INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team cascade

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

Paris - Rocquencourt

Theme : Algorithms, Certification, and Cryptography

Table of contents

1. Team

Research Scientist

Michel Ferreira Abdalla [CR, CNRS]
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 Member

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]
Jean Vuillemin [Professor, ENS, HdR]

PhD Student

Olivier Blazy [University Paris 7 grant]
Charles Bouillaguet [Fondation EADS grant]
David Cadé [AMN grant]
Yuanmi Chen [AMN grant]
Patrick Derbez [AMN grant]
Léo Ducas [AMN grant]
Georg Fuchsbauer [EADS grant]
Jérémy Jean [ANR & DGA grant]
Gaëtan Leurent [DGA grant]
Mario Strefler [INRIA]
Miriam Paiola [INRIA]
Mehdi Tibouchi [NTT & ANR grant]

Post-Doctoral Fellow

Aurélie Bauer [Teaching Assistant, ENS]
Dario Fiore [ANR grant]
Jiqiang Lu [ANR grant]

Administrative Assistant

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

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. Design and provable security, for
   - signature schemes
   - public-key encryption schemes
   - identity-based encryption schemes
   - key agreement protocols
   - group-oriented protocols
2. Attacks, using
   - side-channels
   - algebraic techniques
3. 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 [64], 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 [63], based on the knapsack problem, which took more than 10 years to be totally broken [79], 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) [67], 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" [60] or "concrete security" [72], 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" [56]. 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 [65], and later formalized by Bellare and Rogaway [59]. Similarly, block ciphers are identified with families of truly random permutations in the "ideal cipher model" [57]. 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" [71], [78]. Some works even require several ideal models together to provide some new validations [62].

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 [77], [58], [73] which highlights the computational assumptions, and splits the analysis in small independent problems. We early adopted and developed this technique, and namely in [66].

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 [75], [74], [69], [70], [68], 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 [59]). Recently, a bunch of attacks [61], [80], [81], [82], [83], [85], [84] 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 [55] showed that, up to that point, lattices were used only as tools in cryptanalysis, but they could actually be used to construct cryptographic primitives. He indeed proposed a cryptographic primitive which 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 nice property makes lattice-based cryptographic constructions very attractive. In contrast, virtually all other cryptographic constructions are based on some average-case assumption. Furthermore, we currently do not have too many 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. In fact, efficient quantum algorithms for factoring integers and computing discrete logarithms already exist [76]. Although large-scale quantum computers are not expected to exist for at least a decade, this fact should already be regarded as a warning. There are currently no known quantum algorithms for lattice problems, which makes these problems very hard to solve. In addition, the computations involved in lattice-based cryptography are very simple and often require only modular additions, which make them efficient for users.

For all these reasons, lattice-based cryptography has recently become a hot topic, and we started to work on it.

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. ProVerif

Participant: Bruno Blanchet.

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.

5.2. CryptoVerif

Participant: Bruno Blanchet.

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. Contracts 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, Gaëtan Leurent, Jiqiang Lu.

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

- **SAVE** *(Sécurité et Audit du Vote Electronique)*
  Security and audit for electronic voting.
  Participants: Dario Fiore, David Pointcheval.

  From December 2006 to June 2010.
  Partners: France Telecom R&D, GET/ENST, GET/INT, Supélec, Cryptolog.
  *This project extends an earlier **Crypto++** project, but for electronic voting only, and at a larger scale: not only the security at the cryptographic level will be considered (validity of the computations, correctness of the ballot, anonymity, etc) but also at the network level (infrastructure, etc).*

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

  From December 2007 to November 2011.
  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 November 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.

- **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.

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

7. Other Grants and Activities

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)

7.2. Grants

- **Chaire ENS – France Télécom pour la sécurité des réseaux de télécommunications.**
  From January 2006 to December 2010.
- **EADS Grant.**
  Georg Fuchsbauer, in PhD Thesis from January 2007 to December 2010
- **Fondation EADS Grant.**
  Charles Bouillaguet, in PhD Thesis from September 2008 to August 2011
- **PhD DGA Grant.**
  Gaëtan Leurent, in PhD Thesis from October 2007 to September 2010

7.3. Exterior Research Visitors

- Igor Shparlinski – Macquarie Univ., – Australia
- Orr Dunkelman – Weizmann Inst., Rehovot, Israel
- Angelo De Caro – Univ. Salerno, Italy
- Ronald de Wolf – CWI, The Netherlands
- Masaya Yasuda – Fujitsu Labs, Kawasaki, Japan

