INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Codes

Codage et cryptographie

Paris - Rocquencourt

THEME SYM

Table of contents

1. Team

Head of project-team
Nicolas Sendrier [Research Director (DR) Inria, HdR]

Vice-head of project-team
Daniel Augot [Research Associate (CR) Inria, HdR]

Administrative assistant
Christelle Guiziou-Cloitre [Secretary (TR) Inria]

Staff members
Pascale Charpin [Research Director (DR) Inria, HdR]
Anne Canteaut [Research Director (DR) Inria, HdR]
Jean-Pierre Tillich [Research Associate (CR) Inria]

External collaborators
Matthieu Finiasz [Post-doc EPFL, Lausanne, Switzerland]
Grigory Kabatiansky [Senior Researcher IPIT, Academy of Sciences of Moscow, Russia]
Ayoub Otmani [Assistant Professor (PR), University of Caen]

Post-doctoral fellows
Deepak Kumar Dalai [Post-doc Inria]

Ph.D. students
Bhaskar Biswas [EGIDE grant]
Thomas Camara [ATER]
Christophe Chabot [DGA grant]
Maxime Cote [CIFRE grant]
Frédéric Didier [AMN grant]
Cédric Faure [AMN grant]
Benoît Gérard [DGA grant]
Maria Naya Plasencia [INRIA grant]
Yann Laigle-Chapuy [AMN grant]
Cédric Lauradoux [INRIA grant]
Stéphane Manuel [INRIA grant]
Andrea Roeck [INRIA grant]
Bassem Sakkour [Syrian grant]

Student interns
Benoît Gérard [UVSQ Master 2 internship, 01-04/30-09]
Franck Giton [Université de Limoges Master 2 internship, 20-02/07-09]
Rima Hanèche [EGIDE internship 01-10-2007/31-3-2008]
Iyed Ben Slimen [ENIT Tunis, STIC Tunisie internship 01-04/30-04]
Olfa Trabelsi [ENIT Tunis, STIC Tunisie internship 26-11/16-12]
Alexander Zeh [ENST Master 2 internship, 01-07-2007/31-01-2008]

2. Overall Objectives

2.1. Presentation and scientific foundations

The research work of the team project CODES is mostly devoted to the design and analysis of cryptographic algorithms through the study of the discrete structures that they involve.

Our multiple competences in mathematics and algorithmics have allowed us to address a large variety of problems related to information protection. Most of our work mix fundamental aspects (study of mathematical objects) and practical aspects (cryptanalysis, design of algorithms, implementations).

Our application domains are mainly cryptography, error correcting codes and code recognition (“electronic war”). Even though these domains may appear different, our approach is unified. For instance, decoding techniques are used to design new error correcting codes, but also new cryptanalysis. Code recognition (that is recognizing an unknown coding scheme from a sample), is very similar to stream cipher cryptanalysis...

Our research is driven by the belief that discrete mathematics and algorithmics of finite structure form the scientific core of (algorithmic) data protection. We think that our past results justify this approach and we feel that, with the evolution of cryptographic research, more and more researchers will follow this path.

Our purpose is not to present more evidence that algebraic coding theory or discrete mathematics can be “applied to” cryptography, but to convince that these fields belong the the scientific foundations of cryptography or more generally data protection techniques.

2.2. Highlights

- Submission of 3 ciphers to eSTREAM. eSTREAM is a multi-year project, launched by the European network of excellence ECRYPT, to identify new stream ciphers that might become suitable for widespread adoption[1]. The project-team participates to 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 remaining 18 proposals which have been selected for the next phase of eSTREAM.
- Organization of the international conference WCC’07 (140 attendants) at INRIA Rocquencourt. Program cochairs: Daniel Augot and Nicolas Sendrier. General cochairs: Anne Canteaut and Pascale Charpin. The full version of the best contributions will be published in the journal DCC (Design, Codes and Cryptography). Guest editors: Pascale Charpin and Tor Helleseth (co-guest editors: Daniel Augot, Gregor Leander and Nicolas Sendrier).
- Daniel Augot defended his *habilitation à diriger des recherches* entitled “Décodage des codes algébriques et cryptographie” on June the 7th, 2007. He studied the use of computer algebra for decoding two important classes of codes, evaluation codes and syndrome-defined codes. He also studied the hardness of the related computational problems, and showed how to use such hardness results to define cryptographic primitives.

3. Application Domains

3.1. Application Domains

- Error correcting codes
- Cryptology
- Code reconstruction

4. Software

4.1. Software

Anne Canteaut, Cédric Lauradoux and Marine Minier are co-authors of three new stream cipher proposals which have been submitted to the eSTREAM project: SOSEMANUK, DECIM and F-FCSR. These three ciphers have been implemented in software and the corresponding implementations are available on http://www.ecrypt.eu.org/stream/.

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

Since SOSEMANUK is a software-oriented stream cipher aiming at a high throughput, some optimized implementations have been developed. Actually, SOSEMANUK is one of the fastest and most secure ciphers among the 22 eSTREAM candidates dedicated to software applications.

DECIM and F-FCSR are dedicated to hardware environments where the available resources such as gate complexity and power might be heavily restricted. A VHDL implementation of both ciphers has been realized by Cédric Lauradoux.

