IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Paris

Activity Report 2011

Project-Team CASCADE

Construction and Analysis of Systems for Confidentiality and Authenticity of Data and Entities

IN COLLABORATION WITH: Laboratoire d'Informatique de l'Ecole Normale Supérieure (LIENS)

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithms, Certification, and Cryptography

Table of contents

Project-Team CASCADE

Keywords: Formal Methods, Security, Algorithmic Numbers Theory, Cryptography

1. Members

Research Scientists

Michel Ferreira Abdalla [CR, CNRS, HdR]
Bruno Blanchet [DR, INRIA, HdR]
Vadim Lyubashevsky [CR, INRIA]
Phong Quang Nguyen [DR, INRIA, HdR]
David Pointcheval [DR, CNRS, Team Leader, HdR]
Oded Regev [DR, CNRS]

Faculty Members

Pierre-Alain Fouque [Assistant Professor, ENS, HdR]
David Naccache [Professor, University Paris II, HdR]
Duong Hieu Phan [Assistant Professor, University Paris 8]
Jacques Stern [Professor, ENS, HdR]
Damien Vergnaud [Assistant Professor, ENS]

PhD Students

Olivier Blazy [University Paris 7 grant]
Charles Bouillaguet [Fondation EADS grant]
David Cadé [AMN grant]
Patrick Derbez [AMN grant]
Léo Ducas [AMN grant]
Aurore Guillevic [CIFRE Thales]
Jérémy Jean [ANR & DGA grant]
Roch Lescuyer [CIFRE Orange Labs]
Miriam Paiola [INRIA]
Mario Strefler [INRIA]
Mehdi Tibouchi [NTT & ANR grant]

Post-Doctoral Fellows

Dario Fiore [ANR grant]
Jiqiang Lu [ANR grant]
Christian Rechberger [Chaire FT]

Administrative Assistants

Nathalie Gaudechoux [INRIA]
Joëlle Isnard [Administrative Head DI, CNRS]

2. Overall Objectives

2.1. Presentation

Cryptographic algorithms are the equivalent of locks, seals, security stamps and identification documents on the Internet. They are essential to protect our on-line bank transactions, credit cards, medical and personal information and to support e-commerce and e-government. They come in different flavors. Encryption algorithms are essential to protect sensitive information such as medical data, financial information and Personal Identification Numbers (PINs) from prying eyes. Digital signature algorithms (in combination with hash functions) replace hand-written signatures in electronic transactions. A similar role can be played by

MAC algorithms. Identification protocols allow to securely verify the identity of the party at the other end of the line. Therefore, cryptology is a research area with a high strategic impact for industries, individuals, and for the society as a whole. The research activity of the project-team CASCADE addresses the following topics, which cover almost all the domains that are currently active in the international cryptographic community:

1. Implementation of cryptographic and applied cryptography
2. Design and provable security, for
   - signature schemes
   - public-key encryption schemes
   - identity-based encryption schemes
   - key agreement protocols
   - group-oriented protocols
3. Attacks, using
   - side-channels
   - algebraic techniques
4. Design and analysis of symmetric schemes

3. Scientific Foundations

3.1. Provable Security

Since the beginning of public-key cryptography, with the seminal Diffie-Hellman paper [69], many suitable algorithmic problems for cryptography have been proposed and many cryptographic schemes have been designed, together with more or less heuristic proofs of their security relative to the intractability of the underlying problems. However, many of those schemes have thereafter been broken. The simple fact that a cryptographic algorithm withstood cryptanalytic attacks for several years has often been considered as a kind of validation procedure, but schemes may take a long time before being broken. An example is the Chor-Rivest cryptosystem [68], based on the knapsack problem, which took more than 10 years to be totally broken [84], whereas before this attack it was believed to be strongly secure. As a consequence, the lack of attacks at some time should never be considered as a full security validation of the proposal.

A completely different paradigm is provided by the concept of "provable" security. A significant line of research has tried to provide proofs in the framework of complexity theory (a.k.a. "reductionist" security proofs): the proofs provide reductions from a well-studied problem (factoring, RSA or the discrete logarithm) to an attack against a cryptographic protocol.

At the beginning, researchers just tried to define the security notions required by actual cryptographic schemes, and then to design protocols which could achieve these notions. The techniques were directly derived from complexity theory, providing polynomial reductions. However, their aim was essentially theoretical. They were indeed trying to minimize the required assumptions on the primitives (one-way functions or permutations, possibly trapdoor, etc) [72], without considering practicality. Therefore, they just needed to design a scheme with polynomial-time algorithms, and to exhibit polynomial reductions from the basic mathematical assumption on the hardness of the underlying problem into an attack of the security notion, in an asymptotic way. However, such a result has no practical impact on actual security. Indeed, even with a polynomial reduction, one may be able to break the cryptographic protocol within a few hours, whereas the reduction just leads to an algorithm against the underlying problem which requires many years. Therefore, those reductions only prove the security when very huge (and thus maybe unpractical) parameters are in use, under the assumption that no polynomial time algorithm exists to solve the underlying problem.

For a few years, more efficient reductions have been expected, under the denomination of either "exact security" [65] or "concrete security" [77], which provide more practical security results. The perfect situation is reached when one is able to prove that, from an attack, one can describe an algorithm against the underlying problem, with almost the same success probability within almost the same amount of time: "tight reductions". We have then achieved "practical security" [61].

Unfortunately, in many cases, even just provable security is at the cost of an important loss in terms of efficiency for the cryptographic protocol. Thus, some models have been proposed, trying to deal with the security of efficient schemes: some concrete objects are identified with ideal (or black-box) ones. For example, it is by now usual to identify hash functions with ideal random functions, in the so-called "random-oracle model", informally introduced by Fiat and Shamir [70], and later formalized by Bellare and Rogaway [64]. Similarly, block ciphers are identified with families of truly random permutations in the "ideal cipher model" [62]. A few years ago, another kind of idealization was introduced in cryptography, the black-box group, where the group operation, in any algebraic group, is defined by a black-box: a new element necessarily comes from the addition (or the subtraction) of two already known elements. It is by now called the "generic model" [76], [83]. Some works even require several ideal models together to provide some new validations [67].

More recently, the new trend is to get provable security, without such ideal assumptions (there are currently a long list of publications showing "without random oracles" in their title), but under new and possibly stronger computational assumptions. As a consequence, a cryptographer has to deal with the three following important steps:

computational assumptions, which are the foundations of the security. We thus need to have a strong evidence that the computational problems are reasonably hard to solve. We study several assumptions, by improving algorithms (attacks), and notably using lattice reductions. We furthermore contribute to the list of "potential" hard problems.

security model, which makes precise the security notions one wants to achieve, as well as the means the adversary may be given. We contribute to this point, in several ways:

- by providing a security model for many primitives and protocols, and namely group-oriented protocols, which involve many parties, but also many communications (group key exchange, group signatures, etc);
- by enhancing some classical security models;
- by considering new means for the adversary, such as side-channel information.

design of new schemes/protocols, or more efficient, with additional features, etc.

security proof, which consists in exhibiting a reduction.

For a long time, the security proofs by reduction used classical techniques from complexity theory, with a direct description of the reduction, and then a long and quite technical analysis for providing the probabilistic estimates. Such analysis is unfortunately error-prone. Victor Shoup proposed a nice way to organize the proofs, and eventually obtain the probabilities, using a sequence of games [82], [63], [78] which highlights the computational assumptions, and splits the analysis in small independent problems. We early adopted and developed this technique, and namely in [71]. We applied this methodology to various kinds of systems, in order to achieve the highest security properties: authenticity, integrity, confidentiality, privacy, anonymity. Nevertheless, efficiency was also a basic requirement.

However, such reductions are notoriously error-prone: errors have been found in many published protocols. Security errors can have serious consequences, such as loss of money in the case of electronic commerce. Moreover, security errors cannot be detected by testing, because they appear only in the presence of a malicious adversary.

Security protocols are therefore an important area for formal verification.

We thus worked on the development of two successful automatic protocol verifiers, ProVerif in the formal model and CryptoVerif in the computational model, and we plan to pursue research on this topic, in particular with extensions to CryptoVerif.