8. Dissemination

8.1. Editorial Boards

Editor-in-Chief

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

Managing Editor

– of the *Theory of Computing (ToC)* – ACM SIGACT: 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 *IET - Information Security*: David Naccache
– of *IEEE Security and Privacy*: David Naccache
– of *ACM Transactions on Information and System Security*: David Naccache
– of *Computers & Security Elsevier Advanced Technology* – Elsevier: David Naccache
– of *Cryptologia* – Taylor & Francis: David Naccache
– of *Information Processing Letters* – Elsevier: David Pointcheval

8.2. Program Committees

- FC – January 2010, Tenerife, Canary Islands, Spain: David Naccache, David Pointcheval
- TCC – February 2010, Zurich, Switzerland: Phong Nguyen
- COSADE – February 2010, Darmstadt, Germany: David Naccache
- TACAS – March 2010, Paphos, Cyprus: Bruno Blanchet
- AFRICACRYPT – May 2010, Stellenbosch, South Africa: Michel Abdalla
- CryptoForma workshop – May 2010, Paris France: Bruno Blanchet
- PKC – May 2010, Paris, France: Phong Nguyen (Program co-Chair), David Pointcheval (Program co-Chair), Damien Vergnaud
- EUROCRYPT – June 2010, Monaco: David Pointcheval
- ISCC – June 2010, Riccione, Italy: David Naccache
- HOST – June 2010, Anaheim, CA USA: David Naccache
- ACISP – July 2010, Sydney, Australia: Michel Abdalla, Damien Vergnaud
- CSF – July 2010, Edimburgh, United Kingdom: Bruno Blanchet
- LATINCRYPT – August 2010, Puebla, Mexico: Michel Abdalla (Program Chair), Damien Vergnaud
- SAC – August 2010, Waterloo, Ontario Canada: David Naccache
- CRYPTO – August 2010, Santa-Barbara, CA, USA: Michel Abdalla
- CHES – August 2010, Santa-Barbara, CA, USA: Pierre-Alain Fouque
- SCN – September 2010, Amalfi, Italy: David Naccache
- ProvSec – October 2010, Malacca, Malaysia: David Naccache
- YACC – October 2010, Porquerolles Island, France: David Pointcheval, Damien Vergnaud
- CCS – November 2010, Chicago, IL, USA: Bruno Blanchet
- IWSEC – November 2010, Kobe, Japan: Phong Nguyen

- ICISC – December 2010, Seoul, Korea: David Naccache
- ASIACRYPT – December 2010, Singapore: Phong Nguyen
- CANS – December 2010, Kuala Lumpur, Malaysia: Michel Abdalla, David Pointcheval
- PAIRING – December 2010, Yamanaka Hot Spring, Japan: Michel Abdalla

8.3. Teaching

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

M1 – Introduction to Cryptology (EPITA): Phong Nguyen

M2 – Cryptanalysis (MPRI): Pierre-Alain Fouque, Phong Nguyen

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

M2 – Synchronous Systems (MPRI): Jean Vuillemin

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

M2 – Cryptography (ESIEA): David Pointcheval

8.4. Ph.D/Habilitation Defenses

- Gaëtan Leurent – Ph.D. – 30 sept. 2010 – Université Paris VII – France
  Construction et analyse de fonctions de hachage [15]
- Georg Fuchsbauer – Ph.D. – 13 oct. 2010 – Université Paris VII – France
  Signatures Automorphes et Applications [14]
- Pierre-Alain Fouque – HDR – 10 dec. 2010 – ENS – France
  Sur Quelques Méthodes Algébriques et Statistiques en Cryptanalyse [13]

