INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Codes

Codage et cryptographie

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]

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
Claude Carlet [Professor (PR) University of Paris 8, HdR]
Guy Chassé [Professor (PR) École des Mines de Nantes]
Matthieu Finiasz [Post-doc EPFL, Lausanne, Switzerland]
Philippe Gaborit [Assistant Professor (MC) University of Limoges, HdR]
Grigory Kabatiansky [Senior Researcher IPIT, Academy of Sciences of Moscow, Russia]
Françoise Levy-dit-Vehel [Assistant Professor (MC) ENSTA, Paris]
Pierre Loidreau [Assistant Professor (MC) ENSTA, Paris]
Harold Ollivier [Department of Finance]
Ayoub Otmani [Assistant Professor (PR), University of Caen]

Research engineer
Fabien Galand [Research Engineer (IE) Inria]

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

Ph.D. students
Raghav Bhaskar [EGIDE grant]
Thomas Camara [MESR grant]
Christophe Chabot [DGA grant]
Mathieu Cluzeau [DGA grant]
Maxime Cote [CIFRE grant]
Frédéric Didier [AMN grant]
Cédric Faure [AMN 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]

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.

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/.

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, Claude Carlet, Pascale Charpin, Frédéric Didier, Yann Laigle-Chapuy, 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. We have investigated the recent algebraic attacks, which are an important breakthrough especially in the cryptanalysis of stream ciphers based on linear feedback shift registers. We have proposed new algorithms for computing the algebraic immunity of a function [42], [19], [41]. These algorithms have complexity which ranges from linear to quadratic in the annihilator space dimension (depending on the parameters of the algebraic attack) and are the best known to perform such a task. We have also shown the existence of functions with a high algebraic immunity and have provided some constructions for them in [38].

A last type of attacks investigated in the project are the cache attacks which exploit the power consumption or the timing variations induced by the memory accesses to lookup tables, especially to S-boxes, during the encryption process [60], [59].
Publications : [36], [42], [19], [41], [38], [60], [59], [30]

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 [37], [39]. We have also been interested in APN functions, which are the S-boxes ensuring an optimal resistance to differential cryptanalysis. An important open problem is to find APN permutations depending on an even number of variables. In this context, we have proved that some families of functions do not contain any APN mapping [16].
Publications : [16], [25], [18], [20], [19], [37], [39], [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 [33]. SOSEMANUK is one of the fastest and most secure ciphers among the 22 eSTREAM candidates dedicated to software applications (the first evaluation phase of eSTREAM put it in the "focus cipher" category). DECIM and F-FCSR are hardware-oriented cipher for low-resource environments and have been selected for the next evaluation phase.
Publications : [33]

5.2. Code-based cryptography

Participants: Daniel Augot, Raghav Bhaskar, Cédric Faure, Matthieu Finiasz, Pierre Loidreau, 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 [78], [77] 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 [74]. 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 [79] 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).
Publications : [51], [55], [54]

5.2.2. Cryptosystems based on decoding the rank metric.

This family of cryptosystems is roughly based on the same principle as the McEliece cryptosystem, except that the metric in use is the rank metric [76]. This allows taking public-keys of a much smaller size than for McEliece cryptosystem, typically between ten and twenty times smaller.

Pierre Loidreau and Thierry Berger have been working on new variants of this system [71], [72] which also considered the possibility of achieving non-malleability. Pierre Loidreau also designed the first decoding algorithm of Gabidulin's codes in quadratic time (previous ones were cubic) [50]. Finally, he designed and studied with Cédric Faure [45] a rank metric equivalent of Augot/Finiasz PR based encryption scheme (see next subsubsection).
Publications : [50], [45], [44], [52]

5.2.3. Cryptographic hardness of Reed-Solomon decoding.

The Polynomial Reconstruction problem (PR) considered by Naor and Pinkas 1999 then Kiayias and Yung in 2002 states that decoding more than a certain number of errors in a Reed-Solomon code is difficult. Daniel Augot and Matthieu Finiasz have designed an encryption scheme based on this problem [1]. This system possesses the efficiency of code-based systems and enjoys a much shorter public key. Unfortunately, as pointed out by Coron [73], if the message security reduces to a difficult problem, the key security was not good enough.

