut, *Symmetric cryptography*, M2, Télécom Paris, 3 h;
- A. Canteaut, *Cryptography*, lectures to Tunisian officers, Thales Group, 70 h;
- A. Canteaut, *Principles of programming languages*, L3, Ecole Polytechnique, 40 h;
- J.-P. Tillich, *Error-correcting codes*, M2, Univ. Paris 7, 15 h;
- J.-P. Tillich, *Error-correcting codes*, M2, ISEP (Institut Supérieur d'Electronique de Paris), 10 h.
- J.-P. Tillich, *Cryptography*, lectures to Tunisian officers, Thales Group, 45 h;

8.2. Ph.D. committees

- B. Debraize, *Méthodes de cryptanalyse pour les schémas de chiffrement symétrique*, Université de Versailles-Saint Quentin, April 11, 2008, committee: A. Canteaut (reviewer);
- R. Medeiros , *Zero-error capacity of quantum channels*, Telecom ParisTech, September 24, 2008, committee: J.P. Tillich;
- P.-L. Cayrel, *Construction et optimisation de cryptosystèmes basés sur les codes correcteurs d'erreurs*, Université de Limoges, October 2, 2008, committee: N. Sendrier (reviewer);
- L. Sassatelli, *Codes LDPC multi-binaires hybrides et méthodes de décodage itératif*, Université de Cergy-Pontoise, October 3, 2008, committee: J.P. Tillich (reviewer);
- S. Lachartre, *Algèbre linéaire dans la résolution de systèmes polynomiaux - Applications en cryptologie*, Université Paris 6, December 11, 2008, committee: N. Sendrier (reviewer).

8.3. Participation to workshops/conferences in 2008

- ESC 2008, Echternach, Luxemburg, January 7-11, participant: Anne Canteaut.
- FSE 2008, Lausanne, Switzerland, February 10-13, participants: María Naya-Plasencia, Andrea Röck, Pascale Charpin, Stéphane Manuel.
- SASC 2008, Lausanne, Switzerland, February 13-14, participants: Maria Naya-Plasencia, Andrea Röck.
- Workshop on Coding Theory, Alicante, Spain, March 12-15, participant: Daniel Augot.
- Journées C2, Carcans, France, March 17-21, participants: Daniel Augot, Benoit Gérard, Bhaskar Biswas, Céline Blondeau, Anne Canteaut, Pascale Charpin, Cédric Faure, Yann Laigle-Chapuy, Stéphane Manuel, Maria Naya-Plasencia, Andrea Röck, Nicolas Sendrier, Jean-Pierre Tillich.
- EUROCRYPT 2008, Istanbul, Turkey, April 14-17, participant: Jean-Pierre Tillich.
- MITACS, Montreal, Canada, May 30-June 6, participant: Nicolas Sendrier.
- Workshop hash functions in cryptology, Leiden, The Netherlands, June 1-6, participant: Stéphane Manuel.
- AFRICACRYPT, Marocco, June 11-14, participant: Andrea Röck.

- ACCT, Pamporovo, Bulgaria, June 16-22, participants: Pascale Charpin, Cédric Faure.
- Workshop Kryptowochende, Germany, July 3-7, participant: Andrea Röck.
- IEEE International Symposium on Information Theory - ISIT, Toronto, Canada, July 6-12, participants: Mathieu Cluzeau, Jean-Pierre Tillich, Alexander Zeh.
- Waifi, Sienne, Italy, July 6-9, participant: Daniel Augot.
- SAC 2008, Sackville, Canada, August 13-15, participant: Benoit Gérard.
- Journées Cryptographie, Caen, France, September 5-6, participant: Jean-Pierre Tillich.
- SETA, Lexington, USA, September 13-19, participant: Andrea Röck.
- Workshop on Coding Theory Days, St Petersburg, Russia, October 4-12, participant: Pascale Charpin.
- PQCrypto, Cincinnati, USA, October 16-21, participants: Bhaskar Biswas, Nicolas Sendrier.
- ICT 2008, Lyon, France, November 25-27, participant: Stefan Dodunekov.
- INDOCRYPT, Kharagpur, India, December 14-17, participant: Nicolas Sendrier.