3.2. Cryptanalysis

Because there is no absolute proof of security, it is essential to study cryptanalysis, which is roughly speaking the science of code-breaking. As a result, key-sizes are usually selected based on the state-of-the-art in cryptanalysis. The previous section emphasized that public-key cryptography required hard computational problems: if there is no hard problem, there cannot be any public-key cryptography either. If any of the computational problems mentioned above turns out to be easy to solve, then the corresponding cryptosystems can be broken, as the public key would actually disclose the private key. This means that one obvious way to cryptanalyze is to solve the underlying algorithmic problems, such as integer factorization, discrete logarithm, lattice reduction, Gröbner bases, *etc.* Here, we mean a study of the computational problem in its full generality. The project-team has a strong expertise (both in design and analysis) on the best algorithms for lattice reduction, which are also very useful to attack classical schemes based on factorization or discrete logarithm.

Alternatively, one may try to exploit the special properties of the cryptographic instances of the computational problem. Even if the underlying general problem is NP-hard, its cryptographic instances may be much easier, because the cryptographic functionalities typically require a specific mathematical structure. In particular, this means that there might be an attack which can only be used to break the scheme, but not to solve the underlying problem in general. This happened many times in knapsack cryptography and multivariate cryptography. Interestingly, generic tools to solve the general problem perform sometimes even much better on cryptographic instances (this happened for Gröbner bases and lattice reduction).

However, if the underlying computational problem turns out to be really hard both in general and for instances of cryptographic interest, this will not necessarily imply that the cryptosystem is secure. First of all, it is not even clear what is meant exactly by the term *secure* or *insecure*. Should an encryption scheme which leaks the first bit of the plaintext be considered secure? Is the secret key really necessary to decrypt ciphertexts or to sign messages? If a cryptosystem is theoretically secure, could there be potential security flaws for its implementation? For instance, if some of the temporary variables (such as pseudo-random numbers) used during the cryptographic operations are partially leaked, could it have an impact on the security of the cryptosystem? This means that there is much more into cryptanalysis than just trying to solve the main algorithmic problems. In particular, cryptanalysts are interested in defining and studying realistic environments for attacks (adaptive chosen-ciphertext attacks, side-channel attacks, *etc.*), as well as goals of attacks (key recovery, partial information, existential forgery, distinguishability, *etc.*). As such, there are obvious connections with provable security. It is perhaps worth noting that cryptanalysis also proved to be a good incentive for the introduction of new techniques in cryptology. Indeed, several mathematical objects now considered invaluable in cryptographic design were first introduced in cryptology as cryptanalytic tools, including lattices and pairings. The project-team has a strong expertise in cryptanalysis: many schemes have been broken, and new techniques have been developed.

3.3. Symmetric Cryptography

Even if asymmetric cryptography has been a major breakthrough in cryptography, and a key element in its recent development, conventional cryptography (a.k.a. symmetric, or secret key cryptography) is still required in any application: asymmetric cryptography is much more powerful and convenient, since it allows signatures, key exchange, etc. However, it is not well-suited for high-rate communication links, such as video or audio streaming. Therefore, block-ciphers remain a fundamental primitive. However, since the AES Competition (which started in January 1997, and eventually selected the Rijndael algorithm in October 2000), this domain has become less active, even though some researchers are still trying to develop new attacks. On the opposite, because of the lack of widely admitted stream ciphers (able to encrypt high-speed streams of data), ECRYPT (the European Network of Excellence in Cryptology) launched the eSTREAM project, which investigated research on this topic, at the international level: many teams proposed candidates that have been analyzed by the entire cryptographic community. Similarly, in the last few years, hash functions [80], [79], [74], [75], [73], which are an essential primitive in many protocols, received a lot of attention: they were initially used for improving efficiency in signature schemes, hence the requirement of collision-resistance. But afterwards,

hash functions have been used for many purposes, such as key derivation, random generation, and random functions (random oracles [64]). Recently, a bunch of attacks [66], [85], [86], [87], [88], [90], [89] have shown several drastic weaknesses on all known hash functions. Knowing more (how weak they are) about them, but also building new hash functions are major challenges. For the latter goal, the first task is to formally define a security model for hash functions, since no realistic formal model exists at the moment: in a way, we expect too much from hash functions, and it is therefore impossible to design such "ideal" functions. Because of the high priority of this goal (the design of a new hash function), the NIST has launched an international competition, called SHA-3 (similar to the AES competition 10 years ago), in order to select and standardize a hash function in 2012.

One way to design new hash functions may be a new mode of operation, which would involve a block cipher, iterated in a specific manner. This is already used to build stream ciphers and message authentication codes (symmetric authentication). Under some assumptions on the block cipher, it might be possible to apply the above methodology of provable security in order to prove the validity of the new design, according to a specific security model.

4. Application Domains

4.1. Hash Functions

Since the previous section just ended on this topic, we start with it for the major problems to address within the next 5 years. A NIST competition on hash functions has been launched late 2007. In the first step, cryptographers had to build and analyze their own candidate; in a second step, cryptanalysts are solicited, in order to analyze and break all the proposals. The conclusion is planned for 2012.

The symmetric people of the Cascade team have worked this year on the development of a new hash function called SIMD that has been selected for the second round of the NIST SHA-3 competition. SIMD hash function is quite similar to members of the MD/SHA family. It is based on a familiar Merkle-Damgard design, where the compression function is built from a Feistel-like cipher in Davies-Meyer mode. However there are some innovations in this design: the internal state is twice as big as the output size, we use a strong message expansion, and we use a modified feed-forward in the compression function. The main design criteria was to follow the MD/SHA designs principle which are quite well understood, and to add some elements to avoid all known attacks. SIMD is particularly efficient on platforms with vector instructions (SIMD) which are available on many processors. Such instructions have been proposed since 1997 and are now widely deployed. Moreover, it is also possible to use two cores on multicore processors to boost the performances with a factor 1.8 by splitting the message expansion function and the hashing process.

We've also drawn some analyses and attacks on the other candidates.

4.2. Anonymity and Privacy

A relatively new goal of growing importance of cryptography is *privacy*. In a digital world where data is ubiquitous, users are more and more concerned about confidentiality of their personal data. Cryptography makes it possible to benefit from the advantages of digital technology while at the same time providing means for privacy protection. An example is anonymous authentication: A user can convincingly prove that she has certain rights without however revealing her identity. Privacy and anonymity remains thus one of the main challenges for the next years.

4.3. Copyright Protection

Similarly to the privacy concern, the digital world makes easy the large-scale diffusion of information. But in some cases, this can be used in violation of some copyrights. Cryptography should help at solving this problem, which is actually two-fold: one can either mark the original document in order to be able to follow the distribution (and possibly trace the traitor who illegally made it public) or one can publish information in an encrypted way, so that authorized people only can access it.

4.4. Lattice-Based Cryptography

In 1996, Ajtai [60] showed that lattices, which up to that point had only been used as tools in cryptanalysis, can actually be used to *construct* cryptographic primitives. He proposed a cryptographic primitive whose security is based on the worst-case hardness of lattice problems: if one succeeds in breaking the primitive, even with some small probability, then one can also solve any instance of a certain lattice problem. This powerful property makes lattice-based cryptographic constructions very attractive. In contrast, virtually all other cryptographic constructions are based on some average-case assumption. Furthermore, there are currently very few alternatives to traditional number-theoretic based cryptography such as RSA. Such alternatives will be needed in case an efficient algorithm for factoring integers is ever found, a possibility some leading number theorists consider as quite likely. In fact, efficient quantum algorithms for factoring integers and computing discrete logarithms already exist [81]. Although large-scale quantum computers are not expected to exist for at least a decade, this fact should already be regarded as a warning. In contrast, there are currently no known quantum algorithms for lattice problems. Finally, the computations involved in lattice-based cryptography are typically very fast and often require only modular additions, making them attractive for many applications.

For all these reasons, lattice-based cryptography has become a hot topic, especially in the last few years, and our group is playing an important part in this effort.

4.5. Cryptanalysis

As already explained, even with the *provable security* concept, cryptanalysis is still an important area, and attacks can be done at several levels. Algebraic tools (against integer factoring, discrete logarithm, polynomial multivariate systems, lattice reduction, etc) have thus to be studied and improved in order to further evaluation of the actual security level of cryptographic schemes.

At the hardware level, side-channel information has to be identified (time, power, radiation, noise, heat, etc) in order to securely protect embedded systems. But such information may also be used in a positive way....