5. New Results

5.1. Security analysis of symmetric cryptosystems

Participants: Anne Canteaut, Pascale Charpin, Frédéric Didier, Yann Laigle-Chapuy, Deepak Kumar Dalai, Cédric Lauradoux, Maria Naya Plasencia, 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 functionalities 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...).

Research in symmetric cryptography is obviously characterized by a sequence of defenses and attacks. But, each new dedicated attack against a given cryptosystem must be formalized, its scope must be analyzed and the structural properties which make it feasible must be highlighted. This approach is the only one which can lead to new design criteria and to the constructions of building blocks which guarantee to a provable resistance to the known attacks. However, such an analysis yields a practical system only if it includes the implementation requirements arising from the applications. Therefore, our work 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. This joint approach of the different aspects of symmetric cryptography is quite peculiar to our work.

5.1.1. Cryptanalysis.

In the last few years, with the eSTREAM project, our cryptanalytic effort has focused on stream ciphers. In particular, we have investigated the security of one of the simplest stream cipher, namely the linear feedback shift register (LFSR) filtered by a Boolean function during the contract with the DGA and the CELAR. Many of the cryptanalytic attacks on such a scheme start by finding low-weight multiples of its tap polynomial. We have improved on the best known algorithm for achieving this task in the case of multiples of even weight [35] by calculating discrete logarithms. Furthermore, we have also devised an attack [34] that recovers the initial state of the LFSR by detecting the positions where the inputs of the filtering function are equal to zero. By a careful analysis, we have shown that the attack complexity is among the best known and that it works for virtually all filter functions. A related stream cipher called "Achterbahn" and its variants, which relies on shift registers but this time with non-linear feedback and which is one of the stream cipher proposal to the eSTREAM project has been proved insecure in [44], [45], [46], [43].

We have also investigated attacks using the impact of entropy loss caused by random functions in [49], [48].
Publications : [35], [34], [44], [45], [46], [43], [49], [48]

5.1.2. 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 in our project, both for stream ciphers and for block ciphers. This work involves fundamental aspects related to discrete mathematics 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 [17], [21]. We have also been interested in APN functions, which are the S-boxes ensuring an optimal resistance to differential cryptanalysis. P. Charpin, T. Helleseth and V. Zinoviev continue the extensive study of the differential properties of the AES S-box, i.e. the inverse function, which is the power permutation of an even number of variables offering the best resistance to differential cryptanalysis [20][19]. This work is related with the study of cosets of 3-error-correcting BCH-codes.

Guang Gong, from the university of Waterloo spent two months at INRIA (Codes). During this time, she worked with P. Charpin on a new criterion of S-box design which was introduced in 1999, the *Generalized Nonlinearity*.

More generally, all this work on S-boxes highlights the importance of finding new classes of permutation polynomials. This is the topic of Y. Laigle-Chapuy's PhD thesis and his results in this direction have been published in [23] and [38].
Publications : [30], [17], [21], [20], [19], [32], [33], [41], [23], [38]

5.1.3. Design of new primitives.

The previously described long-term research work in symmetric cryptographic has also led to concrete realizations since A. Canteaut, C. Lauradoux and M. Minier are co-authors of three new stream cipher proposals which have been submitted to the eSTREAM project: SOSEMANUK, DECIM and F-FCSR [60]. SOSEMANUK is one of the fastest and most secure ciphers among all candidates dedicated to software applications. DECIM and F-FCSR are hardware-oriented cipher for low-resource environments. Among the 34 submissions, these three proposals belong to the remaining 18 proposals which have been selected for the next phase of eSTREAM.
Publications : [40], [39], [25]

5.2. Code-based cryptography

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

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 lattices (NTRU,...), multivariate cryptography (HFE,...) and code-based cryptography (McEliece encryption scheme,...).

We have been investigating in details the latter field. The first cryptosystem based on error-correcting codes was a public key encryption scheme proposed by Bob 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, 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 key encryption.

5.2.1. The class of McEliece like cryptosystems.

The original McEliece cryptosystem remains unbroken. Nicolas Sendrier has proved [63], [62] 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 [61]. 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.

Another important work in the period was on the implementation aspects. One of the most promising code-based cryptosystem is the digital signature scheme: with 80 bits, its produces the shortest known digital signatures (without compromising the security level). The drawback is that signing a document required more than one minute on a standard PC. A work in collaboration with ENS Lyon (ARENAIRE) and the LIRMM was initiated, and funded through the ACI OCAM. This resulted in an improved software version (about 10 seconds) and a fast FPGA implementation in less than one second (on a low cost FPGA).

Various aspects of implementation where also considered throughout the period, see [64] for instance, where the problem of fast encoding of words with constant Hamming weight (required in Niederreiter's encryption scheme) is addressed. In practice this encoding is the most expensive part of Niederreiter's encryption and we obtain a speedup factor of 8 (33 Mbit/s instead of 4 Mbits/s).

Some work, by Nicolas Sendrier and Bhaskar Biswas, is in progress for improving the implementation of those systems. The first step being an implementation of McEliece was submitted in 2007 to EBATS[2].