8.5. Ph.D/Habilitation Committees

- Markulf Kohlweiss – Ph.D. – 3 feb. 2010 – KUL – Belgium
  Privacy Enhancing Protocols for Identity Management
  David Pointcheval (reviewer)
- Choudary Gorantla – Ph.D. – 18 mar. 2010 – Queensland University of Technology – Australia
  Design and Analysis of Group Key Exchange Protocols
  Michel Abdalla (reviewer)
- Joana Treger – Ph.D. – 28 jun 2010 – Université de Versailles Saint-Quentin-en-Yvelines – France
  Etude de la Sécurité de Schémas de Chiffrement par Bloc et de Schémas Multivariés
  Pierre-Alain Fouque, David Naccache (reviewer)
- Gilles Macario-Rat – Ph.D. – 28 jun 2010 – Université Paris VII – France
  Cryptanalyse de schémas multivariés et résolution du problème Isomorphisme de Polynômes
  Pierre-Alain Fouque (co-supervisor), Jacques Stern (co-superviser)
- Léonard Dallot – Ph.D. – 15 jul. 2010 – Université de Caen – France
  Sécurité de protocoles cryptographiques fondés sur les codes correcteurs d'erreurs
  Damien Vergnaud
- Gaëtan Leurent – Ph.D. – 30 sept. 2010 – Université Paris VII – France
  Construction et analyse de fonctions de hachage
  Pierre-Alain Fouque (co-supervisor), David Pointcheval (co-superviser)
- Georg Fuchsbauer – Ph.D. – 13 oct. 2010 – Université Paris VII – France
  Signatures Automorphes et Applications
  David Pointcheval (supervisor), Jacques Stern (chair)

- Stéphane Manuel – Ph.D. – 23 nov. 2010 – École polytechnique – France
  Analyse et conception de fonctions de hachage cryptographiques
  Pierre-Alain Fouque (reviewer)
- Iordanis Kerenidis – HDR – 3 dec. 2010 – Université Paris–Sud – France
  Interaction in the Quantum World
  Phong Nguyen, Oded Regev (reviewer)
- Santiago Zanella – Ph.D. – 9 dec. 2010 – Mines de Paris – France
  Certification formelle de preuves cryptographiques basées sur le langage
  David Pointcheval (reviewer)
- Pierre-Alain Fouque – HDR – 10 dec. 2010 – ENS – France
  Sur Quelques Méthodes Algébriques et Statistiques en Cryptanalyse
  David Pointcheval, Jacques Stern (supervisor)
- Alexandre Karlov – Ph.D. – 21 dec. 2010 – EPFL – Switzerland
  Broadcast Encryption and Traitor Tracing for Conditional Access Systems
  David Pointcheval (reviewer)

8.6. Invited Talks

- Franco-Japanese CosyProof Workshop, Barbizon, France (April): Bruno Blanchet, David Pointcheval
- Colloque "Algorithmique et Programmation", Luminy, France (May): Phong Nguyen
- CryptoForma workshop, Paris, France (May): Bruno Blanchet, Dario Fiore
- SecReT, Valencia, Spain (June): Bruno Blanchet
- Summer School on Applied Cryptographic Protocols, Mykonos, Greece (September): Michel Abdalla
- Workshop on Post-Quantum Security Models, Paris, France (October): Phong Nguyen
- Chinacrypt, Beijing, China (October): David Pointcheval
- Basque Colloquim in Mathematics and its Applications, Bilbao, Spain (December): Phong Nguyen

8.7. Invitations

- Invited Professor, Dakar, Senegal, 13-20 June: Damien Vergnaud
- Tsinghua Univ., Beijing, China, 17-20 October: David Pointcheval
- Invited Researcher, Bangalore, India, 3-13 November: Damien Vergnaud
- Tsinghua Univ., Beijing, China, 8-12 November: Phong Nguyen

8.8. Seminar Presentations

- Technische Universität Darmstadt, Germany (January): Aurélie Bauer
- Université du Luxembourg, Luxembourg (January): Gaëtan Leurent
- University College London, UK (March): Georg Fuchsbauer
- Queensland University of Technology, Brisbane, Australia (March): Michel Abdalla
- Tokyo Univ., Tokyo, Japan (March): Phong Nguyen
- Université du Luxembourg (April): Georg Fuchsbauer
- University of Padova, Italy (May): Bruno Blanchet
- Séminaire de Recherche SURI, EPFL (June): Pierre-Alain Fouque

- Microsoft Research-INRIA Joint Centre, France (June): Miriam Paiola
- CWI, Amsterdam, The Netherlands (July): Michel Abdalla
- East China Normal Univ., Shanghai, China (July): Phong Nguyen
- ENPC, Marne la Vallée, France (September): David Pointcheval
- Tsinghua Univ., Beijing, China (October): David Pointcheval
- CCA, Paris, France (October): Damien Vergnaud
- NICT, Tokyo, Japan (October): Phong Nguyen
- Tsinghua Univ., Beijing, China (November): Phong Nguyen
- Technische Universität München, Germany (December): Bruno Blanchet
- NEC Labs, Tokyo, Japan (December) : Phong Nguyen