Interestingly, though it was broken, this cryptosystem raised a lot of interest. The new cryptographic function that was exhibited did not allow the design of an encryption scheme, because the trapdoor (for decryption) could not be securely concealed. However, diversity is among the important concerns of cryptographic research. Proposing new primitives, with different features, might be of interest for future needs.
Publications : [31]

5.2.4. Other cryptographic functionalities with codes.

We have proposed a new collision resistant hash-function based on the problem of decoding general binary linear codes [69]. 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.

5.2.5. Group key agreement for Ad Hoc networks

We have proposed a new protocol for enabling participants to share a common secret key, which is later used with symmetric cryptography (authentication, encryption). This protocol has the desirable property of being resilient to connectivity losses, a property which makes it suitable for Ad Hoc networks.

We have also suggested a new authentication procedure for the service messages in reactive routing protocols. Our procedure enables to aggregate these authentication codes of routing messages in a single, fixed size, message.
Publications : [15], [58], [17], [34]

5.3. Decoding techniques, algebraic systems solving and applications

Participants: Daniel Augot, Thomas Camara, Christophe Chabot, Mathieu Cluzeau, Maxime Cote, Frédéric Didier, Harold Ollivier, 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 [80], 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. On the other hand, Frédéric Didier and Jean-Pierre Tillich have focused on decoding Reed-Muller codes efficiently on the erasure channel. They have proposed various decoding algorithms whose complexity is sometimes linear and in general at most quadratic in the code dimension. These algorithms have been implemented, have lead to several decoding records and can be used to determine the algebraic immunity of Boolean functions against algebraic attacks [24], [41], [42].
Publications : [24], [41], [42], [32]

5.3.2. Solving algebraic systems and applications.

From the algebraic systems point of view, SALSA, in collaboration with CODES, performed the cryptanalysis of the HFE cryptosystems (Hidden Field Equations), performed by Faugère by a computation of a few days [75]. It was followed by the thesis of Magali Bardet [70] which covers theoretical aspects of the HFE cryptanalysis (why it was feasible), and also the decoding of 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 [68], [70].

5.3.3. Coding theory

Concerning the part of our work devoted to error-correcting codes, we have focused on codes which have 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 [29]. 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 [28].

Finally, another important result related to decoding, the coset distribution of some BCH codes, was proven by Charpin, Helleseth and Zinoviev [21]. It answered to an old research problem formulated in the 70s.
Publications : [29], [28], [21], [56]

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). blabla
Publications : [40], [14], [23]

6. Contracts and Grants with Industry

6.1. Industrial contracts

FT R&D $(02/06 \rightarrow 01/08)$ 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

ACI RQ $(07/03 \rightarrow 07/06)$ One of the goals of this project is to propose quantum codes for protecting quantum information against external noise. It has lead us to find quantum analogues for LDPC codes, convolutional codes and serial turbo-codes.

Partners: Université Paris XI.

ACI UNIHAVEGE $(11/03 \rightarrow 11/06)$ The goal of UNIHAVEGE was to test and extend the random number generator HAVEGE (Hardware Volatile Entropy Gathering and Expansion) designed by Andre Seznec and Nicolas Sendrier. During the last three years, no weaknesses were found. HAVEGE has been integrated to Linux Kernel through a module

Partner: IRISA team CAPS (Andre Seznec and Olivier Rochecouste)

ACI OCAM $(07/03 \rightarrow 12/06)$ The primary goal of the project is to produce an FPGA implementation of a digital signature algorithm based on coding theory. This algorithm produces the shortest known signature but is very slow in software. Additional goals are to consider other code-based cryptosystems and their hardware implementation, with a particular focus on finite fields arithmetic.

Partners: ARENAIRE project-team, LIRMM (Montpellier).

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.

RNRT X-CRYPT $(12/03 \rightarrow 12/06)$ The aim is to conceive cryptographic tools crafted to high speed networks and also wireless networks, which both have high security and consume few resources. Two stream ciphers have been developed: SOSEMANUK and DECIM.

Partners: Axalto, ENS Ulm, France Telecom, Cryptolog International, Université de Versailles, INRIA.

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 a working group 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.