5.2.2. Other cryptographic functionalities with codes.

We have proposed a new collision resistant hash-function based on the problem of decoding general binary linear codes [58]. 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 [50] can be exploited in conjunction with quasi-cyclic codes. The purpose is to reduce size of the constants (a big binary matrix). We have made several new proposition, an evolution of the syndrome based hash function [36] and a stream cipher [37]. In another direction, we are considering new hash function operating modes [42] with which we hope to produce primitives with a good resistance to collision search.
Publications : [50], [36], [37], [42]

5.2.3. Group key agreement

Securing messages in dynamic groups is an issue which is usually adressed by establishing a secret session key which is used for encryption and authentication. Establishing such a session key is performed with the principles of public key cryptography. Following the result of Augot et al [16] on dynamic group key agreement, an implementation in NS2 (Network simulator) has been done in collaboration with the Hipercom project team. There is a big gap between the crypto world and the real world, and there is an issue when trying to make a robust protocol resilient to message losses. We have such a proposition for managing message losses, and the implementation is showing that the proposed protocol behaves well. The problem mainly boils down to a robust leader election in an Ad Hoc network. The optimization of the parameters is ongoing.
Publications : [16]

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

5.3. Decoding techniques, algebraic systems solving and applications

Participants: Daniel Augot, Thomas Camara, Christophe Chabot, Mathieu Cluzeau, Maxime Cote, Frédéric Didier, Benoît Gérard, Franck Giton, Rima Hanèche, Bassem Sakkour, Jean-Pierre Tillich.

The announced objective in 2002 which was " applications of new decoding algorithms; resolution of algebraic systems " has evolved with the arrival of Jean-Pierre Tillich. It has laid more stress on probabilistic decoding algorithms and applications in error correcting. We are focusing now on studying or on improving various decoding algorithms which are either algebraic or probabilistic in nature, not only for cryptographic purposes but also for coding theory by itself. We have also strengthened our ties with the INRIA project-team SALSA (formerly SPACES) with the co-direction of Magali Bardet's thesis and during the ACI POLYCRYPT.

Research on decoding algorithms is one of the most active area in coding theory, be they of algebraic or probabilistic nature. These algorithms have found areas of applications outside the sole scope of error-correcting codes: complexity theory, theoretical computer science and cryptology among others. We are mainly interested in cryptographic applications of these algorithms: for example in fast correlation attacks on stream ciphers involving iterative decoding algorithms, or for the approximation of the output bits of the intermediate rounds of block ciphers. We have also found a new domain of application for iterative decoding algorithms, namely quantum error correcting codes for which we have shown that some of them can be decoded successfully with these algorithms. Moreover, the tools we had to investigate, for instance, the Gröbner bases techniques in the problem of decoding general cyclic codes, enabled us to study also algebraic attacks on cryptosystems. We also mention that we still study more traditional aspects of coding theory by searching for codes with good decoding performances for instance.

5.3.1. Decoding algorithms and cryptanalysis.

The first family of codes what 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 [65], Cédric Tavernier found new (local) decoding algorithms for first order Reed-Muller codes over the binary symmetric channel, which improve upon the Goldreich-Rubinfeld-Sudan algorithm. He implemented them for finding approximations of the outputs of several rounds of the DES. This way he found, using his software, not only the linear equations found by Matsui in his famous linear cryptanalysis of the DES, but also several other equations with biases of the same order as Matsui's ones. This work has been followed up by the internship [55] and the PhD of Benoît Gérard which explores how to improve on Matsui's linear cryptanalyis by using all these new equations. It turns out that recovering the key from these approximations is equivalent to decode a linear code on the Gaussian channel. We have used this relationship 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.
Publications : [55]

5.3.2. Solving algebraic systems and applications.

Daniel Augot has studied how to decode 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 [57], [59]. An improved paper has been submitted to the Journal of Symbolic Computation, with computational timings for non trivial codes, of considerable length.
Publications : [26], [27]

5.3.3. Coding theory

Franck Giton was an intern on the topic of the Fourier Transform over small finite fields, with precomputation. He studied an algorithm from Fedorenko, and produced an implementation. At this stage, the implementation is not very efficient, but nevertheless shows the improvement obtained with Fedorenko's method [54]. To improve the implementation requires skills in compilation and code optimisation, we plan to eventually continue this action. An efficient Fourier Transform has good potentialities to improve the decoding of algebraic codes. This has impact on code based cryptosystems, like the McEliece one.

Alexander Zeh has studied an old paper (2000) from Roth and Ruckenstein, where the authors describe a very efficient method for implementing the Sudan decoding algorithm. It has yet to be done to generalize this method to the Guruswami-Sudan list decoding algorithm, where multiplicities are involved. This internship will be finished in 2008, with an implementation. We hope to have the first efficient implementation of the Guruswami-Sudan algorithm.

In his habilitation, Daniel Augot has generalized the Guruswami-Sudan algorithm to the multivariate case. Yet another generalization relies on the very large theory of *order domain*, and codes defined with *order domain*. Geil and Matsumoto have designed a Sudan algorithm for these codes, which encompass Reed-Solomon codes, Reed-Muller codes and Algebraic-Geometry codes. An internship (Rima Hanèche) is ongoing for studying the theory of order domains and related bounds for the obtained codes.

We have also studied 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 which are in a sense intermediate between turbo-codes and LDPC codes, and have found several instances of this family covering a large range of rates which are among the best known for a large range of target error probabilities after decoding [24]. We have also investigated the minimum distance properties of such families in [47]. This work has been supported by France Telecom.

