IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Paris

Activity Report 2012

Project-Team CASCADE

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

IN COLLABORATION WITH: Département d'Informatique de l'Ecole Normale Supérieure

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithms, Certification, and Cryptography

Table of contents

Project-Team CASCADE

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

Creation of the Project-Team: July 01, 2008 .

1. Members

Research Scientists

Michel Ferreira Abdalla [CR, CNRS, HdR]
Vadim Lyubashevsky [CR, Inria]
David Pointcheval [DR, CNRS, Team Leader, HdR]
Oded Regev [DR, CNRS]

Faculty Members

Maribel Fernandez [Assistant Professor, ENS, HdR]
David Naccache [Professor, University Paris II, HdR]
Duong Hieu Phan [Assistant Professor, University Paris 8]
Damien Vergnaud [Assistant Professor, ENS]
Sorina Ionica [ATER ENS]

PhD Students

Sonia Belaid [Thales]
Fabrice Ben Hamouda [ENS]
Olivier Blazy [University Paris 7 grant]
Patrick Derbez [AMN grant]
Léo Ducas [AMN grant]
Aurore Guillevic [CIFRE Thales]
Jérémy Jean [ANR & DGA grant]
Tancrède Lepoint [CIFRE CryptoExperts]
Roch Lescuyer [CIFRE Orange Labs]
Diana Maimut [Crocus Technology]
Delphine Masgana [DGA]
Thomas Prest [ENS]
Sylvain Ruhault [Oppida]
Olivier Sanders [CIFRE Orange Labs]
Mario Strefler [Inria]

Post-Doctoral Fellow

Elizabeth Quaglia [ANR grant]

Administrative Assistants

Nathalie Gaudechoux [Inria]
Joëlle Isnard [Administrative Head DI/ENS, 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 [75], 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 [74], based on the knapsack problem, which took more than 10 years to be totally broken [90], 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) [78], 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" [71] or "concrete security" [83], 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" [67].

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 [76], and later formalized by Bellare and Rogaway [70]. Similarly, block ciphers are identified with families of truly random permutations in the "ideal cipher model" [68]. 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" [82], [89]. Some works even require several ideal models together to provide some new validations [73].

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 [88], [69], [84] which highlights the computational assumptions, and splits the analysis in small independent problems. We early adopted and

developed this technique, and namely in [77]. 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.

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 [86], [85], [80], [81], [79], 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 [70]). Recently, a bunch of attacks [72], [91], [92], [93], [94], [96], [95] 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. Keccak has been officially chosen on October 2nd, 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 years. A NIST competition on hash functions has been launched late 2007 and finished a few months ago. In the first step, cryptographers had to build and analyze their own candidate; in a second step, cryptanalysts were solicited, in order to analyze and break all the proposals. The conclusion has been announced with the winner Keccak, on October 2nd, 2012.

The symmetric people of the Cascade team have worked these years 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.

More recently, we essentially worked on the other candidates, with some analyses and attacks. Even if the winner has been selected, there is still a lot of work to do on hash functions, as there is on block-ciphers, even if AES was selected a long time ago.

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 [66] 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 [87]. 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....

4.6. Access Control

Access control policies describe the rights that different users have on the resources available and are used to protect systems against attacks by unauthorised users. Many authorisation and access control models have been proposed so far; we focus mainly on category-based access control. Amongst the most important issues that have to be addressed in this area are the development of techniques and tools for the analysis and verification of access control policies, and the design of transparent and efficient mechanisms to enforce access control policies.

5. Software

5.1. MitMTool

Participants: Patrick Derbez, Jérémy Jean.

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.

6. Partnerships and Cooperations

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: Patrick Derbez, Jérémy Jean.

  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, David Pointcheval, 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.
- **BEST: Broadcast Encryption for Secure Telecommunications.**
  Participants: Duong Hieu Phan, David Pointcheval, Elizabeth Quaglia, 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: Fabrice Ben Hamouda, Michel Ferreira Abdalla, 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.**
  Participant: David Pointcheval.

  From December 2010 to November 2014.
  Partners: ENS Cachan-Inria/Secsi, LORIA-Inria/Cassis, Inria/Prosecco, 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.
- **ROMAnTIC: Randomness in Mathematical Cryptography.**
  Participant: Damien Vergnaud.