IEEE Transactions on Information Theory associate editors: Anne Canteaut for *Cryptography and Complexity* 2005-2008.

Designs, Codes and Cryptography associate editor: Pascale Charpin, since 2003.

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 2006

ISIT IEEE International Symposium on Information Theory) G. Kabatianski;

FSE Fast Software Encryption, A. Canteaut;

Indocrypt A. Canteaut, C. Carlet, N. Sendrier;

SETA International conference on sequences and their applications, A. Canteaut, C. Carlet;

ACCT International Workshop on Algebraic and Combinatorial Coding Theory, G. Kabatianski, program chair;

ICETE International Joint Conference on E-business and Telecommunications, P. Charpin;

YACC Yet Another Conference on Cryptography, C. Carlet;

SASC State of the Art in Stream ciphers, eSTREAM workshop, A. Canteaut, program chair;

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 will be held at INRIA in 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);

SetIn Scientific committee of the national research program SetIn (Security and Computer Science) of the National Agency for Research (ANR): 2006 (A. Canteaut);

GDR *Computer Science - Mathematics* (IM): Claude Carlet is in charge of the group *Coding and Cryptography*;

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

"Commission de spécialistes" (Committees for the selection of professors and assistant professors): University Paris 8 (C. Carlet, J-P. Tillich), University of Limoges (A. Canteaut, P. Charpin, C. Carlet), École Normale Supérieure Paris (J-P. Tillich);

CR2 Pascale Charpin was a member of the committee for the selection of CR2 at INRIA-Rocquencourt (2006);

"Comité de Suivi Doctoral" Anne Canteaut is a member of the "Comité de Suivi Doctoral" of INRIA-Rocquencourt since 2004.

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/.

8. Dissemination

8.1. Teaching

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 teaching in Master Recherche 2 "Science Informatique", University of Marne-la-Vallée, 9 hours.

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

March the 8th An Braeken, *Cryptographic properties of Boolean functions and S-boxes*, University of Leuven, Belgium, committee : A. Canteaut (reviewer).

April the 13th Yi Lu, *Applied stream ciphers in mobile communications.*, EPFL, Switzerland, committee : A. Canteaut (reviewer).

June the 26th R. Bhaskar, *Cryptographic protocols for mobile ad hoc networks*, École Polytechnique, committee : D. Augot.

June the 29th V. Bénony, *Étude et conception de systèmes de chiffrement à flot dans le contexte d'architectures matérielles fortement contraintes*, Université de Lille, committee : N. Sendrier (reviewer).

September the 15th A. Canteaut, *Analyse et conception de chiffrements à clé secrète*, Université Paris VI, committee : C. Carlet, P. Charpin.

November the 28th Mathieu Cluzeau, *Reconnaissance d'un schéma de codage*, École Polytechnique, committee : A. Canteau (co-director), N. Sendrier (director), J.P. Tillich.

December the 15th Iryna Andryanova, *Etude d'une certaine construction de codes définis par des graphes: les codes TLDPC*, École Nationale Supérieure des Télécommunications, committee : J.P. Tillich.

8.3. Participation to workshops/conferences in 2006

February the 1st-3rd SASC 2006, Leuven, Belgique, Anne CANTEAUT, Fabien GALAND, Cédric LAURADOUX, Andrea ROECK, Bassem SAKKOUR.

March the 14th-18th FSE, Graz, Anne CANTEAUT, Pascale CHARPIN, Frédéric DIDIER, Andrea ROECK, Jean-Pierre TILLICH.

April the 30th- May 5th Special semester on Groebner bases and related methods, Linz, Daniel AUGOT, Frédéric DIDIER, Yann LAIGLE-CHAPUY.

May the 21st-24th Workshop on Coding and Cryptography, Cork, Irland,Daniel AUGOT.

May the 23rd-26th Post Quantum Cryptography, Leuven Belgique, Nicolas SENDRIER.

May the 27th-June the 1st EUROCRYPT, St Petersbourg, Claude CARLET .

May the 30th-June the 2nd SSTIC Conference, Rennes, Cédric LAURADOUX.

June the 10th-15th ICC Conference, Istambul, Jean-Pierre TILLICH.