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 ACI project "RQ" in which we were involved is 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 [29].
Publications : [11], [54], [24], [29], [47]

5.3.4. Code reconstruction.

The context of this work is the reverse engeneering of the components of a transmission scheme. We start from the observation of a noisy binary stream. We wish to determine by algorithmic means which error correcting code has been used. Matthieu Cluzeau is the main contributor with a conference at ISIT 2006 and an article in IEEE Computers. He defended his phd thesis in November (co-advisors: Anne Canteaut and Nicolas Sendrier). Two new phd students started on this topic in 2006: Maxime Côte (co-advisors: Nicolas Sendrier and Jean-Pierre Tillich) and Christophe Chabot (co-advisors: Thierry Berger and Nicolas Sendrier).
Publications : [31], [22]

6. Contracts and Grants with Industry

6.1. Industrial contracts

Contract I2E $(01/07 \rightarrow 06/10)$ "Reconnaissance de schémas de codage". 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.

Partners: ENSTA, LIX, XLIM, INRIA

FT R&D $(02/06 \rightarrow 02/08)$ This is a follow-up of a previous contract, aiming at constructing new family 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.

6.2. Grants

IPSIS $(10/06 \rightarrow 9/09)$ We collaborate with the IPSIS company on the code reconstruction problem by sharing a PhD student, Maxime Côte, who is paid by a CIFRE grant.

7. Other Grants and Activities

7.1. Other external funding

7.1.1. National initiatives

ANR EDHASH $(01/07 \rightarrow 12/09)$ Evaluation and Design of secure HASH functions. This project has two purposes : understanding the recent attacks on cryptographic hash functions and suggesting new constructions based on coding theory.

Partners: INRIA (CODES) and UVSQ/PRISM (Equipe Crypto).

ACI ACSION $(09/04 \rightarrow 09/07)$ New applications of error correcting codes to information security. The project studies the impact of certain error-correcting tools for cryptographic purposes, more specifically:
- attacks on ciphers making use of decoding techniques are investigated,
- authentication and biometric schemes based on error-correcting codes are developed.

Partners: ENST, Université Paris VIII.

ACI SERAC $(09/04 \rightarrow 09/07)$ Security for Wireless Ad Hoc Networks. This covers several aspects of security: first the problem of securing the routing process itself, like OLSR; then the problem of developing more high level security primitives, which still have to be secured even in presence of network failures typical of Ad Hoc networks.

Partners: USTL (Lille), INRIA (CODES, TANC and HIPERCOM) and GET (ENST).

ACI ASPHALES $(05/04 \rightarrow 05/07)$ Interactions between computer security and legal security for the progress of regulations in the Information Society.

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 which concern the notion of proof, probative value and also to convervation of numerical documents. Anne Canteaut and Marion Videau have provided a scientific view of many laws on these topics. This project has also some consequences on cryptographic protocols, since the legal requirements may differ from classical cryptographic hypotheses.

Partners: CNRS (labo. CECOJI), Univ. Versailles, Univ. Montpellier, INT, Univ. Lille 2, INRIA.

ANR RAPIDE $(01/07 \rightarrow 12/10)$ Design and analysis of stream ciphers dedicated to constraint environments. 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.

Partners: LORIA (project-team CACAO), INRIA (project-team CODES), INSA Lyon (team Middleware/Security), University of Limoges (XLIM).

7.1.2. European projects

IST NoE ECRYPT $(02/04 \rightarrow 02/08)$ This a Network of Excellence in research in all the aspects of cryptology. It has been structured in "virtual labs". Anne Canteaut is leading the working group "Open research areas in symmetric cryptography" within the virtual lab on symmetric techniques, and CODES is also involved in the AZTEC virtual lab (new primitives for public key cryptography).

Partners: more than thirty, both academic and industry.

7.1.3. Other funding

Contract DGA-CELAR $(09/06 \rightarrow 09/07)$ The aim of this study is to analyze the efficiency of fast correlation attacks (of stream ciphers) based on iterative decoding algorithms. The work is to cryptanalyze several challenging stream ciphers, provided by the CELAR, which are weak versions of public domain ciphers. This should lead to a precise analysis of the efficiency of these attacks, and also to variants of the classical iterative decoding algorithms.

7.2. Visibility

7.2.1. Publishing activities.

Cahiers droit, sciences et techniques editorial board : A. Canteaut.

IEEE Transactions on Information Theory associate editors: Anne 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 and N. Sendrier.

Journal of Symbolic Computation Special Issue on *Gröbner Bases Techniques in Cryptography and Coding Theory* (2007), D. Augot guest editor.

7.2.2. Program commitees in 2007

Africacrypt 2008, Casablanca, A. Canteaut;

ECYPT Hash functions workshop, Barcelona, A. Canteaut;

Eurocrypt Barcelona, A. Canteaut;

ISIT IEEE International Symposium on Information Theory, Nice, A. Canteaut;

FSE 2008 Fast Software Encryption, Lausanne A. Canteaut;

SASC State of the Art in Stream ciphers, Bochum, A. Canteaut;

ICCC *Eleventh IMA International Conference onCryptography and Coding*, Cirencester, P. Charpin;

WCC *International Workshop on Coding and Cryptography*, Paris, D. Augot (program, co-chair), A. Canteaut (organizing co-chair), P. Charpin (organizing co-chair), N. Sendrier (program co-chair), J.P. Tillich.