8.4. Visiting researchers

- Pr. Stefan Dodunekov, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria, 01-28/11/08;
- Pr. Sugata Gangopadhyay, Indian Institute of Technology, Roorkee, India, 20/05-20/07/08;
- Pr. Grigory Kabatianskiy, Institute for Problems of Information Transmission, RAS, Moscow, Russia, 30/03-13/04/08, 15-19/12/08;
- Lorenz Minder, LMA, EPFL, Switzerland, 03-06/02/08;
- Raphael Overbeck, Technische Universität Darmstadt, Germany, 03-08/03/08;
- Christiane Peters, Technische Universität Eindhoven, The Netherlands, 24-28/11/08;
- Pr. Victor Zinoviev, Institute for Problems of Information Transmission, RAS, Moscow, Russia, 31/03-12/04/08.

8.5. Visit to other laboratories

- Princeton University, USA (collaboration with C. Lauradoux), Andrea Röck, January 6-February 7.
- EPFL, Communications Laboratory, Lausanne, Switzerland, Jean-Pierre Tillich, September 28-October 2.
- Fachhochschule Nordwestschweiz, Windisch, Zurich, Switzerland (collaboration with W. Meier), Maria Naya-Plasencia, November 3-28.

9. Bibliography

Major publications by the team in recent years

[1] D. AUGOT, M. FINIASZ. *A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem*, in "Advances in Cryptology - EUROCRYPT 2003", Lecture Notes in Computer Science, n^{o} 2656, Springer-Verlag, 2003, p. 229-240.

[2] A. CANTEAUT, M. TRABBIA. *Improved fast correlation attacks using parity-check equations of weight 4 and 5*, in "Advances in Cryptology - EUROCRYPT 2000", LNCS, n^{o} 1807, Springer Verlag, 2000, p. 573–588.

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

[4] P. CHARPIN. *Cyclic codes with few weights and Niho exponents*, in "Journal of Combinatorial Theory, Series A", vol. 108, n^{o} 2, November 2004, p. 247-259.

[5] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *The Coset Distribution of the Triple-Error-Correcting Binary Primitive BCH Codes*, in "IEEE Transactions on Information Theory", vol. 52, n^{o} 4, 2006, p. 1727-1732.

[6] 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.

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

[8] J. FRIEDMAN, J.-P. TILLICH. *Generalized Alon-Boppana Theorems and Error-Correcting Codes*, in "SIAM Journal of Discrete Mathematics", vol. 19, n^{o} 3, 2005, p. 700-718.

[9] H. OLLIVIER, J.-P. TILLICH. *Description of a quantum convolutional code*, in "Phys. Rev. Lett.", quant-ph 0304189, vol. 91, n^{o} 17, 2003, http://www.arxiv.org/abs/quant-ph/0304189.

[10] A. SEZNEC, N. SENDRIER. *HAVEGE: User-level Software Heuristic for Strong Random Numbers*, in "ACM Transactions on Modeling and Computer Simulation", vol. 14, n^{o} 4, October 2003, p. 334-346.

Year Publications

Articles in International Peer-Reviewed Journal

[11] 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", to appear, 2008, 29, http://www-rocq.inria.fr/secret/Daniel.Augot/gbdecode.pdf.

[12] A. CANTEAUT, P. CHARPIN, G. KYUREGHYAN. *A new class of monomial bent functions*, in "Finite Fields and Their Applications", vol. 14, n^{o} 1, January 2008, p. 221-241.

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

[14] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *Divisibility properties of classical binary Kloosterman sums*, in "Discrete Mathematics", In press, 2008.

[15] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *On cosets of weight 4 of $BCH(2^m, 8)$, m even, and exponential sums*, in "SIAM Journal of Discrete Math.", vol. 23, n^{o} 1, 2008, p. 59-78.

[16] P. CHARPIN, G. KYUREGHYAN. *Cubic monomial bent functions: a subclass of $\mathcal{M}$*, in "SIAM Journal of Discrete Math.", vol. 22, n^{o} 2, 2008, p. 650-665.