June the 11th-15th Summer school, Louvain la Neuve, Cédric LAURADOUX.

June the 18th-23rd YACC'2006, Porquerolles, Françoise LEVY-DIT-VEHEL, Nicolas SENDRIER.

July the 8th-15th ISIT, USA, Anne CANTEAUT, Pascale CHARPIN, Mathieu CLUZEAU, Fabien GALAND, Jean-Pierre TILLICH.

September the 2nd-9th ACCT 10, Zvenigorod, Russie, Daniel AUGOT, Pascale CHARPIN, Cédric FAURE, Pierre LOIDREAU.

September the 24th-27th CLC 2006, Darmstadt, Allemagne, Daniel AUGOT, Andrea ROECK.

October the 15th-20th Journées C2, Eymoutiers, Daniel AUGOT, Anne CANTEAUT, Pascale CHARPIN, Mathieu CLUZEAU, Frédéric DIDIER, Cédric FAURE, Yann LAIGLE-CHAPUY, Cédric LAURADOUX, Maria NAYA PLASENCIA, Andrea ROECK.

November the 16th-17th ECRYPT meeting, Graz, Autriche, Anne CANTEAUT.

November the 22nd-24th Paristic meeting, Nancy, Anne CANTEAUT, Cédric LAURADOUX, Nicolas SENDRIER, Jean-Pierre TILLICH.

December the 7th-9th Coding meeting, Zurich, Daniel AUGOT, Françoise LEVY-DIT-VEHEL.

December the 8th-15th INDOCRYPT, Calcutta, Frédéric DIDIER, Nicolas SENDRIER.

8.4. Visiting researchers

Grigory KABATIANSKIY 13-23/12/06, 24/09-07/10/06, 09-22/04/06.

Matthew PARKER 27/11-01/12/06.

Raghav BHASKAR 17-29/11/06.

Thomas JOHANSSON 14-16/09/06.

Tor HELLESETH 14-18/09/06.

Serge VAUDENAY 13-18/09/06.

Raphael OVERBECK 01/08-15/12/06 (internship).

Markku-Juhani O. SAARINEN 05-15/06/06.

Sourav MUKHOPADHYAY 03-30/04/06.

Sumanta SARKAR 17-24/03/06.

Gohar KYUREGHYAN 15-20/01/06.

Bimal ROY 13-14/01/06.

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

Books and Monographs

[11] P. CHARPIN, G. KABATIANSKY (editors). *Discrete Applied Mathematics*, Special issue on Coding and Cryptography, vol. 154 (2), Elsevier, 2006.

Doctoral dissertations and Habilitation theses

[12] R. BHASKAR. *Protocoles Cryptographiques pour les réseaux Ad hoc*, Thèse de doctorat, École Polytechnique, June 2006.

[13] A. CANTEAUT. *Analyse et conception de chiffrements à clef secrète*, Mémoire d'habilitation à diriger des recherches, Université Paris 6, September 2006.

[14] M. CLUZEAU. *Reconnaissance d'un schéma de codage*, Thèse de doctorat, Ecole Polytechnique, nov 2006.

Articles in refereed journals and book chapters

[15] D. AUGOT, R. BHASKAR, V. ISSARNY, D. SACCHETTI. *A three round authenticated group key agreement protocol for adhoc networks*, in "Pervasive and Mobile Computing", to appear, vol. 3, n^{o} 1, 2006, p. 36–52, http://www.sciencedirect.com/science/article/B7MF1-4KTVPCX-1/2/69e95fcd91a4ec5a8dc05ed06301def5.

[16] T. BERGER, A. CANTEAUT, P. CHARPIN, Y. LAIGLE-CHAPUY. *On Almost Perfect Nonlinear functions*, in "IEEE Trans. Inform. Theory", vol. 52, n^{o} 9, September 2006, p. 4160-4170.

[17] R. BHASKAR, J. HERRANZ, F. LAGUILLAUMIE. *Aggregate Designated Verifier Signatures and Application to Secure Routing*, in "International Journal of Security and Networks", to appear, 2006.

[18] A. CANTEAUT, M. DAUM, G. LEANDER, H. DOBBERTIN. *Normal and non normal bent functions*, in "Discrete Applied Mathematics", Special issue in Coding and Cryptology, vol. 154, n^{o} 2, February 2006, p. 202-218.