7.2.3. Organization of conferences.

All members of CODES are involved in the organization of the *Workshop on Coding Theory and Cryptography (WCC)* which was at INRIA in April 2007. A. Canteaut and P. Charpin are general co-chairs. This workshop aims at bringing together researchers in all aspects of coding theory, cryptography and related areas.

7.2.4. Other responsibilities in the national community.

ACI-Sécurité et Informatique Scientific committee of the national research program on Security and Computer Science, *ACI-Sécurité et Informatique*: P. Charpin (2003-07);

SeSur Scientific committee of the national research program SeSur ("Sécurité et Sûreté) of the National Agency for Research (ANR), (2007), A. Canteaut;

DGA Pascale Charpin is an external expert for the Délégation Générale pour l'Armement (DGA);

Scientific committee A. Canteaut is 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);

CR2 A. Canteaut is member of the committee for the CR2 selection at INRIA-Futurs (2007);

"Comité des Bourses" Anne Canteaut is president of the "Comité des Bourses de l'INRIA Rocquencourt".

7.2.5. Other responsabilities 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

Cryptography A. Canteaut is teaching symmetric cryptography at the ENST, 6 hours.

Principles of programming languages A. Canteaut is giving exercise sessions on this topic at the École Polytechnique.

Error-correcting codes, symbolic computing and applications to cryptography Daniel Augot and J.P. Tillich are teaching in Master Recherche 2, Master Parisien de Recherche en Informatique (MPRI), University Paris 7, ENS Paris, ENS Cachan and École Polytechnique, 30 hours.

Introduction to cryptography Daniel Augot is giving exercise sessions on this subject at the École Polytechnique.

Theoretical Computer Science and *Information Theory* Nicolas Sendrier is "professeur chargé de cours" in Computer Science at École Polytechnique Palaiseau. He is teaching 80-100 hours.

Error-correcting codes Jean-Pierre Tillich is teaching at the Institut Supérieur d'Électronique de Paris (ISEP), 3rd year of engineering school, 10 hours.

Quantum codes Jean-Pierre Tillich is teaching in Master 2, ENST Paris, 6 hours, since 2006.

Most of the Ph.D. students in the team are associated either with the doctoral program of the University Pierre and Marie Curie (Paris 6) or with the doctoral program of École Polytechnique Palaiseau.

8.2. Ph.D. committees

January the 25th P. Loidreau, *Métrique rang et cryptographie*, Université Paris VI, committee : N. Sendrier.

April the 6th B. Sakkour, *Étude et amélioration du décodage des codes de Reed-Muller d'ordre deux*, Ecole Polytechnique, committee : P. Charpin (co-director).

April the 24th R. Overbeck, *Public key cryptography based on coding theory*, TU Darmstadt, committee : N. Sendrier (reviewer).

May the 11th V. Nesme, *Complexité en requêtes et symétries*, Ecole Normale Supérieure de Lyon, committee : J.P. Tillich.

June the 15th L. Minder, *Cryptography based on error correcting codes*, EPFL Lausanne, committee : A. Canteaut (reviewer), N. Sendrier (reviewer).

June the 22nd C. Lauradoux, *Conception et synthèse en cryptographie symétrique*, Ecole Polytechnique, committee : A. Canteaut, N. Sendrier (director).

June the 22nd A. Brown, *Codes, graphs and and graph based codes*, EPFL Lausanne, committee : D. Augot.

July the 6th O. Hamdi, *Analyse des nouvelles structures cryptographiques utilisant les codes chaînés*, Ecole Nationale d'ingénieurs de Tunis, committee : J.P. Tillich (reviewer).

July the 18th J.C. Faugère, Calcul efficace des bases de Gröbner et applications, Habilitation à diriger de Recherches, Université Paris VI, committee : P. Charpin (reviewer).

December the 18th F. Didier, *Codes de Reed-Muller et cryptanalyse du registre filtré*, Ecole Polytechnique, committee : A, Canteaut, J.P. Tillich (director).

8.3. Participation to workshops/conferences in 2007

January the 22nd-24th Journée d'Arithmétique de l'Informatique, Montpellier, participant : Cédric LAURADOUX .

January the 30th-February the 2nd SASC 2007, Bochum, Allemagne, participants : Anne CANTEAUT, Yann LAIGLE-CHAPUY, Cédric LAURADOUX, Maria NAYA PLASENCIA, Andrea ROECK.

March the 25th-28th FSE, Luxembourg, participants : Anne CANTEAUT, Pascale CHARPIN, Maria NAYA PLASENCIA.

April the 29th-May the 5th ECRYPT PhD SUMMER SCHOOL SAMOS, Greece, participants : Bhaskar BISWAS, Anne CANTEAUT, Christophe CHABOT, Frédéric DIDIER, Stéphane MANUEL, Maria NAYA PLASENCIA, Andrea ROECK, Nicolas SENDRIER.

May the 2nd-4th NTMS, News Technologies Mobility Security, Caen, participant : Daniel AUGOT.

May the 2nd-3rd Workshop on Boolean Functions, Paris, participant : Deepak DALAI.