5. Software

5.1. MitMTool

Participants: Charles Bouillaguet, Patrick Derbez, Pierre-Alain Fouque.

The purpose of MITMTOOL is to look for guess-and-determine and meet-in-the-middle attacks on AES and AES-based constructions. This tool allows us to improve known attacks on round-reduced versions of AES, on the LEX stream-cipher on the PELICAN Message Authentication Code and on fault attack on AES. Basically, it solves the problem to find all the solutions of a linear system of equations on the variables x and $S(x)$ where S is an inert function. The tool allows to compute the complexity of some good attack as well as the C code of the attack. We verify that the complexity estimates are accurate using experiments. We also use it to find one solution of the system for chosen-key differential attacks. There are mainly two tools: the first one only looks for guess-and-determine attack and tries to propagate some knowledge and guesses value when it cannot find automatically the value of some variable. The second tool uses the technique of the first tool and more advanced technique to take into account attacks with memory that use the meet-in-the-middle attack.

5.2. ProVerif

Participants: Bruno Blanchet, Vincent Cheval.

PROVERIF (www.proverif.ens.fr) is an automatic security protocol verifier, in the formal model (so called Dolev–Yao model). In this model, cryptographic primitives are considered as black boxes. This protocol verifier is based on an abstract representation of the protocol by Horn clauses. Its main features are:

- It can handle many different cryptographic primitives, including shared- and public-key cryptography (encryption and signatures), hash functions, and Diffie–Hellman key agreements, specified both as rewrite rules or as equations.
- It can handle an unbounded number of sessions of the protocol (even in parallel) and an unbounded message space. This result has been obtained thanks to some well-chosen approximations. This means the verifier can give false attacks, but if it claims that the protocol satisfies some property, then the property is actually satisfied. PROVERIF also provides attack reconstruction: when it cannot prove a property, it tries to reconstruct an attack, that is, an execution trace of the protocol that falsifies the desired property.

The PROVERIF verifier can prove the following properties:

- secrecy (the adversary cannot obtain the secret);
- authentication and more generally correspondence properties, of the form "if an event has been executed, then other events have been executed as well";
- strong secrecy (the adversary does not see the difference when the value of the secret changes);
- equivalences between processes that differ only by terms;

PROVERIF has been used by researchers for studying various kinds of protocols, including electronic voting protocols, certified email protocols, and zero-knowledge protocols. It has been used as a back-end for the tool TULAFALE implemented at Microsoft Research Cambridge, which verifies web services protocols. It has also been used as a back-end for verifying implementations of protocols in F# (a dialect of ML included in .NET), by Microsoft Research Cambridge and the joint INRIA-Microsoft research center.

PROVERIF is freely available on the web, at www.proverif.ens.fr, under the GPL license.

5.3. CryptoVerif

Participants: Bruno Blanchet, David Cadé.

CRYPTOVERIF (www.cryptoverif.ens.fr) is an automatic protocol prover sound in the computational model. In this model, messages are bitstrings and the adversary is a polynomial-time probabilistic Turing machine. CRYPTOVERIF can prove:

- secrecy;
- correspondences, which include in particular authentication.

CRYPTOVERIF provides a generic mechanism for specifying the security assumptions on cryptographic primitives, which can handle in particular symmetric encryption, message authentication codes, public-key encryption, signatures, hash functions, Diffie-Hellman key agreement.

The generated proofs are proofs by sequences of games, as used by cryptographers. These proofs are valid for a number of sessions polynomial in the security parameter, in the presence of an active adversary. CRYPTOVERIF can also evaluate the probability of success of an attack against the protocol as a function of the probability of breaking each cryptographic primitive and of the number of sessions (exact security).

CRYPTOVERIF is still at a rather early stage of development, but it has already been used for a study of Kerberos in the computational model. It is also used as a back-end for verifying implementations of protocols in F# at Microsoft Research Cambridge and at the joint INRIA-Microsoft research center.

CRYPTOVERIF is freely available on the web, at www.cryptoverif.ens.fr, under the CeCILL-B license.

6. Contracts and Grants with Industry

6.1. ANR Projects with Industrials

- **SAPHIR-II** *(Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes)*
  Security and analysis of innovating and recent hashing primitives.
  Participants: Charles Bouillaguet, Pierre-Alain Fouque, Jiqiang Lu, Christian Rechberger.

  From April 2009 to March 2013.
  Partners: France Telecom R&D, Gemalto, EADS, SAGEM, DCSSI, Cryptolog, INRIA/Secret, UVSQ, XLIM, CryptoExperts.

- **PACE: Pairings and Advances in Cryptology for E-cash.**
  Participants: Olivier Blazy, Pierre-Alain Fouque, David Pointcheval, Mehdi Tibouchi, Damien Vergnaud.

  From December 2007 to February 2012.
  Partners: France Telecom R&D, NXP, Gemalto, CNRS/LIX (INRIA/TANC), Univ. Caen, Cryptolog.
  This project aims at studying new properties of groups (similar to pairings, or variants), and then to exploit them in order to achieve more practical e-cash systems.

- **PAMPA: Password Authentication and Methods for Privacy and Anonymity.**
  Participants: Michel Ferreira Abdalla, Dario Fiore, David Pointcheval.

  From December 2007 to December 2011.
  Partners: EADS, Cryptolog.
  One of the goals of this project is to improve existing password-based techniques, not only by using a stronger security model but also by integrating one-time passwords (OTP). This could avoid for example having to trust the client machine, which seems hard to guarantee in practice due the existence of numerous viruses, worms, and Trojan horses. Another extension of existing techniques is related to group applications, where we want to allow the establishment of secure multicast networks via password authentication. Several problems are specific to this scenario, such as dynamicity, robustness, and the random property of the session key, even in the presence of dishonest participants.
  Finally, the need for authentication is often a concern of service providers and not of users, who are usually more interested in anonymity, in order to protect their privacy. Thus, the second goal of this project is to combine authentication methods with techniques for anonymity in order to address the different concerns of each party. However, anonymity is frequently associated with fraud, without any possible pursuit. Fortunately, cryptography makes it possible to provide conditional anonymity, which can be revoked by a judge whenever necessary. This is the type of anonymity that we will privilege.

- **BEST: Broadcast Encryption for Secure Telecommunications.**
  Participants: Duong Hieu Phan, David Pointcheval, Mario Strefler.

  From December 2009 to November 2013.
  Partners: Thales, Nagra, CryptoExperts, Univ Paris 8.
  This project aims at studying broadcast encryption and traitor tracing, with applications to the Pay-TV and geolocalisation services.

- **PRINCE: Proven Resilience against Information leakage in Cryptographic Engineering.**
  Participants: Michel Ferreira Abdalla, Bruno Blanchet, Dario Fiore, David Pointcheval.

  From December 2010 to November 2014.
  Partners: UVSQ, Oberthur Technologies, Ingenico, Gemalto, Tranef.
  We aim to undertake research in the field of leakage-resilient cryptography with a practical point of view. Our goal is to design efficient leakage-resilient cryptographic algorithms and invent new countermeasures for non-leakage-resilient cryptographic standards. These outcomes shall realize a provable level of security against side-channel attacks and come with a formally verified implementation. For this every practical aspect of the secure implementation of cryptographic schemes must be taken into account, ranging from the high-level security protocols to the cryptographic algorithms and from these algorithms to their implementation on specific devices which hardware design may feature different leakage models.

6.2. ANR Projects within Academics

- **ProSe: Security protocols : formal model, computational model, and implementations.**
  Participants: Bruno Blanchet, David Cadé, Miriam Paiola, David Pointcheval.

  From December 2010 to November 2014.
  Partners: ENS Cachan-INRIA/Secsi, LORIA-INRIA/Cassis, Verimag.
  The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the symbolic level, in which messages are terms; the computational level, in which messages are bitstrings; the implementation level: the program itself.