[19] C. CARLET, D. DALAI, K. GUPTA, S. MAITRA. *Algebraic immunity for cryptographically significant Boolean functions: analysis and construction*, in "IEEE Transactions on Information Theory", vol. 52, n^{o} 7, July 2006, p. 3105- 3121.

[20] C. CARLET, C. DING. *Nonlinearities of S-boxes*, in "Finite Fields and Their Applications", In press, 2006.

[21] 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.

[22] 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", In press, 2006.

[23] M. CLUZEAU. *Reconstruction of a Linear Scrambler*, in "IEEE Transactions on Computers", to appear, 2006.

[24] F. DIDIER. *A new bound on the block error probability after decoding over the erasure channel*, in "IEEE Transactions on Information Theory", vol. 52, n^{o} 10, October 2006, p. 4496-4503.

[25] H. DOBBERTIN, G. LEANDER, A. CANTEAUT, C. CARLET, P. FELKE, P. GABORIT. *Construction of bent functions via Niho power functions*, in "Journal of Combinatorial Theory, Series A", vol. 113, n^{o} 5, July 2006, p. 779-798.

[26] J. FRIEDMAN, R. MURTY, J. TILLICH. *Spectral estimates for Abelian Cayley graphs*, in "Journal of Combinatorial Theory Ser.B", vol. 96, n^{o} 1, 2006, p. 111–121.

[27] F. LEVY-DIT-VEHEL. *Encyclopédie des systèmes d'information*, In press, chap. Cryptographie, C. Kichner editeur,Editions Vuibert, 2006.

[28] H. OLLIVIER, J.-P. TILLICH. *Trellises for stabilizer codes : definition and uses*, in "Phys. Rev. A", vol. 74, n^{o} 3, September 2006.

Publications in Conferences and Workshops

[29] I. ANDRIYANOVA, J.-P. TILLICH, J.-C. CARLACH. *A new family of codes with high iterative decoding performances*, in "ICC 2006, Istambul, Turquie", June 2006.

[30] F. ARMKNECHT, C. CARLET, P. GABORIT, S. KÜNZLI, W. MEIER, O. RUATTA. *Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks*, in "EUROCRYPT 2006", LNCS, n^{o} 4004, Springer-Verlag, 2006, p. 147-164.

[31] D. AUGOT, M. EL-KHAMY, R. MCELIECE, F. PARVARESH, M. STEPANOV, A. VARDY. *Algebraic List Decoding of Reed-Solomon product codes*, in "Proceedings of ACCT'10, Zvenigorod, Russia", September 2006, p. 210-214.

[32] D. AUGOT, M. STEPANOV. *Interpolation based decoding of Reed-Muller codes*, in "Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics, RICAM, University of Linz, Austria", Invited talk, May 2006.

[33] 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, http://www.ecrypt.eu.org/stream/.

[34] R. BHASKAR, J. HERRANZ, F. LAGUILLAUMIE. *Efficient Authentication for Reactive Routing Protocols*, in "Proceedings of Second International Workshop on Security in Networks and Distributed Systems", Vienna, Austria, April 2006.

[35] L. BUDAGHYAN, C. CARLET, P. FELKE, G. LEANDER. *An infinite class of quadratic APN functions which are not equivalent to power mappings*, in "ISIT 2006, Proceedings, Seattle, USA", IEEE Press, July 2006, p. 2637-2641.

[36] A. CANTEAUT. *Open problems related to algebraic attacks on stream ciphers*, in "Coding and Cryptography - WCC 2005 - Revised selected papers", O. YTREHUS (editor). , LNCS, Invited paper, vol. 3969, Springer-Verlag, 2006, p. 120-134.

[37] A. CANTEAUT, P. CHARPIN, G. KYUREGHYAN. *A new class of monomial bent functions*, in "Proceedings of the 2006 IEEE International Symposium on Information Theory - ISIT, Seattle, USA", IEEE Press, July 2006.

[38] C. CARLET. *On bent and highly nonlinear balanced-resilient functions and their algebraic immunities*, in "AAECC 16,, Las Vegas, USA", Invited talk, February 2006.