May the 20th-23rd The Claude Shannon Workshop on Coding Theory, Cork, Irland, participant : Daniel AUGOT.

May the 24th-25th ECRYPT Hash Workshop 2007, Barcelone, Espagne, participants : Stéphane MANUEL, Nicolas SENDRIER.

May the 30th-June the 1st SSTIC 2007, Rennes, participant : Stéphane MANUEL.

June the 24th-29th ISIT, Nice, participants : Daniel AUGOT, Thomas CAMARA, Pascale CHARPIN, Christophe CHABOT, Frédéric DIDIER, Yann LAIGLE-CHAPUY, Cédric LAURADOUX, Nicolas SENDRIER, Jean-Pierre TILLICH.

July the 3rd-7th WEWORC, Bochum, Allemagne,participants : Benoit GERARD, Stéphane MANUEL, Maria NAYA PLASENCIA, Andrea ROECK.

August 16th-17th SAC Ottawa, participant : Cédric LAURADOUX.

August the 18th-24th CRYPTO 2007, Santa Barbara, USA, participants : Cédric LAURADOUX, Stéphane MANUEL, Nicolas SENDRIER.

October the 28th-31st MAJECSTIC, Caen, participants : Maria NAYA PLASENCIA, Andrea ROECK.

November 9th , KRYPTOTAG, Bonn, Allemagne, participant : Andrea ROECK.

December the 2nd-8th Workshop on Coding Theory, Oberwolfach, participants (invited) : Daniel AUGOT, Jean-Pierre TILLICH.

December the 9th-13th , INDOCRYPT, Chennai, Inde, participant : Frédéric DIDIER.

December the 16th-20th , AAECC-17, Bangalore, Inde, participants : Daniel AUGOT, Yann LAIGLE-CHAPUY.

8.4. Visiting researchers

Rachit AGARWAL Dept. of Microelectronic Engineering, University College of Cork, IRELAND, 15/03-16/03/07,

Pr. Guang GONG Dept. of Electrical and Computer Engineering, University of Waterloo, Ontario, CANADA, 07/06-07/08/07,

Pr. Kathy HORADAM Dept. Mathematics and Statistics, RMIT City Campus, Melbourne, AUSTRALIA, 12/04-13/05/07,

Pr. Grigory KABATIANSKIY Institute for Problems of Information Transmission, RAS, Moscow, RUSSIA, 21/01-27/01/07, 04/03-11/03/07, 24/03-28/04/07,

Pr. Gohar KYUREGHYAN University of Magdeburg, GERMANY, 14/10-27/10/07,

Raphael OVERBECK Technische Universität Darmstadt, GERMANY, 31/07-04/08/07,

Christian RECHBERGER Institute for Applied Information Processing and Communications, TU Graz, AUSTRIA, 13/06-19/06/07,

Pr. Bimal ROY Indian Statistical Institute, Kolkata, INDIA, 10/01-12/01/07,

Pr. Victor ZINOVIEV Institute for Problems of Information Transmission, RAS, Moscow, RUSSIA, 15/04-15/05/07.

8.5. Visit to other laboratories

October CSIC (Centro superior de investigaciones cientificas), Madrid, Maria Naya Plasencia.

November 18th-24th University of Bergen, Norway, Pascale Charpin (invited).

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", E. BIHAM (editor), Lecture Notes in Computer Science, n^{o} 2656, Springer-Verlag, 2003, p. 229-240.

[2] D. AUGOT, L. PECQUET. *A Hensel Lifting to Replace Factorization in List-Decoding of Algebraic-Geometric and Reed-Solomon Codes*, in "IEEE Transactions on Information Theory", vol. 46, n^{o} 7, November 2000, p. 2605-2614.

[3] A. CANTEAUT, P. CHARPIN, H. DOBBERTIN. *Binary m-sequences with three-valued crosscorrelation: A proof of Welch conjecture*, in "IEEE Transactions on Information Theory", Regular paper, vol. 46, n^{o} 1, January 2000, p. 4–8.

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

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

[6] 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.

[7] 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.

[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

Doctoral dissertations and Habilitation theses

[11] D. AUGOT. *Décodage des codes algébriques et cryptographie*, Mémoire d'habilitation à diriger des recherches, Université Paris 6, June 2007.

[12] F. DIDIER. *Codes de Reed-Muller et cryptanalyse du registre filtré*, Ph. D. Thesis, École Polytechnique, December 2007.

[13] C. LAURADOUX. *Conception et synthèse en cryptographie symétrique*, Ph. D. Thesis, École Polytechnique, Palaiseau, Juin 2007.

[14] P. LOIDREAU. *Métrique rang et cryptographie*, Mémoire d'habilitation à diriger des recherches, Université Paris 6, January 2007.

[15] B. SAKKOUR. *Étude et amélioration du décodage des codes de Reed-Muller d'ordre deux*, Ph. D. Thesis, École Polytechnique, Palaiseau, avr 2007.

Articles in refereed journals and book chapters

[16] D. AUGOT, R. BHASKAR, V. ISSARNY, D. SACCHETTI. *A Three Round Authenticated Group Key Agreement Protocol for Ad hoc Networks*, in "Pervasive and Mobile Computing", vol. 3, n^{o} 1, 2007, p. 36-52, http://www.sciencedirect.com/science/article/B7MF1-4KTVPCX-1/2/69e95fcd91a4ec5a8dc05ed06301def5.