  From October 2012 to September 2016.
  Partners: ANSSI, Univ. Paris 7, Univ. Paris 8.
  The goal of this project is to get a better understanding of the interplay between randomness and cryptography and to study the security of various cryptographic protocols at different levels (information-theoretic and computational security, number-theoretic assumptions, design and provable security of new and existing constructions).

6.3. European Initiatives

- **ECRYPT-II: Network of Excellence in Cryptology.**
  From August 2008 to January 2013.
  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.**
  From September 2010 to August 2012
- **SecFuNet: Security for Future Networks.**
  From July 2011 to December 2013

6.4. International Research Visitors

- Angelo De Caro (PhD student) – Univ. Salerno, Italy
- Karina M. Magalhães (PhD student) – University of Campinas, Brazil
- Daniel Masny (PhD student) – University of Bochum, Germany
- Nuttapong Attrapadung – The National Institute of Advanced Industrial Science and Technology, Japan
- Manuel Bernardo Barbosa – University of Minho, Portugal
- Yu Long – Shanghai Jiao Tong University, China
- Igor Shparlinski – Macquarie U., Australia
- Hoeteck Wee – George Washington University, USA
- Christian Schaffner – CWI, Amsterdam

7. Dissemination

7.1. Editorial Boards

Editor-in-Chief

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

Associate Editor-in-Chief

  - of *Theory of Computing (ToC)*: Oded Regev

Associate Editor

  - 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 *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

7.2. Program Committees

- RIVF – February 2012, Ho Chi Minh, Vietnam: David Naccache, Duong Hieu Phan
- TCC – March 2012, Taormina, Italy: Vadim Lyubashevsky
- EUROCRYPT – April 2012, Cambridge, UK: David Pointcheval (Program Chair)
- Pairing – May 2012, Cologne, Germany: Michel Abdalla (Program Chair), Damien Vergnaud
- STOC – May 2012, New York, NY, USA: Oded Regev
- AICT – May 2012, Stuttgart: David Naccache
- COSADE – May 2012, Darmstadt, Germany: David Naccache
- NTMS – May 2012, Istanbul, Turkey: David Naccache
- PKC – May, 2012, Darmstadt, Germany: Michel Abdalla, Vadim Lyubashevsky
- ACNS – June 2012, Singapore: Michel Abdalla
- HOST – June 2012, San Francisco, CA, USA: David Naccache
- ACISP – July 2012, Wollongong, Australia: Michel Abdalla
- Africacrypt – July 2012, Ifrane, Morocco: David Naccache
- ISCC – July 2012, Cappadocia, Turkey: David Naccache
- Secrypt – July 2012, Roma, Italy: David Naccache
- AReS – August 2012, Prague: David Naccache
- YACC – September 2012, Porquerolles, France: Michel Abdalla, Damien Vergnaud
- ProvSec – September 2012, Chengdu, China: Michel Abdalla, David Naccache
- ESORICS – September 2012, Pisa Italy: David Naccache
- Latincrypt – October 2012, Santiago, Chile: Michel Abdalla, Vadim Lyubashevsky
- IWSEC – November 2012, Fukuoka, Japan: Damien Vergnaud
- CARDIS – November 2012, Graz, Austria: David Naccache
- Intrust – December 2012, Egham, UK: David Naccache
- Indocrypt – December 2012, Kolkata, India: David Naccache
- CANS – December 2012, Darmstadt, Germany: Michel Abdalla

7.3. Teaching - Supervision - Juries

7.3.1. Teaching

Licence: David Naccache, Introduction to computer science, L1, Univ. Paris II

Licence: Maribel Fernandez, Formal languages, computability and complexity, ENS

Master: David Naccache, Scientific programming through practice, M1, ENS

Master: David Naccache, Jacques Stern, Damien Vergnaud, Introduction to Cryptology, M1, ENS

Master: Michel Abdalla, Vadim Lyubashevsky, Cryptography, M2, MPRI

Master: David Naccache, Computer Security, M2, Univ. Paris II

Master: David Naccache, Risk Management, M2, Univ. Paris II

Master: David Naccache, Computer forensics, M2, Univ. Paris II

Master: Duong-Hieu Phan, Provable Security, M2, Univ. Paris VIII

Master: David Pointcheval, Cryptography, M2, ESIEA

7.3.2. Supervision

PhD : Delphine Masgana Leresteux, *Injection de fautes et de logiciels sur les implémentations cryptographiques* Université Paris VII, 5 jul. 2012, Pierre-Alain Fouque