[39] P. CHARPIN, G. KYUREGHYAN. *On cubic bent functions in the class* $\mathcal{M}$, in "Proceedings of ACCT'10, Zvenigorod, Russia", September 2006, p. 52-56.

[40] M. CLUZEAU. *Block code reconstruction using iterative decoding techniques*, in "Proceedings of the 2006 IEEE International Symposium on Information Theory - ISIT, Seattle, USA", IEEE Press, July 2006.

[41] F. DIDIER. *Using Wiedemann's algorithm to compute the immunity against algebraic and fast algebraic attacks*, in "INDOCRYPT 2006, Proceedings, Kolkata, India", to appear, Springer Verlag, December 2006.

[42] F. DIDIER, J.-P. TILLICH. *Computing the algebraic immunity efficiently*, in "FSE 2006", LNCS, To appear, Springer-Verlag, 2006.

[43] I. DUMER, G. KABATIANSKY, C. TAVERNIER. *List decoding of second order Reed-Muller codes up to the Johnson bound with almost linear complexity*, in "Proceedings of the 2006 IEEE International Symposium on Information Theory - ISIT, Seattle, USA", IEEE Press, July 2006, p. pp. 138-142.

[44] C. FAURE. *Average number of Gabidulin codewords within a sphere*, in "Proceedings of ACCT'10, Zvenigorod, Russia", September 2006, p. 86-90.

[45] C. FAURE, P. LOIDREAU. *A new public-key cryptosystem based on the problem of reconstruction of p-polynomials*, in "Coding and Cryptography - WCC 2005 - Revised selected papers", O. YTREHUS (editor). , LNCS, vol. 3969, Springer-Verlag, 2006, p. 304-315.

[46] M. FINIASZ. *Syndrome decoding in the non-standard cases*, in "CLC 2006, Darmstadt, Germany", Invited talk, September 2006.

[47] F. GALAND. *Practical Construction Against Theoretical Approach in Fingerprinting*, in "Proceedings of the 2006 IEEE International Symposium on Information Theory - ISIT, Seattle, USA", IEEE Press, July 2006.

[48] G. KABATIANSKY, C. TAVERNIER. *List decoding of second order Reed-Muller codes, second part*, in "Proceedings of ACCT'10, Zvenigorod, Russia", September 2006, p. 131-135.

[49] F. LEVY-DIT-VEHEL, L. PERRET. *On Wagner-Magyarik cryptosystem*, in "Coding and Cryptography - WCC 2005 - Revised selected papers", O. YTREHUS (editor). , LNCS, vol. 3969, Springer-Verlag, 2006, p. 316-329.

[50] P. LOIDREAU. *A Welch-Berlekamp like algorithm for decoding Gabidulin codes*, in "Coding and Cryptography - WCC 2005 - Revised selected papers", O. YTREHUS (editor). , LNCS, vol. 3969, Springer-Verlag, 2006, p. 36-45.

[51] P. LOIDREAU. *How to reduce public-key size in McEliece-like public key cryptosystems*, in "CLC 2006, Darmstadt, Germany", Invited talk, September 2006.

[52] P. LOIDREAU, R. OVERBECK. *Decoding rank errors beyond the error-correcting capacity*, in "Proceedings of ACCT'10, Zvenigorod, Russia", September 2006, p. 186-190.

[53] N. SENDRIER, C. LAURADOUX. *HAVEGE: true random number generator in software*, in "YACC 06, Porquerolles Island, France", Invited talk, June 2006.

[54] N. SENDRIER. *Key security of code-based public key cryptosystem*, in "CLC 2006, Darmstadt, Germany", Invited talk, September 2006.

[55] N. SENDRIER. *Post-quantum code-based cryptography*, in "PQcrypto 2006, Leuven, Belgium", Invited talk, May 2006.

[56] J.-P. TILLICH, G. ZÉMOR. *On the minimum distance of structured LDPC codes with two variable nodes of degree 2 per parity-check equation*, in "ISIT 2006, Proceedings, Seattle, USA", IEEE Press, July 2006, p. 1549–1553.