[17] A. CANTEAUT, P. CHARPIN, G. KYUREGHYAN. *A new class of monomial bent functions*, in "Finite Fields and Their Applications", In press, 2007.

[18] C. CARLET, C. DING. *Nonlinearities of S-boxes*, in "Finite Fields and Their Applications", vol. 13, n^{o} 1, January 2007, p. 121-135.

[19] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *Propagation characteristics of $x \mapsto 1/x$ and Kloosterman sums*, in "Finite Fields and Their Applications", vol. 13, n^{o} 2, 2007, p. 366–381.

[20] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *The divisibility modulo 24 of Kloosterman sums on GF(2^m), m odd*, in "Journal of Combinatorial Theory, Series A", vol. 114, n^{o} 2, 2007, p. 322–338.

[21] P. CHARPIN, G. KYUREGHYAN. *Cubic monomial bent functions: a subclass of $\mathcal{M}$*, in "SIAM Journal of Discrete Math.", In press, 2007.

[22] M. CLUZEAU. *Reconstruction of a Linear Scrambler*, in "IEEE Transactions on Computers", vol. 56, n^{o} 9, Septembre 2007, p. 1283-1291.

[23] Y. LAIGLE-CHAPUY. *Permutation Polynomials and applications to coding theory*, in "Finite Fields and Their Applications", vol. 13, n^{o} 1, 2007, p. 58–70.

Publications in Conferences and Workshops

[24] I. ANDRIYANOVA, J. TILLICH. *A family of non-binary TLDPC codes: density evolution, convergence and thresholds*, in "IEEE Conference, ISIT'07, Nice, France", June 2007, p. 1216-1220.

[25] F. ARNAULT, T. BERGER, C. LAURADOUX, M. MINIER. *X-FCSR: a new software oriented stream cipher based upon FCSRs*, in "INDOCRYPT 2007", LNCS, To appear, Springer-Verlag, 2007.

[26] D. AUGOT. *On the Newton's identities for decoding cyclic codes with Grobner basis*, in "The Claude Shannon workshop on Coding and Cryptography, Cork, Ireland", Invited talk, May 2007, http://www.bcri.ucc.ie/workshops.html.

[27] D. AUGOT, M. BARDET, J. FAUGÈRE. *On formulas for decoding binary cyclic codes*, in "IEEE Conference, ISIT'07, Nice, France", June 2007, p. 2646-2650.

[28] F. BANAT-BERGER, A. CANTEAUT. *Intégrité, signature et processus d'archivage*, in "La Sécurité aujourd'hui dans la société de l'information", S. LACOUR (editor), L'Harmattan, 2007, p. 213–235.

[29] T. CAMARA, H. OLLIVIER, J. TILLICH. *A class of quantum LDPC codes: construction and performances under iterative decoding*, in "IEEE Conference, ISIT'07, Nice, France", June 2007, p. 811-815.

[30] A. CANTEAUT. *Boolean Functions for cryptography*, in "ECRYPT PhD SUMMER SCHOOL, Emerging Topics in Cryptographic Design and Cryptanalysis,, Samos, Greece", Invited talk, April 30 -May 4 2007, http://ecrypt-ss07.rhul.ac.uk/sstt.htm.

[31] C. CHABOT. *Recognition of a code in a noisy environment*, in "IEEE Conference, ISIT'07, Nice, France", jun 2007, p. 2211-2215.

[32] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *On binary primitive BCH codes with minimum distance 8 and exponential sums*, in "IEEE Conference, ISIT'07, Nice, France", June 2007, p. 1976-1980.

[33] D. DALAI, S. MAITRA. *Balanced Boolean functions with (more than) maximum algebraic immunity*, in "Proceedings of the Workshop on Coding and Cryptography, WCC 07, Versailles, France", April 2007, p. 99-106.

[34] F. DIDIER. *Attacking the filter generator by finding zero inputs of the filtering function*, in "INDOCRYPT 2007", LNCS, To appear, Springer-Verlag, dec 2007.

[35] F. DIDIER, Y. LAIGLE-CHAPUY. *Finding low-weight polynomila multiples using discrete logarithms*, in "IEEE Conference, ISIT'07, Nice, France", June 2007, p. 1036-1040.

[36] M. FINIASZ, P. GABORIT, N. SENDRIER. *Improved fast syndrome based cryptographic hash function*, in "ECRYPT Hash Workshop 2007, Barcelona, Spain", May 2007.

[37] P. GABORIT, C. LAURADOUX, N. SENDRIER. *SYND: a Very Fast Code-Based Cipher Stream with a Security Reduction*, in "IEEE Conference, ISIT'07, Nice, France", June 2007, p. 186-190.

[38] Y. LAIGLE-CHAPUY. *A note on a class of quadratic permutations over F_{2^n}*, in "AAECC 17", LNCS, To appear, Springer-Verlag, 2007.

[39] C. LAURADOUX. *From Hardware to Software Synthesis of Linear Feedback Shift Registers*, in "Proceedings of Workshop on Performance Optimization for High-Level Languages and Libraries - POHLL POHLL 2007 -, Long Beach, USA", March 2007.