7. Partnerships and Cooperations

7.1. European Initiatives

- **ECRYPT-II: Network of Excellence in Cryptology.**
  From August 2008 to July 2012.
  There are three virtual labs that focus on the following core research areas: symmetric key algorithms (STVL), public key algorithms and protocols (MAYA), and secure and efficient implementations (VAMPIRE).
  ENS/INRIA/CASCADE leads the MAYA virtual lab.
- **ERC Starting Grant: LATTICE.**
  Oded Regev (2008 – 2013)
- **SecFuNet: Security for Future Networks.**
  From July 2011 to December 2013

7.2. Grants

- **Chaire ENS – France Télécom pour la sécurité des réseaux de télécommunications.**
  From January 2006 to December 2012.
- **Fondation EADS Grant.**
  Charles Bouillaguet, in PhD Thesis from September 2008 to August 2011
- **Donation of Tilera multicore cluster (512 core, 64 bits each) by Tilera.**
  This supercomputer allows the team to experiment various cryptanalysis and simulations. The machine was installed at ENS for the team, in recognition of the team's cryptanalytic and research achievements.

7.3. Exterior Research Visitors

- Zvika Brakerski – Weizmann Institute, Israel
- Vincent Cheval – ENS Cachan, France
- Angelo De Caro – Univ. Salerno, Italy
- Karina M. Magalhães – University of Campinas, Brazil)
- Petros Mol – UC San Diego, USA
- Takashi Nishide – Kyushu University, Japan
- Chris Peikert – Georgia Tech , USA
- Adi Shamir – Weizmann Institute, Israel

8. Dissemination

8.1. Editorial Boards

Editor-in-Chief

– of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: David Pointcheval

Associate Editor-in-Chief

– of the *Theory of Computing (ToC)*: Oded Regev

Associate Editor

– of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: Bruno Blanchet
– of the *Journal of Cryptology*: Phong Nguyen
– of the *Journal of Mathematical Cryptology*: Phong Nguyen
– of *Security and Communication Networks*: David Naccache
– of *Journal of Cryptographic Design*: David Naccache
– of *Encyclopedia of Cryptography and Security*: David Naccache
– of *Journal of Small Scale Digital Device Forensics (publication currently on hold for financial reasons)*: David Naccache
– of *Computers & Security Elsevier Advanced Technology* – Elsevier: David Naccache
– of *Cryptologia* – Taylor & Francis: David Naccache
– of *Information Processing Letters* – Elsevier: David Pointcheval
– of *IEEE Transactions on Information Forensics and Security*: Michel Abdalla

Columnist (in charge of the bi-monthly CryptoCorner)

– of the *IEEE Security and Privacy Magazine*: David Naccache

8.2. Program Committees

- SOFSEM – January 2011, Nový Smokovec, Slovakia: Phong Nguyen
- COSADE – February 2011, Darmstadt, Germany: David Naccache
- CT-RSA – February 2011, San Francisco, USA: David Pointcheval

- ESSoS – February 2011, Madrid, Spain: Bruno Blanchet
- FSE – February 2011, Copenhague, Denmark: Pierre-Alain Fouque
- NTMS - Security Track – February 2011, Paris, France: David Naccache
- AsiaCCS – March 2011, Hong Kong, China: Damien Vergnaud
- TCC – March 2011, Providence, USA : Vadim Lyubashevsky
- PKC – March 2011, Taormina, Italy: Dario Fiore
- EUROCRYPT – May 2011, Tallinn, Estonia: Michel Abdalla, Vadim Lyubashevsky, David Pointcheval
- CryptoForma workshop – June 2011, Limerick, Ireland: Bruno Blanchet
- ACNS – June 2011, Malaga, Spain: Michel Abdalla, David Naccache
- TRUST – June 2011, Pittsburgh, PA USA: David Naccache
- FCC workshop – June 2011, Paris, France: Bruno Blanchet
- IEEE ISCC – June 2011, Kerkyra, Greece: David Naccache
- ACISP – July 2011, Melbourne, Australia: Michel Abdalla, Damien Vergnaud
- AFRICACRYPT – July 2011, Dakar, Senegal: David Pointcheval (Program Chair), Damien Vergnaud
- SECRYPT – July 18-21, Seville, Spain: David Naccache
- CRYPTO – August 2011, Santa-Barbara, USA: Phong Nguyen
- CHES – September 2011, Nara, Japan: Pierre-Alain Fouque, David Naccache
- ISC – October 2011, Xi'an, China: Michel Abdalla
- CCS – October 2011, Chicago, USA: Bruno Blanchet, David Naccache
- Provsec – October 2011, Xi'an, China: David Naccache, Damien Vergnaud
- PQC – November 2011, Taipei, Taiwan : Vadim Lyubashevsky
- INTRUST – November 2011, Beijing, China: David Naccache
- ECRYPT Workshop on Lightweight Cryptography – November 2011, Louvain-la-Neuve, Belgium: David Naccache
- ASIACRYPT – December 2011, Seoul, South Korea: Michel Abdalla, Phong Nguyen
- IMACC – December 2011, Oxford, UK: David Naccache
- Indocrypt – December 2011: Vadim Lyubashevsky

8.3. Teaching

L1 – Introduction to computer science (Univ. Paris II): David Naccache

L3 – Analytical Methods in Computer Science (ENS): Oded Regev

M1 – Scientific programming through practice (ENS): David Naccache

M1 – Introduction to Cryptology (ENS): David Naccache, Jacques Stern, Damien Vergnaud

M1 – Introduction to Cryptology (EPITA): Phong Nguyen

M2 – Cryptography (MPRI): Michel Abdalla, Vadim Lyubashevsky

M2 – Provable Security for Cryptographic Protocols (MPRI): Bruno Blanchet

M2 – Computer Security (Univ. Paris II): David Naccache

M2 – Risk Management (Univ. Paris II): David Naccache

M2 – Computer forensics (Univ. Paris II): David Naccache

M2 – Provable Security (Univ. Paris VIII): Duong-Hieu Phan

M2 – Cryptography (ESIEA): David Pointcheval

Summer school – Marktoberdorf (Bayrischzell, Germany): Bruno Blanchet

Summer school – VTSA (Liege, Belgium): Bruno Blanchet

8.4. Ph.D/Habilitation Defenses

- Mehdi Tibouchi – Ph.D. – 23 sept. 2011 – Université Paris VII – France
  Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA [16]
- Charles Bouillaguet – Ph.D. – 26 sept. 2011 – Université Paris VII – France
  Etudes d'hypothèses algorithmiques et analyse de primitives cryptographiques [15]
- Michel Abdalla – HDR – 24 nov. 2011 – ENS – France
  Reducing The Need For Trusted Parties In Cryptography [14]

8.5. Ph.D/Habilitation Committees

- Alexandre Venelli – Ph.D. – 31 Jan. 2011 - Uni. Aix-Marseille 2 – France
  Contribution à la sécurité physique des cryptosystèmes embarqués
  David Naccache (reviewer)
- Amandine Jambert – Ph.D. – 15 Mar. 2011 – Uni. Bordeaux I – France
  Outils Crytographiques pour la Protection des Contenus et de la Vie Privée des Utilisateurs
  David Pointcheval (reviewer)
- Steve Kremer – HDR – 17 Mar. 2011 – Ecole Normale Supérieure de Cachan – France
  Modelling and Analyzing Security Protocols in Cryptographic Process Calculi
  David Pointcheval
- Stéphanie Delaune – HDR – 18 Mar. 2011 – Ecole Normale Supérieure de Cachan – France
  Verification of security protocols: from confidentiality to privacy
  Bruno Blanchet
- Moez Ben Mbarka – Ph.D. – 6 Apr. 2011 – Université Bordeaux I – France
  Signatures électroniques avancées : modélisation de la validation à long terme et sécurité des autorités de certification
  Bruno Blanchet
- Jean Lancrenon – Ph.D. – 22 June 2011 – Univ. Grenoble – France
  Protocoles d'authentification d'objets à distance
  David Pointcheval (reviewer)
- Carla Ràfols – Ph.D. – 19 July 2011 – Universitat Politècnica de Catalunya – Spain
  Some issues in public key cryptography: hard-core predicates, distributed protocols and functional encryption
  Damien Vergnaud (reviewer)
- Mehdi Tibouchi – Ph.D. – 23 Sept. 2011 – Université Paris VII – France
  Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA
  Pierre-Alain Fouque, David Naccache (co-advisor), Jacques Stern
- Charles Bouillaguet – Ph.D. – 26 Sept. 2011 – Université Paris VII – France
  Etudes d'hypothèses algorithmiques et analyse de primitives cryptographiques
  Pierre-Alain Fouque (co-advisor), David Pointcheval (co-advisor), Jacques Stern
- Luk Bettale – Ph.D. – 3 Oct. 2011 – Université Paris VI – France
  Cryptanalyse Algébrique: Outils et Applications
  Pierre-Alain Fouque (reviewer)