Invited Conferences

[17] A. CANTEAUT. *Approximation of a combining function by functions of fewer variables*, in "ESC 2008 - Echternach Symmetric Cryptography seminar, Echternach, Luxembourg", Invited talk, January 2008.

[18] A. CANTEAUT. *La cryptographie symétrique : comment protéger la confidentialité des données à moindre coût*, in "Le modèle et l'algorithme, INRIA Paris-Rocquencourt", November 2008, http://www-c.inria.fr/Internet/rendez-vous/modele-et-algo/les-exposes-de-2008/la-cryptographie-symetrique-comment-proteger-la-confidentialite-des-donnees-a-moindre-cout.

[19] J.-P. TILLICH. *Quantum Turbo-codes*, in "Journées "Informatique Quantique" 2008, Paris", Invited Talk, January 2008.

[20] J.-P. TILLICH. *Une introduction aux codes correcteurs quantiques*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", Invited Talk, March 2008.

International Peer-Reviewed Conference/Proceedings

[21] D. AUGOT, A. ZEH. *On the Roth and Ruckenstein Equations for the Guruswami-Sudan Algorithm*, in "Proceedings of the 2008 IEEE International Symposium on Information Theory, ISIT 2008, Toronto, Canada", July 2008, p. 2620-2624.

[22] B. BISWAS, N. SENDRIER. *McEliece cryptosystem in real life: theory and practice*, in "International Workshop on Post-Quantum Cryptography - PQCrypto 2008", LNCS, vol. 5299, Springer, 2008, p. 47-62.

[23] P. CHARPIN, G. GONG. *Hyperbent functions, Kloosterman sums and Dickson polynomials*, in "Proceedings of the 2008 IEEE International Symposium on Information Theory, ISIT 2008, Toronto, Canada", July 2008, p. 1758-1762.

[24] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *Divisibility properties of Kloosterman sums over finite fields of characteristic two*, in "Proceedings of the 2008 IEEE International Symposium on Information Theory, ISIT 2008, Toronto, Canada", July 2008, p. 2608-2612.

[25] P. CHARPIN, G. KYUREGHYAN. *On a class of permutation polynomials over* $\mathbf{F}_{2^n}$, in "Sequences and Their Applications, SETA 2008", LNCS, n$^{\text{o}}$ 5203, Springer, 2008, p. 368–376.

[26] M. CLUZEAU, J.-P. TILLICH. *On the code reverse engineering problem*, in "Proceedings of the 2008 IEEE International Symposium on Information Theory, ISIT 2008, Toronto, Canada", July 2008, p. 634-638.

[27] D. K. DALAI. *On 3-to-1 and power APN S-boxes*, in "Sequences and Their Applications, SETA 2008", LNCS, n$^{\text{o}}$ 5203, Springer, 2008, p. 377–389.

[28] C. FAURE, L. MINDER. *Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes*, in "Proceedings of the 11th international workshop on Algebraic and Combinatorial Coding Theory, ACCT 2008", 2008, p. 99–107.

[29] C. LAURADOUX, A. RÖCK. *Parallel Generation of l-sequences*, in "Sequences and Their Applications, SETA 2008", LNCS, n$^{\text{o}}$ 5203, Springer, 2008, p. 299-312.

[30] S. MANUEL, T. PEYRIN. *Collisions on SHA-0 in One Hour*, in "Fast Software Encryption - FSE 2008", LNCS, n^{o} 5086, Springer, 2008, p. 16-35.

[31] A. OTMANI, J.-P. TILLICH, L. DALLOT. *Cryptanalysis of McEliece Cryptosystem Based on Quasi-Cyclic LDPC Codes*, in "Proceedings of First International Conference on Symbolic Computation and Cryptography, Beijing, China", LMIB Beihang University, April 28-30 2008, p. 69–81.

[32] D. POULIN, J.-P. TILLICH, H. OLLIVIER. *Quantum serial turbo-codes*, in "Proceedings of the 2008 IEEE International Symposium on Information Theory, ISIT 2008, Toronto, Canada", July 2008, p. 310-314.