8.9. Participation to Workshops and Conferences

ESC – January 2010, Luxembourg: Pierre-Alain Fouque, Gaëtan Leurent

TCC – February 2010, Zurich, Switzerland: Michel Abdalla, Georg Fuchsbauer

FSE – February 2010, Seoul, South Korea: Pierre-Alain Fouque, Gaëtan Leurent

CT-RSA – March 2010, San Francisco, Calofornia, USA: Léo Ducas, Gaëtan Leurent, Mehdi Tibouchi

Franco-Japanese CosyProof Workshop – April 2010, Barbizon, France: Bruno Blanchet, David Cadé, Miriam Paiola, David Pointcheval

CSC – April 2010, Montreal, Canada: Damien Vergnaud

Africacrypt – May 2010, Stellenbosch, South Africa: Georg Fuchsbauer

CryptoForma workshop – May 2010, Paris, France: Bruno Blanchet, David Cadé

PKC – May 2010, Paris, France: Michel Abdalla, Aurélie Bauer, Olivier Blazy, Charles Bouillaguet, David Cadé, Yuanmi Chen, Patrick Derbez, Léo Ducas, Dario Fiore, Pierre-Alain Fouque, Georg Fuchsbauer, Jérémy Jean, David Naccache, Phong Nguyen, David Pointcheval, Jacques Stern, Mario Strefler, Mehdi Tibouchi, Damien Vergnaud

Eurocrypt – June 2010, Monaco: Aurélie Bauer, Charles Bouillaguet, David Cadé, Yuanmi Chen, Patrick Derbez, Dario Fiore, Georg Fuchsbauer, Jérémy Jean, David Naccache, Miriam Paiola, David Pointcheval, Jacques Stern, Mario Strefler

SecReT – June 2010, Valencia, Spain: Bruno Blanchet

ACNS – June 2010, Beijing, China: Olivier Blazy, Mehdi Tibouchi

SCC – July 2010, London, UK: Charles Bouillaguet

CSF – July 2010, Edinburgh, UK: Bruno Blanchet, David Cadé, Miriam Paiola

FCC – July 2010, Edinburgh, UK: Bruno Blanchet, David Cadé, Miriam Paiola

ASA – July 2010, Edinburgh, UK: Bruno Blanchet

ANTS – July 2010, Nancy, France: Mehdi Tibouchi

Latincrypt – August 2010, Puebla, Mexico: Michel Abdalla, Mehdi Tibouchi, Damien Vergnaud

SAC – August 2010, Waterloo, Canada: Gaëtan Leurent

Crypto – August 2010, Santa-Barbara, California, USA: Michel Abdalla, Charles Bouillaguet, Pierre-Alain Fouque, Georg Fuchsbauer, Gaëtan Leurent, Phong Nguyen, Mehdi Tibouchi, Jacques Stern

2nd SHA-3 Conference – August 2010, Santa Barbara, California, USA: Gaëtan Leurent

CHES – August 2010, Santa-Barbara, California, USA: Charles Bouillaguet

SAS – September 2010, Perpignan, France: Miriam Paiola

European Cryptography Day – September 2010, Leuven: Michel Abdalla, Dario Fiore

Chinacrypt – October 2010, Beijing, China: David Pointcheval

IWSEC – November 2010, Kobe, Japan: Phong Nguyen

Colloque ANR "Télécommunications - Réseaux du futur et Services" – December 2010, Rennes, France: Bruno Blanchet

CRISMATH – December 2010, Tokyo, Japan: Mehdi Tibouchi

IWSEC – November 2010, Kobe, Japan: Phong Nguyen

Pairing – December 2010, Ishikawa, Japan: Dario Fiore, Medhi Tibouchi, Phong Nguyen

Asiacrypt – December 2010, Singapore: Jérémy Jean, Jacques Stern, Damien Vergnaud

8.10. Scientific Animation

8.10.1. Organisation of Events

- the CASCADE project-team organized the 13th Internal Conference on Practice and Theory of Public Key Cryptography (PKC 2010), in May 2010
- we organized the Lattice Crypto Day, in May 2010
- a weekly seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html