[57] I. DE LAMBERTERIE, M. VIDEAU. *Regards croisés de juristes et d'informaticiens sur la sécurité informatique*, in "Actes du Symposium sur la Sécurité des Techologies de l'Information et des Communications", Article invité, 2006.

Internal Reports

[58] R. BHASKAR, P. MÜHLETHALER, D. AUGOT, C. ADJIH, S. BOUDJIT. *Efficient and Dynamic Group Key Agreement in Ad Hoc Networks*, Technical report, n° RR-5915, INRIA, 2006, http://hal.inria.fr/inria-00071348.

[59] A. CANTEAUT, C. LAURADOUX, A. SEZNEC. *Understanding cache attacks*, Rapport de recherche, n° RR-5881, INRIA, April 2006, http://hal.inria.fr/inria-00071387.

Miscellaneous

[60] D. AUGOT, A. BIRYUKOV, A. CANTEAUT, C. CID, N. COURTOIS, C. D. CANNIÈRE, H. GILBERT, C. LAURADOUX, M. PARKER, B. PRENEEL, M. ROBSHAW, Y. SEURIN. *D.STVL.2 – AES Security Report*, 73 pages, 2006, Rapport du réseau d'excellence européen ECRYPT.

[61] A. CANTEAUT. *Parcours et fiches sur les générateurs pseudo-aléatoires et le chiffrement à flot*, 2006, http://www.picsi.org/, portail Internet Cryptologie et Sécurité de l'Information.

[62] A. CANTEAUT, D. AUGOT, A. BIRYUKOV, A. BRAEKEN, C. CID, H. DOBBERTIN, H. ENGLUND, H. GILBERT, L. GRANBOULAN, H. HANDSCHUH, M. HELL, T. JOHANSSON, A. MAXIMOV, M. PARKER, T. PORNIN, B. PRENEEL, M. ROBSHAW, M. WARD. *D.STVL.4 – Open Research Areas in Symmetric Cryptography and Technical Trends in Lightweight Cryptography*, 88 pages, February 2006, Rapport du réseau d'excellence européen ECRYPT.

[63] M. DIARRA. *Analyse de la sécurité d'un protocole d'identification pour les RFID*, Direction : N. Sendrier, Stage d'option, École Polytechnique, July 2006.

[64] J. KEMPE, H. OLLIVIER, J. KEMPE. *Rapport final du projet "Réseaux Quantiques" de l'ACI "Sécurité Informatique" numéro 03510*, 13 pages, August 2006.

[65] M. N. PLASENCIA. *Cryptanalyse de systèmes de chiffrement à flot : étude de la sécurité d'Achterbahn*, Direction : A. Canteaut, Rapport de stage de Master Recherche II, Université de Versailles-St Quentin, INRIA, September 2006.

[66] O. TRABELSI. *Codes stabilisateurs quantiques*, Direction : J.P. Tillich, Technical report, ENIT Tunisie, September 2006.

[67] I. BEN SLIMEN. *Codes correcteurs pour les protocoles de reconciliation quantique de clés*, Direction : J.P. Tillich, Rapport de stage, INRIA, ENIT Tunisie, June 2006.

References in notes

[68] 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.

[69] 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.

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

[71] T. BERGER, P. LOIDREAU. *Security of the Niederreiter version of the GPT public key cryptosystem*, in "ISIT 2002, Proceedings, Lausanne, Switzerland", IEEE Press, July 2002, 267.

[72] T. BERGER, P. LOIDREAU. *How to mask the structure of codes for a cryptographic use*, in "Designs, Codes and Cryptography", vol. 35, April 2005, p. 63-79.

[73] J.-S. CORON. *Cryptanalysis of a Public-Key Encryption Scheme Based on the Polynomial Reconstruction Problem.*, in "Public Key Cryptography", 2004, p. 14-27.

[74] 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.

[75] J.-C. FAUGÈRE, A. JOUX. *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases.*, in "CRYPTO", 2003, p. 44-60.

[76] E. GABIDULIN, A. PARAMONOV, O. TRETJAKOV. *Ideals over a non-commutative ring and their application to cryptology*, in "EUROCRYPT'91", Lecture Notes in Computer Science, vol. LNCS 547, Springer Verlag, 1991, p. 482–489.

[77] 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.

[78] 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.

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

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