[33] A. RÖCK. *Entropy of the Internal State of an FCSR in Galois representation*, in "Fast Software Encryption - FSE 2008", LNCS, n^{o} 5086, Springer, 2008, p. 343-362.

[34] A. RÖCK. *Stream Ciphers Using a Random Update Function: Study of the Entropy of the Inner State*, in "AFRICACRYPT 2008", LNCS, n^{o} 5023, Springer, 2008, p. 258-275.

[35] 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.

Workshops without Proceedings

[36] D. AUGOT, A. ZEH. *Key Equations for the Guruswami-Sudan Decoding Algorithm*, in "Workshop on Coding and Systems, Alicante, Spain", March 2008.

[37] B. BISWAS, N. SENDRIER. *Cryptosystème de McEliece: sécurité et implémentation*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

[38] A. CANTEAUT, M. NAYA-PLASENCIA. *Approximation d'une fonction à l'aide de moins de variables*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

[39] F. DIDIER, Y. LAIGLE-CHAPUY. *Cryptanalyse de LFSRs combinés*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

[40] B. GÉRARD, J.-P. TILLICH. *Codage et cryptanalyse linéaire*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

[41] C. LAURADOUX, A. RÖCK. *Parallel Generation of ℓ-Sequences*, in "Kryptowochenende, Tabarz, Germany", March 2008.

[42] C. LAURADOUX, A. RÖCK. *Synthèse des ℓ-séquences décimées*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

[43] S. MANUEL. *Produire une collision pour SHA-0 en une heure*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

[44] A. OTMANI, J.-P. TILLICH, L. DALLOT. *Cryptanalyse d'un cryptosystème de McEliece utilisant des codes LDPC quasi-cycliques*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

[45] N. SENDRIER. *Codage des mots de poids constant*, in "Journées "Codage et Cryptographie" 2008, Carcans (Gironde)", March 2008.

Scientific Books (or Scientific Book chapters)

[46] F. ARNAULT, T. BERGER, C. LAURADOUX. *F-FCSR stream ciphers*, in "New Stream Cipher Designs - The eSTREAM finalists", LNCS, vol. 4986, Springer, 2008, p. 170-178.

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

[48] 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, to appear, Springer, Heidelberg, 2009.

[49] C. BERBAIN, O. BILLET, A. CANTEAUT, N. COURTOIS, B. DEBRAIZE, H. GILBERT, L. GOUBIN, A. GOUGET, L. GRANBOULAN, C. LAURADOUX, M. MINIER, T. PORNIN, H. SIBERT. *Decim v2*, in "New Stream Cipher Designs - The eSTREAM finalists", LNCS, vol. 4986, Springer, 2008, p. 140-151.

[50] C. BERBAIN, O. BILLET, A. CANTEAUT, N. COURTOIS, H. GILBERT, L. GOUBIN, A. GOUGET, L. GRANBOULAN, C. LAURADOUX, M. MINIER, T. PORNIN, H. SIBERT. *Sosemanuk: a fast software-oriented stream cipher*, in "New Stream Cipher Designs - The eSTREAM finalists", LNCS, vol. 4986, Springer, 2008, p. 98-118.

[51] R. OVERBECK, N. SENDRIER. *Code-based cryptography*, in "Post-Quantum Cryptography", to appear, Springer, 2008.

Books or Proceedings Editing

[52] D. AUGOT, J.-C. FAUGÈRE, L. PERRET (editors). *Gröbner Bases Techniques in Cryptography and Coding Theory*, Springer, to appear.

[53] P. CHARPIN, T. HELLESETH, D. AUGOT, G. LEANDER, N. SENDRIER (editors). *Special issue in Coding and Cryptography - In memory of Hans Dobbertin*, vol. 49 (1–3), Designs, Codes and Cryptography, Springer, 2008.

Other Publications

[54] D. AUGOT, M. FINIASZ, P. GABORIT, S. MANUEL, N. SENDRIER. *SHA-3 proposal: FSB*, October 2008, http://www-rocq.inria.fr/secret/CBCrypto/fsbdoc.pdf, Submission to NIST.