8.10.2. Board of International Organizations

- Chairs of the Program Committee of PKC – Phong Nguyen and David Pointcheval
- General Chairs of PKC – Michel Abdalla and Pierre-Alain Fouque
- Chairs of the Program Committee of Latincrypt – Michel Abdalla
- Board of the *International Association for Cryptologic Research* (IACR) – David Naccache (2010 – 2012), David Pointcheval (2008–2013)
- International Scientific Advisory Board of National ICT Australia – Jean Vuillemin (2008–2011)
- Chair of the Scientific Advisory Board of the Institute for Infocomm Research I2R in Singapore – Jean Vuillemin (2008–2010)

8.10.3. French Research Community

- Recruitment committee at ENS: Jean Vuillemin, Pierre-Alain Fouque
- Recruitment committee at VERIMAG: Bruno Blanchet
- Recruitment committee at Université du Sud Toulon-Var: Damien Vergnaud
- Foreign student recruitment committee at ENS: Damien Vergnaud
- INRIA Paris-Rocquencourt seminar committee: Phong Nguyen

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. 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

Year Publications

Doctoral Dissertations and Habilitation Theses

[13] P.-A. FOUQUE. *Sur Quelques Méthodes Algébriques et Statistiques en Cryptanalyse*, Ecole normale supérieure, 2010, Habilitation, Ph. D. Thesis.

[14] G. FUCHSBAUER. *Signatures Automorphes et Applications*, Université Paris VII, 2010, Ph. D. Thesis.

[15] G. LEURENT. *Construction et analyse de fonctions de hachage*, Université Paris VII, 2010, Ph. D. Thesis.

Articles in International Peer-Reviewed Journal

[16] D. CATALANO, M. D. RAIMONDO, D. FIORE, M. MESSINA. *Zero-Knowledge Sets with Short Proofs*, in "IEEE Transactions on Information Theory.", 2010, To appear.

[17] D. FIORE, R. GENNARO. *Identiy-Based Key-Exchange Protocols without Pairings.*, in "Transactions on Computational Science XI. Special Issue on Security in Computing, Part I.", 2010, vol. 6340, p. 42–77, To appear.

[18] F. LAGUILLAUMIE, D. VERGNAUD. *Time-selective convertible undeniable signatures with short conversion receipts*, in "Inf. Sci.", 2010, vol. 180, n^{o} 12, p. 2458-2475.

[19] B. LIBERT, D. VERGNAUD. *Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption*, in "IEEE Transactions on Information Theory", 2010, to appear.

International Peer-Reviewed Conference/Proceedings

[20] M. ABDALLA, M. BELLARE, G. NEVEN. *Robust Encryption*, in "Seventh Theory of Cryptography Conference (TCC 2010)", Lecture Notes in Computer Science, Springer, 2010, vol. 5978, p. 480–497.

[21] M. ABDALLA, C. CHEVALIER, M. MANULIS, D. POINTCHEVAL. *Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys*, in "Third African International Conference on Cryptology (AfricaCrypt '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6055, p. 351–368.

[22] M. ABE, G. FUCHSBAUER, J. GROTH, K. HARALAMBIEV, M. OHKUBO. *Structure-Preserving Signatures and Commitments to Group Elements*, in "Advances in Cryptology – Proceedings of CRYPTO '10", Lecture Notes in Computer Science, Springer, 2010, vol. 6223, p. 209-236.

[23] M. AGOYAN, J.-M. DUTERTRE, D. NACCACHE, B. ROBISSON, A. TRIA. *When Clocks Fail: On Critical Paths and Clock Faults*, in "Smart Card Research and Advanced Application, International Conference (CARDIS 2010)", Lecture Notes in Computer Science, Springer, 2010, vol. 6035, p. 182-193.

[24] M. BARNI, T. BIANCHI, D. CATALANO, M. D. RAIMONDO, R. D. LABATI, P. FAILLA, D. FIORE, R. LAZZERETTI, V. PIURI, F. SCOTTI. *A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercode Templates*, in "IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems.", IEEE, 2010, p. 1-7.

[25] M. BARNI, T. BIANCHI, D. CATALANO, M. D. RAIMONDO, R. D. LABATI, P. FAILLA, D. FIORE, R. LAZZERETTI, V. PIURI, F. SCOTTI. *Privacy-Preserving Fingercode Authentication*, in "12th ACM Workshop on Multimedia and Security (ACM MM&Sec 2010).", ACM, 2010, p. 231–241.