[40] C. LAURADOUX. *Throughput/code size tradeoff for stream ciphers*, in "Proceedings of SASC 2007 - ECRYPT Workshop on stream ciphers, Bochum, Germany", January 2007, http://www.ecrypt.eu.org/stream/.

[41] S. MAITRA, S. SARKAR, D. DALAI. *On Dihedral Group Invariant Boolean Functions*, in "Workshop on Boolean Functions :Cryptography and Applications, (BFCA07), Paris, France", May 2007.

[42] S. MANUEL, N. SENDRIER. *XOR-Hash : A Hash Function Based on XOR*, in "WEWoRC 2007, Bochum, Germany", July 2007.

[43] M. NAYA-PLASENCIA. *Cryptanalyse de Achterbahn-128/80 avec une nouvelle limitation de suite chiffrante*, in "MajecSTIC 2007, Caen,France", October 2007.

[44] M. NAYA-PLASENCIA. *Cryptanalysis of Achterbahn-128/80*, in "Proceedings of SASC 2007 - ECRYPT Workshop on stream ciphers, Bochum, Germany", January 2007, http://www.ecrypt.eu.org/stream/.

[45] M. NAYA-PLASENCIA. *Cryptanalysis of Achterbahn-128/80*, in "FSE 2007", LNCS, n^{o} 4593, Springer-Verlag, 2007, p. 73-86.

[46] M. NAYA-PLASENCIA. *Cryptanalysis of Achterbahn-128/80 with a new Keystream Limitation*, in "WEWoRC 2007, Bochum, Germany", July 2007.

[47] A. OTMANI, J. TILLICH, I. ANDRIYANOVA. *On the Minimum Distance of Generalized LDPC Codes*, in "IEEE Conference, ISIT'07, Nice, France", June 2007, p. 751-755.

[48] A. RÖCK. *Attaques par collision basés sur la perte d'entropie causée par des fonctions aléatoires*, July 2007.

[49] A. RÖCK. *The Impact of Entropy Loss Caused by Random Functions*, in "MajecSTIC 2007, Caen,France", October 2007.

[50] N. SENDRIER. *Codes based One-way functions*, in "ECRYPT PhD SUMMER SCHOOL, Emerging Topics in Cryptographic Design and Cryptanalysis,, Samos, Greece", Invited talk, April 30 -May 4 2007, http://ecrypt-ss07.rhul.ac.uk/sstt.htm.

Miscellaneous

[51] S. BABBAGE, C. DE CANNIÈRE, A. CANTEAUT, C. CID, H. GILBERT, T. JOHANSSON, C. PAAR, M. PARKER, B. PRENEEL, V. RIJMEN, M. ROBSHAW, H. WU. *eSTREAM - Short Report on the End of the Second Phase*, March 2007, http://www.ecrypt.eu.org/stream/PhaseIIreport.pdf, Rapport du réseau d'excellence européen ECRYPT.

[52] A. CANTEAUT, F. DIDIER, Y. LAIGLE-CHAPUY, J. TILLICH. *Contrat de recherche 06.42.113: veille technologique dans le domaine du décodage itératif*, 49 pages, nov 2007, Rapport final du contrat CELAR 06.42.113.

[53] A. CANTEAUT, D. AUGOT, C. CID, H. ENGLUND, H. GILBERT, M. HELL, T. JOHANSSON, M. PARKER, T. PORNIN, B. PRENEEL, M. ROBSHAW. *D.STVL.5 – Ongoing Research Areas in Symmetric Cryptography*, 93 pages, March 2007, Rapport du réseau d'excellence européen ECRYPT.

[54] F. GITON. *Etude de l'algorithme cyclotomique de transformée de Fourier de Sidorenko*, Direction : D. Augot, Rapport de stage de Master Cryptographie-Codage, Université de Limoges, September 2007.

[55] B. GÉRARD. *Utilisation de techniques de codage correcteur d'erreurs pour la cryptanalyse de systèmes de chiffrement à clé secrète,*, Direction : J.P. Tillich, Rapport de stage de Master Algèbre appliquée, Université de Versailles-St Quentin, Avril-Juin 2007.

[56] I. B. SLIMEN. *Les problèmes de réconciliation dans les protocoles quantiques d'échange de clés*, Direction : J.P. Tillich, Rapport de stage de l'ENIT, Université de Cergy Pontoise, Mai 2007.

References in notes

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

[58] 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.

[59] M. BARDET. *Etude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*, Thèse de doctorat, Université Paris 6, December 2004.

[60] 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. DECIMV2, in "Proceedings of SASC 2006 - ECRYPT Workshop on stream ciphers, Leuven, Belgique", February 2006, p. 293-301, http://www.ecrypt.eu.org/stream/.

[61] 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.

[62] 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.

[63] N. SENDRIER. *On the security of the McEliece public-key cryptosystem*, in "Information, Coding and Mathematics", M. BLAUM, P. FARRELL, H. VAN TILBORG (editors), In honor of Bob McEliece on his 60th birthday. Invited paper, Kluwer, 2002, p. 141–163.

[64] N. SENDRIER. *Encoding information into constant weight words*, in "ISIT 2005, Proceedings, Adelaide, Australie", IEEE Press, September 2005, p. 435-438.

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