- Damien Stehlé – HDR – 14 Oct. 2011 – ENS Lyon – France
  Euclidean Lattices: Algorithms and Cryptography
  Oded Regev (reviewer)
- Pierre Girard – HDR – 20 Oct. 2011 – Uni. Limoges (XLIM) – France
  Contribution à la sécurité des cartes à puce et de leur utilisation
  David Naccache (reviewer)
- Jop Briët – Ph.D. – 27 Oct. 2011 – CWI, Amsterdam – The Netherlands
  Grothendieck inequalities, Nonlocal games and Optimization
  Oded Regev (reviewer)
- Jean Martinelli – Ph.D. – 18 Nov. 2011 – Université Versailles-Saint Quentin en Yvelines – France
  Protection d'algorithmes de chiffrement par blocs contre les attaques par canaux auxiliaires d'ordre supérieur
  Pierre-Alain Fouque (reviewer)
- Michel Abdalla – HDR – 24 Nov. 2011 – ENS – France
  Reducing The Need For Trusted Parties In Cryptography
  David Pointcheval (advisor), Jacques Stern
- Youssef Souissi – Ph.D. – 6 December 2011 – Telecom ParisTech – France
  Méthodes optimisant l'analyse des cryptoprocesseurs sur les canaux cachés
  David Naccache (reviewer)
- Moulay Abdelaziz El Aabid – Ph.D. – 7 Dec. 2011 – Univ. Paris 8 – France
  Attaques par canaux cachés : expérimentations avancées sur les attaques templates
  David Naccache (reviewer)
- Ştefan Ciobâcă – Ph.D. – 9 Dec. 2011 – Ecole Normale Supérieure de Cachan – France
  Verification and Composition of Security Protocols with Applications to Electronic Voting
  Bruno Blanchet (reviewer)
- Eric Laurent Ricard – Ph.D. – 9 Dec. 2011 – Univ. Paris 2 – France
  Rétablir la confiance dans les messages électroniques
  David Naccache (advisor)
- Fabien Laguillaumie – HDR – 12 Dec. 2011 – Univ. Caen Basse Normandie – France
  Public-Key Cryptography: Design and Algorithmic
  David Pointcheval (reviewer)
- Jean-René Reinhard – Ph.D. – 14 Dec. 2011 – Université Versailles-Saint Quentin en Yvelines – France
  Étude de Primitives Cryptographiques Symétriques: Chiffrements par Flot et Fonctions de Hachage
  Pierre-Alain Fouque (reviewer)
- Khaled Ouafi – Ph.D. – 19 Dec. 2011 – EPFL – Switzerland
  Security and privacy in RFID Systems
  David Naccache (reviewer)
- Amir Pasha Mirbaha – Ph.D. – 20 Dec. 2011 – Ecole nationale sup. des Mines de St Etienne – France
  Study of the Vulnerability of Cryptographic Circuits by Laser Fault Injection
  David Naccache (co-advisor)
- Marco Ramilli – Ph.D. – [date to be set in 2011] – DEIS University of Bologna – Italy
  A design methodology for security test planning in distributed systems
  David Naccache (reviewer)

8.6. Invited Talks

- QIP 2010, Singapore (January): Oded Regev

- CASED Distinguished Lecture + Additional Lecture for Students, Germany (January): David Naccache
- Anniversary workshop in honour of Gérard Berry and Jean-Jacques Lévy, Gérardmer, France (February): Bruno Blanchet
- Two talks in workshop, Dagstuhl, Germany (March): Oded Regev
- Journées Codage et Cryptographie, St. Pierre d'Oleron, France (April): Vadim Lyubashevsky, Damien Vergnaud
- 30th EUROCRYPT Conference, Tallinn, Estonia (May): Phong Nguyen
- Mathématiques en mouvement, Paris, France (May): Phong Nguyen
- Coding, Cryptology, and Combinatorial Design, Singapore (May): Vadim Lyubashevsky
- International Workshop on Mathematical Cryptology, Daejeon, South Korea (June): Michel Abdalla
- WISTP 2011, Heraklion, Crete, Greece (June): David Naccache
- Introductory Workshop on Quantitative Geometry, MSRI, Berkeley, California, USA (August): Oded Regev
- Course on Foundations of Cryptography and Impossibility Results, Scuola Superiore di Catania, Catania, Italy (September): Dario Fiore
- Faces of Modern Cryptography, New York City, USA (September) : Vadim Lyubashevsky
- 5th CHINACRYPT, Changsha, China (October): Phong Nguyen
- IEEE Information Theory Workshop, Paraty, Brazil (October): Vadim Lyubashevsky
- São Paulo Advanced School of Cryptography, Campinas, Brazil (October): Michel Abdalla, Vadim Lyubashevsky, Jacques Stern
- 4th PQCrypto Conference, Taipeh, Taiwan (November): Phong Nguyen
- European Postdoctoral Day of Excellence in Cryptography, Darmstadt, Germany (November): Dario Fiore
- Congrès du LIA CNRS Formath Vietnam (November): Duong Hieu Phan
- New York Theory Day (November): Oded Regev
- 7th INSCRYPT Conference, Beijing, China (December): Phong Nguyen
- 10th CANS Conference, Sanya, China (December): Phong Nguyen
- IMACC, Oxford, UK (December): David Naccache

8.7. Invitations

- Weizmann Institute, Jan 23 - Feb 8: Oded Regev
- New York University, Oct 8 - Jan 2: Oded Regev
- Weizmann Institute, Oct 28 - Nov 8: Pierre-Alain Fouque

8.8. Seminar Presentations

- Séminaire Codage, Cryptologie, Algorithmes (CCA), Paris, France (January): Oded Regev
- Theory seminar, Technion, Israel (January): Oded Regev
- Cryptography Group, Bristol University, UK (January): Mehdi Tibouchi
- LIRMM, Montpellier, France (January): Mehdi Tibouchi
- Theory seminar, Weizmann Institute, Israel (February): Oded Regev
- GREYC, Université de Caen, France (February): Mehdi Tibouchi

- TELECOM ParisTech, Paris, France (February): Mehdi Tibouchi
- Newton Institute, Cambridge (March): Oded Regev
- Univ. of Limoges, France (March): Vadim Lyubashevsky
- ENS Lyon, France (March): Vadim Lyubashevsky
- Univ. of Grenoble, France (March): Phong Nguyen
- East China Normal Univ., China (April): Phong Nguyen
- IRSEM – IDEST, Paris, France (June): David Naccache
- Univ. of Grenoble, France (June): David Pointcheval
- Univ. of Rennes, France (June): Vadim Lyubashevsky
- ENPC, Marne la Vallée, France (September): David Pointcheval
- IQC, Waterloo, Canada (September) : Vadim Lyubashevsky
- IRISA, Rennes, France (October): Bruno Blanchet
- ENS Cachan, Ker Lann, France (November): Pierre-Alain Fouque
- Univ. of Rennes, France (November): David Naccache
- LACS, University of Luxembourg, Luxembourg (May): Dario Fiore
- GREYCC, Université de Caen, France (June): Dario Fiore
- Tsinghua Univ., China (August): Phong Nguyen
- Seminar, Haifa University, Israel (November): Pierre-Alain Fouque
- Theory seminar, Weizmann Institute, Israel (November): Pierre-Alain Fouque
- CSDM seminar, Institute for Advanced Study, Princeton, USA (November): Oded Regev
- IMATH, Université Sud Toulon Var, France (November): Aurore Guillevic
- PRiSM, Université de Versailles, France (November): Aurore Guillevic
- ENS Cachan, Cachan, France (November): Pierre-Alain Fouque
- IRISA, Rennes, France (December): Pierre-Alain Fouque

8.9. Participation in Workshops and Conferences

QIP – January 2011, Singapore: Oded Regev

Computational Complexity of Discrete Problems – March 2011, Dagstuhl, Germany: Oded Regev

Cryptography and Security in Clouds Workshop – March 2011, Zurich, Switzerland: Michel Abdalla