[26] A. BAUER, J.-S. CORON, D. NACCACHE, M. TIBOUCHI, D. VERGNAUD. *On the Broadcast and Validity-Checking Security of PKCS#1 v1.5 Encryption*, in "Applied Cryptography and Network Security, 8th International Conference, ACNS 2010", Lecture Notes in Computer Science, Springer, 2010, vol. 6123, p. 1-18.

[27] O. BLAZY, G. FUCHSBAUER, M. IZABACHÈNE, A. JAMBERT, H. SIBERT, D. VERGNAUD. *Batch Groth-Sahai*, in "Applied Cryptography and Network Security, 8th International Conference, ACNS 2010", Lecture Notes in Computer Science, Springer, 2010, vol. 6123, p. 218-235.

[28] C. BOUILLAGUET, H.-C. CHEN, C.-M. CHENG, T. CHOU, R. NIEDERHAGEN, A. SHAMIR, B.-Y. YANG. *Fast Exhaustive Search for Polynomial Systems in F_2*, in "Cryptographic Hardware and Embedded Systems (CHES 2010)", Lecture Notes in Computer Science, Springer, 2010, vol. 6225, p. 203–218.

[29] C. BOUILLAGUET, O. DUNKELMAN, G. LEURENT, P.-A. FOUQUE. *Another Look at Complementation Properties*, in "Fast Software Encryption (FSE 2010)", Lecture Notes in Computer Science, Springer, 2010, vol. 6147, p. 347–364.

[30] C. BOUILLAGUET, O. DUNKELMAN, G. LEURENT, P.-A. FOUQUE. *Attacks on Hash Functions based on Generalized Feistel – Application to Reduced-Round Lesamnta and Shavite-3 512*, in "Selected Areas in Crypgraphy (SAC 2010)", Lecture Notes in Computer Science, Springer, 2010, To appear.

[31] C. BOUILLAGUET, G. LEURENT, P.-A. FOUQUE. *Security Analysis of SIMD*, in "Selected Areas in Crypgraphy (SAC 2010)", Lecture Notes in Computer Science, Springer, 2010, To appear.

[32] X. BOYEN, C. CHEVALIER, G. FUCHSBAUER, D. POINTCHEVAL. *Strong Cryptography from Weak Secrets - Building Efficient PKE and IBE from Distributed Passwords*, in "Third African International Conference on Cryptology (AfricaCrypt '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6055, p. 297–315.

[33] E. BRIER, J.-S. CORON, T. ICART, D. MADORE, H. RANDRIAM, M. TIBOUCHI. *Efficient Indifferentiable Hashing into Ordinary Elliptic Curves*, in "30th Annual Cryptology Conference (CRYPTO '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6223, p. 237–254.

[34] B. CHEVALLIER-MAMES, J.-S. CORON, N. MCCULLAGH, D. NACCACHE, M. SCOTT. *Secure Delegation of Elliptic-Curve Pairing*, in "Smart Card Research and Advanced Application, International Conference (CARDIS 2010)", Lecture Notes in Computer Science, Springer, 2010, vol. 6035, p. 24-35.

[35] J.-S. CORON, D. NACCACHE, M. TIBOUCHI. *Fault attacks against EMV signatures*, in "The Cryptographers' Track at the RSA Conference (CT-RSA '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 5985, p. 208–220.

[36] D. FIORE, R. GENNARO, N. P. SMART. *Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key-Agreement*, in "Pairing-Based Cryptography - Pairing 2010", Lecture Notes in Computer Science, Springer, 2010, vol. 6487, p. 167–186.

[37] P.-A. FOUQUE, M. TIBOUCHI. *Deterministic Encoding and Hashing to Odd Hyperelliptic Curves*, in "Fourth International Conference on Pairing-based Cryptography (Pairing '10)", Lecture Notes in Computer Science, Springer, 2010, To appear.

[38] P.-A. FOUQUE, M. TIBOUCHI. *Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves*, in "First International Conference on Cryptology and Information Security (LatinCrypt '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6212, p. 81–91.

[39] G. FUCHSBAUER, J. KATZ, D. NACCACHE. *Efficient Rational Secret Sharing in Standard Communication Networks*, in "7th Theory of Cryptography Conference (TCC '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 5978, p. 419–436.

[40] G. FUCHSBAUER, D. VERGNAUD. *Fair Blind Signatures without Random Oracles*, in "Progress in Cryptology - AFRICACRYPT 2010", Lecture Notes in Computer Science, Springer, 2010, vol. 6055, p. 16-33.