[55] J.-P. AUMASSON, W. MEIER, M. NAYA-PLASENCIA, T. PEYRIN. *Inside the Hypercube*, November 2008, http://eprint.iacr.org/2008/486.pdf, Cryptology ePrint Archive, Report 2008/486.

[56] J.-P. AUMASSON, M. NAYA-PLASENCIA. *Second preimages on MCSSHA-3*, November 2008, http://131002.net/data/papers/AN08.pdf, Available online.

[57] C. BLONDEAU. *La cryptanalyse différentielle tronquée*, 64 pages. Supervision : Pascale Charpin, Masters Thesis report, Université de Limoges, September 2008.

[58] A. CANTEAUT, D. AUGOT, C. CID, H. ENGLUND, H. GILBERT, M. HELL, T. JOHANSSON, M. PARKER, T. PORNIN, B. PRENEEL, C. RECHBERGER, M. ROBSHAW. *D.STVL.9 - Ongoing Research Areas in Symmetric Cryptography*, 108 pages, July 2008, Report of the ECRYPT European Network of Excellence.

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

[60] C. CID, M. ALBRECHT, D. AUGOT, A. CANTEAUT, R.-P. WEINMANN. *D.STVL.7 - Algebraic cryptanalysis of symmetric primitives*, 42 pages, July 2008, Report of the ECRYPT European Network of Excellence.

[61] V. HERBERT. *Systèmes d'authentification basés sur les codes correcteurs d'erreurs*, 60 pages. Supervision: Nicolas Sendrier, Masters Thesis report, Université de Grenoble, September 2008.

[62] S. JACOB. *Analyse de la résistance aux attaques algébriques des fonctions de filtrage augmentées*, Supervision: Anne Canteaut, Masters Thesis report, Université Paris 7, November 2008.

[63] M. NAYA-PLASENCIA. *Second preimage attack on Ponic*, November 2008, http://131002.net/data/papers/ponic.pdf, Available online.

[64] J.-C. SIBEL. *Décodage de codes correcteurs quantiques*, Supervision: Jean-Pierre Tillich, September 2008, Engineering school internship report.

[65] J.-P. TILLICH. *Contrat de recherche France Télécom: application des codes Treillis/turbo-LDPC aux modulations codées à grand nombre d'états*, 54 pages, November 2008, Final report of the France Télécom contract.

[66] A. ZEH. *A Key Equation for the Guruswami-Sudan Algorithm*, Supervision : Daniel Augot, Masters Thesis report, Télécom Paris, February 2008.

References in notes

[67] D. AUGOT, M. BARDET, J.-C. FAUGÈRE. *Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Groebner bases*, in "Proceedings of the 2003 IEEE International Symposium on Information Theory, ISIT 2003, Yokohama, Japan", IEEE Press, June 2003, 362.

[68] D. AUGOT, M. FINIASZ, N. SENDRIER. *A Family of Fast Syndrome Based Cryptographic Hash Function*, in "Ecrypt Conference on Hash Functions, Krakow, Poland", June 2005.

[69] M. BALDI, F. CHIARALUCE. *Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes*, in "Proceedings of the 2007 IEEE International Symposium on Information Theory, ISIT 2007, Nice, France", March 2007, p. 2591–2595.

[70] M. BARDET. *Etude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*, PhD Thesis, Université Paris 6, December 2004.

[71] 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.

[72] P. GABORIT. *Shorter keys for code based cryptography*, in "International Workshop on Coding and Cryptography - WCC 2005, Bergen, Norway", March 2005, p. 81–91.

[73] N. SENDRIER. *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs*, Mémoire d'habilitation à diriger des recherches, Université Paris 6, March 2002.

[74] N. SENDRIER. *On the security of the McEliece public-key cryptosystem*, in "Information, Coding and Mathematics", In honor of Bob McEliece on his 60th birthday. Invited paper, Kluwer, 2002, p. 141–163.

[75] C. TAVERNIER. *Testeurs, problèmes de reconstruction univariés et multivariés, et application à la cryptanalyse du DES.*, PhD thesis, École Polytechnique, Palaiseau, January 2004.