Discrete Harmonic Analysis Workshop – March 2011, Cambridge, UK: Oded Regev

TCC – March 2011, Providence, USA : Vadim Lyubashevsky

FSE – March 2011, Copenhagen, Danmark: Jérémy Jean

FSE – March 2011, Copenhagen, Danmark: Pierre-Alain Fouque

PKC – March 2011, Taormina, Italy: Michel Abdalla, David Pointcheval, Dario Fiore, Mehdi Tibouchi, Damien Vergnaud, Olivier Blazy, David Naccache

CT-RSA – April 2011, San Francisco, California, USA: David Pointcheval

Eurocrypt – May 2011, Tallinn, Estonia: Phong Nguyen, David Pointcheval, Jacques Stern, Dario Fiore, Damien Vergnaud, David Naccache

ACNS – June 2011, Malaga, Spain: Dario Fiore, Mario Strefler

CSF and FCC – June 2011, Paris, France: Bruno Blanchet, David Cadé, Miriam Paiola

MathCrypt – June 2011, Daejeon, South Korea: Michel Abdalla

STOC and CCC – June 2011, San Jose, California, USA: Oded Regev

WISTP – June 2011, Heraklion, Crete, Greece: David Naccache

Africacrypt – July 2011, Dakar, Senegal: David Pointcheval, Damien Vergnaud

MAYA Workshop "New Applications of New Computational Problems" – July 2011, Bochum, Germany : Michel Abdalla, Dario Fiore

SAC – August 2011, Toronto, Canada: Charles Bouillaguet, Jérémy Jean

Crypto – August 2011, Santa-Barbara, California, USA: Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, Patrick Derbez, Charles Bouillaguet, Jacques Stern, Jérémy Jean, Dario Fiore, Mehdi Tibouchi, Vadim Lyubashevsky

Workshop on Quantitative Geometry – August 2011, MSRI, Berkeley, USA: Oded Regev

Elliptic Curve Cryptography Workshop – September 2011, Nancy, France: Aurore Guillevic

CHES – September 2011, Nara, Japan: Mehdi Tibouchi

Annual ECRYPT II overview event – September 2011, Leuven, Belgium : Michel Abdalla

Quantum Computer Science Workshop – October 2011, Montreal, Canada: Oded Regev

Lightweight Cryptography Workshop – November 2011, Louvain-la-Neuve, Belgium : Vadim Lyubashevsky

Asiacrypt – December 2011, Seoul, South Korea: Michel Abdalla, Pierre-Alain Fouque, Damien Vergnaud

8.10. Scientific Animation

8.10.1. Organisation of Events

- a weekly seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html

8.10.2. Board of International Organizations

- Chair of the Program Committee of Africacrypt – David Pointcheval
- Board of the *International Association for Cryptologic Research* (IACR) – David Naccache (2010 – 2012), David Pointcheval (2008–2013)

8.10.3. French Research Community

- Recruitment committee at Université Paris VIII (PR 27): David Pointcheval
- Recruitment committee at Université Versailles-Saint Quentin en Yvelines (MdC 27): Pierre-Alain Fouque
- Recruitment committee at Université Paris II (MdC 26): David Naccache
- Recruitment committee at Université Paris I (PR 27): David Naccache
- INRIA Paris-Rocquencourt seminar committee: Phong Nguyen
- Member of the scientific committee of the LabEx AMIES (Agence pour les Mathématiques et Interaction avec l'Entreprise et la Société)

9. Bibliography

Major publications by the team in recent years

[1] M. ABDALLA, M. BELLARE, D. CATALANO, E. KILTZ, T. KOHNO, T. LANGE, J. MALONE-LEE, G. NEVEN, P. PAILLIER, H. SHI. *Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions*, in "Journal of Cryptology", July 2008, vol. 21, n^{o} 3, p. 350–391.

[2] M. ABDALLA, C. CHEVALIER, D. POINTCHEVAL. *Smooth Projective Hashing for Conditionally Extractable Commitments*, in "Advances in Cryptology – Proceedings of CRYPTO '09", Lecture Notes in Computer Science, Springer, 2009, vol. 5677, p. 671–689.

[3] B. BLANCHET, D. POINTCHEVAL. *Automated Security Proofs with Sequences of Games*, in "Advances in Cryptology – Proceedings of CRYPTO '06", Lecture Notes in Computer Science, Springer, 2006, vol. 4117, p. 538–554.

[4] C. BOUILLAGUET, P. DERBEZ, P.-A. FOUQUE. *Automatic Search of Attacks on Round-Reduced AES and Applications*, in "Advances in Cryptology – Proceedings of CRYPTO '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6841, p. 169–187.

[5] C. DELERABLÉE, D. POINTCHEVAL. *Dynamic Threshold Public-Key Encryption*, in "Advances in Cryptology – Proceedings of CRYPTO '08", Lecture Notes in Computer Science, Springer, 2008, vol. 5157, p. 317–334.

[6] V. DUBOIS, P.-A. FOUQUE, A. SHAMIR, J. STERN. *Practical Cryptanalysis of SFLASH*, in "Advances in Cryptology – Proceedings of CRYPTO '07", Lecture Notes in Computer Science, Springer, 2007, vol. 4622, p. 1–12.

[7] P.-A. FOUQUE, G. LEURENT, PHONG Q. NGUYEN. *Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5*, in "Advances in Cryptology – Proceedings of CRYPTO '07", Lecture Notes in Computer Science, Springer, 2007, vol. 4622, p. 13–30.

[8] P.-A. FOUQUE, G. MACARIO-RAT, J. STERN. *Key Recovery on Hidden Monomial Multivariate Schemes*, in "Advances in Cryptology – Proceedings of EUROCRYPT '08", Lecture Notes in Computer Science, Springer, 2008, vol. 4965, p. 19–30.

[9] E. FUJISAKI, T. OKAMOTO, D. POINTCHEVAL, J. STERN. *RSA–OAEP is Secure under the RSA Assumption*, in "Journal of Cryptology", 2004, vol. 17, n^{o} 2, p. 81–104.

[10] N. GAMA, P. Q. NGUYEN. *Finding Short Lattice Vectors within Mordell's Inequality*, in "Proc. 40th ACM Symposium on the Theory of Computing (STOC '08)", ACM, 2008, p. 207–216.

[11] D. NACCACHE, N. P. SMART, J. STERN. *Projective Coordinates Leak*, in "Advances in Cryptology – Proceedings of EUROCRYPT '04", Lecture Notes in Computer Science, Springer, 2004, vol. 3027, p. 257–267.

[12] P. Q. NGUYEN, O. REGEV. *Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures*, in "J. Cryptology", 2009, vol. 22, n^{o} 2, p. 139–160.

[13] P. Q. NGUYEN, D. STEHLÉ. *An LLL Algorithm with Quadratic Complexity*, in "SIAM J. Comput.", 2009, vol. 39, n^{o} 3, p. 874-903.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[14] M. ABDALLA. *Reducing The Need For Trusted Parties In Cryptography*, Ecole normale supérieure, 2011, Habilitation, Ph. D. Thesis.

[15] C. BOUILLAGUET. *Etudes d'hypothèses algorithmiques et analyse de primitives cryptographiques*, Université Paris VII, 2011.

[16] M. TIBOUCHI. *Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA.*, Université Paris VII, 2011.

Articles in International Peer-Reviewed Journal

[17] M. ABDALLA, J. BIRKETT, D. CATALANO, A. W. DENT, J. MALONE-LEE, G. NEVEN, J. C. N. SCHULDT, N. P. SMART. *Wildcarded Identity-Based Encryption*, in "Journal of Cryptology", 2011, vol. 24, n^{o} 1, p. 42–82.

[18] E. BRIER, W. FANG, D. NACCACHE. *How to Scatter a Secret?*, in "Cryptologia", 2012, To appear.

[19] E. BRIER, D. NACCACHE, P. Q. NGUYEN, M. TIBOUCHI. *Modulus fault attacks against RSA-CRT signatures*, in "J. Cryptographic Engineering", 2011, vol. 1, n^{o} 3, p. 243-253.

[20] D. CATALANO, M. D. RAIMONDO, D. FIORE, M. MESSINA. *Zero-Knowledge Sets with Short Proofs*, in "IEEE Transactions on Information Theory.", 2011, vol. 57, n^{o} 4, p. 2488–2502.

[21] D. FIORE, R. GENNARO, N. SMART. *Relations between the security models for Certificateless Encryption and ID-Based Key Agreement*, in "International Journal of Information Security.", 2011, To appear..