[41] D. GALINDO, B. LIBERT, M. FISCHLIN, G. FUCHSBAUER, A. LEHMANN, M. MANULIS, D. SCHRÖDER. *Public-Key Encryption with Non-Interactive Opening: New Constructions and Stronger Definitions*, in "Third African International Conference on Cryptology (AfricaCrypt '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6055, p. 333-350.

[42] N. GAMA, P. Q. NGUYEN, O. REGEV. *Lattice Enumeration Using Extreme Pruning*, in "Advances in Cryptology – Proceedings of EUROCRYPT '10", Lecture Notes in Computer Science, Springer, 2010, vol. 6110, p. 257-278.

[43] P. GAURAVARAM, G. LEURENT, F. MENDEL, M. NAYA-PLASENCIA, T. PEYRIN, C. RECHBERGER, M. SCHÄFFER. *Cryptanalysis of the 10-Round Hash and Full Compression Function of Shavite-3-512*, in "Third African International Conference on Cryptology (AfricaCrypt '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6055, p. 419–436.

[44] M. IZABACHÈNE, D. POINTCHEVAL, D. VERGNAUD. *Mediated Traceable Anonymous Encryption*, in "First International Conference on Cryptology and Information Security (LatinCrypt '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6212, p. 40–60.

[45] M. JOYE, D. NACCACHE, S. PORTE. *The Polynomial Composition Problem in (Z/Z)[]*, in "Smart Card Research and Advanced Application, International Conference (CARDIS 2010)", Lecture Notes in Computer Science, Springer, 2010, vol. 6035, p. 1-12.

[46] M. JOYE, M. TIBOUCHI, D. VERGNAUD. *Huff's Model for Elliptic Curves*, in "Algorithmic Number Theory, 9th International Symposium, ANTS-IX", Lecture Notes in Computer Science, Springer, 2010, vol. 6197, p. 234-250.

[47] G. LEURENT. *Practical Key Recovery Attack against Secret-IV Edon-R*, in "CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010", Lecture Notes in Computer Science, Springer, 2010, vol. 5985, p. 334–349.

[48] M. NAYA-PLASENCIA, A. RÖCK, J.-P. AUMASSON, Y. LAIGLE-CHAPUY, G. LEURENT, W. MEIER, T. PEYRIN. *Cryptanalysis of ESSENCE*, in "Fast Software Encryption (FSE '10)", Lecture Notes in Computer Science, Springer, 2010, vol. 6147, p. 134–152.

Workshops without Proceedings

[49] B. BLANCHET, D. POINTCHEVAL. *The computational and decisional Diffie-Hellman assumptions in CryptoVerif*, in "Workshop on Formal and Computational Cryptography (FCC '10)", Edimburgh, United Kingdom, July 2010.

Scientific Books (or Scientific Book chapters)

[50] B. CHEVALLIER-MAMES, P.-A. FOUQUE, D. POINTCHEVAL, J. STERN, J. TRAORÉ. *On Some Incompatible Properties of Voting Schemes*, in "Towards Trustworthy Elections", Lecture Notes in Computer Science, Springer, 2010, vol. 6000, p. 191–199.

[51] P. Q. NGUYEN. *Hermite's Constant and Lattice Algorithms*, in "The LLL Algorithm: Survey and Applications", P. Q. NGUYEN, B. VALLÉE (editors), Information Security and Cryptography, Springer, 2010.

[52] J. PIEPRZYK, D. POINTCHEVAL. *Parallel Signcryption*, in "Practical Signcryption", A. DENT, Y. ZHENG (editors), Information Security and Cryptography, Springer, 2010.

Books or Proceedings Editing

[53] P. Q. NGUYEN, D. POINTCHEVAL (editors). *The 13th International Conference on Practice and Theory in Public Key Cryptography (PKC '10)*, Lecture Notes in Computer Science, Springer, 2010, vol. 6056.

[54] P. Q. NGUYEN, B. VALLÉE (editors). *The LLL Algorithm: Survey and Applications*, Information Security and Cryptography, Springer, 2010.

References in notes

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

[60] 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.

[61] 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.

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

[63] 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.

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

[65] 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.

[66] 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.

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

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

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

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

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

[72] 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.

[73] 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).

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

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

[76] 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.

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

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] 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.

[85] 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.