[22] B. LIBERT, D. VERGNAUD. *Towards Practical Black-Box Accountable Authority IBE: Weak Black-Box Traceability with Short Ciphertexts and Private Keys*, in "IEEE Transactions on Information Theory", 2011, vol. 57, n^{o} 10, p. 7189-7204.

[23] B. LIBERT, D. VERGNAUD. *Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption*, in "IEEE Transactions on Information Theory", 2011, vol. 57, n^{o} 3, p. 1786-1802.

Articles in Non Peer-Reviewed Journal

[24] H. CHABANNE, M. TIBOUCHI. *Securing e-passports with elliptic curves*, in "IEEE Security and Privacy", 2011, vol. 9, n^{o} 2, p. 75-78.

International Conferences with Proceedings

[25] M. ABDALLA, C. CHEVALIER, L. GRANBOULAN, D. POINTCHEVAL. *Contributory Password-Authenticated Group Key Exchange with Join Capability*, in "The Cryptographers' Track at RSA Conference '11 (CT-RSA '11)", San Francisco, California, A. KIAYIAS (editor), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2011, vol. 6558, p. 142–160.

[26] A. AMARILLI, S. MÜLLER, D. NACCACHE, D. PAGE, P. RAUZY, M. TUNSTALL. *Can Code Polymorphism Limit Information Leakage?*, in "WISTP 2011", Lecture Notes in Computer Science, Springer, 2011, vol. 6633, p. 1-21.

[27] O. BLAZY, S. CANARD, G. FUCHSBAUER, A. GOUGET, H. SIBERT, J. TRAORÉ. *Achieving Optimal Anonymity in Transferable E-cash with a Judge*, in "Progress in Cryptology – AFRICACRYPT 2011", Lecture Notes in Computer Science, 2011, vol. 6737, p. 206–223.

[28] O. BLAZY, G. FUCHSBAUER, D. POINTCHEVAL, D. VERGNAUD. *Signatures on Randomizable Ciphertexts*, in "Conference on Practice and Theory in Public-Key Cryptography (PKC '11)", Taormina, Italy, D. CATALANO, N. FAZIO, R. GENNARO, A. NICOLOSI (editors), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2011, vol. 6571, p. 403–422.

[29] C. BOUILLAGUET, P. DERBEZ, P.-A. FOUQUE. *Automatic Search of Attacks on Round-Reduced AES and Applications*, in "CRYPTO", 2011, p. 169-187.

[30] C. BOUILLAGUET, J.-C. FAUGÈRE, P.-A. FOUQUE, L. PERRET. *Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial with One Secret Problem*, in "Public Key Cryptography", 2011, p. 473-493.

[31] E. BRIER, D. NACCACHE, P. Q. NGUYEN, M. TIBOUCHI. *Modulus Fault Attacks against RSA-CRT Signatures*, in "Proc. CHES '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6917, p. 192-206.

[32] H. BUHRMAN, O. REGEV, G. SCARPA, R. DE WOLF. *Near-Optimal and Explicit Bell Inequality Violations*, in "Proc. of 26th IEEE Annual Conference on Computational Complexity (CCC)", 2011, p. 157–166, arXiv:1012.5043.

[33] D. CATALANO, D. FIORE, B. WARINSCHI. *Adaptive Pseudo-Free Groups and Applications*, in "Proc. EUROCRYPT '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6632, p. 207–223.

[34] D. CATALANO, M. D. RAIMONDO, D. FIORE, R. GENNARO, O. PUGLISI. *Fully Non-Interactive Onion Routing with Forward-Secrecy*, in "ACNS 2011", Lecture Notes in Computer Science, Springer, 2011, vol. 6715, p. 255–273.

[35] A. CHAKRABARTI, O. REGEV. *An Optimal Lower Bound on the Communication Complexity of Gap Hamming Distance*, in "Proc. 43rd Annual ACM Symposium on the Theory of Computing", 2011, p. 51–60.

[36] T. CHARDIN, P.-A. FOUQUE, D. LERESTEUX. *Cache Timing Analysis of RC4*, in "ACNS", 2011, p. 110-129.

[37] Y. CHEN, P. Q. NGUYEN. *BKZ 2.0: Better Lattice Security Estimates*, in "Proc. ASIACRYPT '11", Lecture Notes in Computer Science, Springer, 2011.

[38] J.-S. CORON, A. JOUX, A. MANDAL, D. NACCACHE, M. TIBOUCHI. *Cryptanalysis of the RSA subgroup assumption from TCC 2005*, in "Proc. PKC '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6571, p. 147-155.

[39] J.-S. CORON, A. MANDAL, D. NACCACHE, M. TIBOUCHI. *Fully homomorphic encryption over the integers with shorter public keys*, in "Proc. CRYPTO '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6841, p. 487-504.

[40] P. DERBEZ, P.-A. FOUQUE, D. LERESTEUX. *Meet-in-the-Middle and Impossible Differential Fault Analysis on AES*, in "CHES", 2011, p. 274-291.

[41] B. HEMENWAY, B. LIBERT, R. OSTROVSKY, D. VERGNAUD. *Lossy Encryption: Constructions from General Assumptions and Efficient Selective Opening Chosen Ciphertext Security*, in "Advances in Cryptology -

Asiacrypt 2011", Seoul, South Korea, D. H. LEE, H. WANG (editors), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2011, to appear.

[42] M. IZABACHÈNE, B. LIBERT, D. VERGNAUD. *Block-wise P-Signatures and Non-Interactive Anonymous Credentials with Efficient Attributes*, in "Cryptography and Coding, 13th IMA International Conference", Oxford, UK, L. CHEN (editor), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2011, to appear.

[43] J. JEAN, P.-A. FOUQUE. *Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function*, in "FSE", 2011, p. 107–127.

[44] J. JEAN, P.-A. FOUQUE. *Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function*, in "FSE", 2011, p. 107-127.

[45] J. JEAN, M. NAYA-PLASENCIA, M. SCHLÄFFER. *Improved Analysis of ECHO-256*, in "Selected Area in Cryptography", 2011.

[46] B. KLARTAG, O. REGEV. *Quantum One-Way Communication can be Exponentially Stronger Than Classical Communication*, in "Proc. 43rd Annual ACM Symposium on the Theory of Computing", 2011, p. 31–40.

[47] P. Q. NGUYEN. *Lattice Reduction Algorithms: Theory and Practice*, in "Proc. EUROCRYPT '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6632, p. 2-6.

[48] D. H. PHAN, D. POINTCHEVAL, M. STREFLER. *Security Notions for Broadcast Encryption*, in "Conference on Applied Cryptography and Network Security (ACNS '11)", Nerja, Espagne, J. LOPEZ, G. TSUDIK (editors), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2011, vol. 6715, p. 377–394.

[49] D. H. PHAN, V. C. TRINH. *Identity-Based Trace and Revoke Schemes*, in "Conference on Provable Security (ProvSec '11)", Xian, China, X. BOYEN, X. CHEN (editors), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2011, vol. 6980, p. 204–221.

[50] D. VERGNAUD. *Efficient and Secure Generalized Pattern Matching via Fast Fourier Transform*, in "Progress in Cryptology - AFRICACRYPT 2011", Dakar, Sénégal, A. NITAJ, D. POINTCHEVAL (editors), Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2011, vol. 6737, p. 41–58.

Conferences without Proceedings

[51] B. BLANCHET. *A second look at Shoup's lemma*, in "Workshop on Formal and Computational Cryptography (FCC 2011)", Paris, France, June 2011.

Scientific Books (or Scientific Book chapters)

[52] B. BLANCHET. *Mechanizing Game-Based Proofs of Security Protocols*, in "Tools for Analysis and Verification of Software Safety and Security", O. GRUMBERG, T. NIPKOW, J. ESPARZA (editors), NATO Science for Peace and Security Series – D: Information and Communication Security, IOS Press, 2011, Proceedings of the 2011 MOD summer school. To appear.

[53] B. BLANCHET. *Using Horn Clauses for Analyzing Security Protocols*, in "Formal Models and Techniques for Analyzing Security Protocols", V. CORTIER, S. KREMER (editors), Cryptology and Information Security Series, IOS Press, March 2011, vol. 5, p. 86–111.

[54] D. NACCACHE, E. SIMION, A. MIHĂIŢĂ, R.-F. OLIMID, A.-G. OPRINA. *Criptografie si securitatea informatiei. Aplicatii.*, 1st, 107 pages, Matrix Rom, 2011.

[55] D. NACCACHE. *Entries in the Encyclopedia of Cryptography and Security: Phenotyping , Naccache-Stern Higher Residues Cryptosystem, Multiplicative Knapsack Cryptosystem, Monotone Signatures, Barrett's Algorithm, Autotomic Signatures, Gröbner Basis, Generic Model, Cryptophthora, Chemical Combinatorial Attack, Reverse Public Key Encryption, von Neumann Correction, Standard Model, Blackmailing Attacks, Twin Signatures, Temperature Attack*, 2011.

[56] E. SIMION, M. ANDRAŞIU, D. NACCACHE, G. SIMION. *Cercetări operaţionale,probabilităţi si criptologie. Aplicatii.*, 1st, 292 pages, Editura Academiei Tehnice Militare, 2011.

Books or Proceedings Editing

[57] L. BREVEGLIERI, S. GUILLEY, I. KOREN, D. NACCACHE, J. TAKAHASHI (editors). *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011*, IEEE, Tokyo, Japan, September 29, 2011, 2011.

[58] D. NACCACHE (editor). *Festschrift for Jean-Jacques Quisquater*, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2012, vol. 6805, To appear.

[59] A. NITAJ, D. POINTCHEVAL (editors). *The Fourth International Conference on Cryptology in Africa (AFRICACRYPT '11)*, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Dakar, Senegal, 2011, vol. 6737.

References in notes

[60] M. AJTAI. *Generating Hard Instances of Lattice Problems (Extended Abstract)*, in "28th Annual ACM Symposium on Theory of Computing", ACM Press, 1996, p. 99–108.

[61] M. BELLARE. *Practice-Oriented Provable-Security (Invited Lecture)*, in "ISC '97: 1st International Workshop on Information Security", E. OKAMOTO, G. I. DAVIDA, M. MAMBO (editors), Lecture Notes in Computer Science, Springer, 1997, vol. 1396, p. 221–231.

[62] M. BELLARE, D. POINTCHEVAL, P. ROGAWAY. *Authenticated Key Exchange Secure against Dictionary Attacks*, in "Advances in Cryptology – EUROCRYPT '00", Lecture Notes in Computer Science, Springer, 2000, vol. 1807, p. 139–155.

[63] M. BELLARE, P. ROGAWAY. *The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs*, in "Advances in Cryptology – EUROCRYPT '06", Lecture Notes in Computer Science, Springer, 2006, vol. 4004, p. 409–426.

[64] M. BELLARE, P. ROGAWAY. *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, in "ACM CCS '93: 1st Conference on Computer and Communications Security", ACM Press, 1993, p. 62–73.

[65] M. BELLARE, P. ROGAWAY. *The Exact Security of Digital Signatures: How to Sign with RSA and Rabin*, in "Advances in Cryptology – EUROCRYPT '96", Lecture Notes in Computer Science, Springer, 1996, vol. 1070, p. 399–416.

[66] E. BIHAM, R. CHEN, A. JOUX, P. CARRIBAULT, C. LEMUET, W. JALBY. *Collisions of SHA-0 and Reduced SHA-1.*, in "Advances in Cryptology – EUROCRYPT '05", Lecture Notes in Computer Science, Springer, 2005, vol. 3494, p. 36–57.

[67] D. R. L. BROWN. *The Exact Security of ECDSA*, January 2001, Contributions to IEEE P1363a, http://grouper.ieee.org/groups/1363/.

[68] B. CHOR, R. L. RIVEST. *A Knapsack Type Public Key Cryptosystem Based On Arithmetic in Finite Fields*, in "Advances in Cryptology – CRYPTO '84", Lecture Notes in Computer Science, Springer, 1985, vol. 196, p. 54–65.

[69] W. DIFFIE, M. E. HELLMAN. *New Directions in Cryptography*, in "IEEE Transactions on Information Theory", 1976, vol. 22, n^{o} 6, p. 644–654.

[70] A. FIAT, A. SHAMIR. *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, in "Advances in Cryptology – CRYPTO '86", Lecture Notes in Computer Science, Springer, 1987, vol. 263, p. 186–194.

[71] E. FUJISAKI, T. OKAMOTO, D. POINTCHEVAL, J. STERN. *RSA–OAEP is Secure under the RSA Assumption*, in "Journal of Cryptology", 2004, vol. 17, n^{o} 2, p. 81–104.

[72] L. LAMPORT. *Constructing Digital Signatures from a One-Way Function*, SRI Intl., 1979, n^{o} CSL 98.

[73] NIST. *Descriptions of SHA–256, SHA–384, and SHA–512*, October 2000, Federal Information Processing Standards PUBlication 180–3, http://www.nist.gov/sha/.

[74] NIST. *Secure Hash Standard (SHS)*, April 1993, Federal Information Processing Standards PUBlication 180, Draft.

[75] NIST. *Secure Hash Standard (SHS)*, April 1995, Federal Information Processing Standards PUBlication 180–1.

[76] V. I. NECHAEV. *Complexity of a Determinate Algorithm for the Discrete Logarithm*, in "Mathematical Notes", 1994, vol. 55, n^{o} 2, p. 165–172.

[77] K. OHTA, T. OKAMOTO. *On Concrete Security Treatment of Signatures Derived from Identification*, in "Advances in Cryptology – CRYPTO '98", Lecture Notes in Computer Science, Springer, 1998, vol. 1462, p. 354–369.

[78] D. POINTCHEVAL. *Provable Security for Public-Key Schemes*, Advanced Courses CRM Barcelona, Birkhauser Publishers, Basel, June 2005, p. 133–189, ISBN: 3-7643-7294-X (248 pages).

[79] R. L. RIVEST. *The MD4 Message-Digest Algorithm*, April 1992, RFC 1320, The Internet Engineering Task Force.

[80] R. L. RIVEST. *The MD5 Message-Digest Algorithm*, April 1992, RFC 1321, The Internet Engineering Task Force.

[81] P. SHOR. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, in "SIAM J. on Computing", 1997, vol. 26, n^{o} 5, p. 1484–1509.

[82] V. SHOUP. *Sequences of games: a tool for taming complexity in security proofs*, 2004, Cryptology ePrint Archive 2004/332.

[83] V. SHOUP. *Lower Bounds for Discrete Logarithms and Related Problems*, in "Advances in Cryptology – EUROCRYPT '97", Lecture Notes in Computer Science, Springer, 1997, vol. 1233, p. 256–266.

[84] S. VAUDENAY. *Cryptanalysis of the Chor-Rivest Cryptosystem*, in "Advances in Cryptology – CRYPTO '98", Lecture Notes in Computer Science, Springer, 1998, vol. 1462, p. 243–256.

[85] X. WANG, X. LAI, D. FENG, H. CHEN, X. YU. *Cryptanalysis of the Hash Functions MD4 and RIPEMD*, in "Advances in Cryptology – EUROCRYPT '05", Lecture Notes in Computer Science, Springer, 2005, vol. 3494, p. 1–18.

[86] X. WANG, Y. L. YIN, H. YU. *Finding Collisions in the Full SHA-1*, in "Advances in Cryptology – CRYPTO '05", Lecture Notes in Computer Science, Springer, 2005, vol. 3621, p. 17–36.

[87] X. WANG, H. YU. *How to Break MD5 and Other Hash Functions*, in "Advances in Cryptology – EUROCRYPT '05", Lecture Notes in Computer Science, Springer, 2005, vol. 3494, p. 19–35.

[88] X. WANG, H. YU, Y. L. YIN. *Efficient Collision Search Attacks on SHA-0*, in "Advances in Cryptology – CRYPTO '05", Lecture Notes in Computer Science, Springer, 2005, vol. 3621, p. 1–16.

[89] H. YU, X. WANG, A. YUN, S. PARK. *Cryptanalysis of the Full HAVAL with 4 and 5 Passes*, in "FSE '06", Lecture Notes in Computer Science, Springer, 2006, vol. 4047, p. 89–110.

[90] H. YU, G. WANG, G. ZHANG, X. WANG. *The Second-Preimage Attack on MD4*, in "CANS '05", Lecture Notes in Computer Science, Springer, 2005, vol. 3810, p. 1–12.