PhD : Olivier Blazy, *Preuves de connaissances interactives et non-interactives*, Université Paris VII, 27 sept. 2012, David Pointcheval

PhD : Roch Lescuyer, *Outils cryptographiques pour les accréditations anonymes*, Université Paris VII, 21 nov. 2012, David Pointcheval

PhD in progress: Mario Strefler, Diffusion chiffrée, 2009, David Pointcheval

PhD in progress: Viet Cuong Trinh, Traçage de traîtres et diffusion de données chiffrée, 2009, Duong Hieu Phan

PhD in progress: Léo Ducas, La cryptographie à base de réseaux, 2009, Phong Nguyen

PhD in progress: Aurore Guillevic, Étude de l'arithmétique des couplages sur des courbes algébriques pour la cryptographie, 2010, Damien Vergnaud

PhD in progress: Diana Maimut, Chiffrement pleinement homomorphe, 2011, David Naccache

PhD in progress: Eric Freyssinet, Modélisation de Botnets, 2011, David Naccache

PhD in progress: Tancrède Lepoint, La cryptographie à base de réseaux, 2011, Vadim Lyubashevsky

PhD in progress: Sylvain Ruhault, L'aléa en cryptographie, 2011, David Pointcheval & Damien Vergnaud

PhD in progress: Fabrice Ben Hamouda, La fuite d'information en cryptographie, 2012, Michel Abdalla & David Pointcheval

PhD in progress: Thomas Prest, La cryptographie à base de réseaux, 2012, Vadim Lyubashevsky & David Pointcheval

PhD in progress: Olivier Sanders, Externalisation de calculs cryptographiques, 2012, David Pointcheval

7.3.3. Juries

- HdR: Karthikeyan Bhargavan, *Towards the Automated Verification of Cryptographic Protocol Implementations*, Ecole Normale Supérieure, 4 may 2012: David Pointcheval
- HdR: Carlos Aguilar Melchor, *Sécurité, protection de la vie privée et cryptographie : quelques contributions*, Univ. Limoges, 26 jun. 2012: David Pointcheval (chair)
- HdR: Pascal Lafourcade, *Computer Aided Security for Cryptographic Primitives, Voting protocols, and Wireless Sensor Networks*, Univ. Grenoble, 6 nov. 2012: David Pointcheval (chair)

- PhD: Marion Daubignard, *Formal Methods for Concrete Security Proofs*, Univ. Grenoble, 12 jan. 2012: David Pointcheval (reviewer)
- PhD: Saeed Sedghi, *Towards Provably Secure Efficiently Searchable Encryption*, Univ. Twente, 17 feb. 2012: Michel Abdalla
- PhD: Avradip Mandal, *Provable Security and Indifferentiability* Univ. Luxembourg, 25 jun. 2012: David Pointcheval
- PhD: Delphine Masgana Leresteux, *Injection de fautes et de logiciels sur les implémentations cryptographiques*, Univ. Paris VII, 5 jul. 2012: David Pointcheval (co-advisor), David Naccache (chair)
- PhD: Adriana Suarez Corona, *Compilers and protocols for key establishment*, Univ. Oviedo, 24 jul. 2012: Michel Abdalla (Examiner)
- PhD: Olivier Blazy, *Preuves de connaissances interactives et non-interactives*, Univ. Paris VII, 27 sept. 2012: David Pointcheval (advisor), Michel Abdalla, Damien Vergnaud
- PhD: Anja Becker *La technique de représentation – Application à des problèmes difficiles en cryptographie* UVSQ, 26 oct. 2012: David Naccache (chair)
- PhD: Roch Lescuyer, *Outils cryptographiques pour les accréditations anonymes*, Univ. Paris VII, 21 nov. 2012: David Pointcheval (advisor), David Naccache (chair), Damien Vergnaud
- HdR: Bruno Robisson *Contribution à la sécurisation des composants vis-à-vis des attaques physiques* UMPC, 12 dec. 2012: David Naccache
- HdR: Olivier Ly *Un parcours de recherche des méthodes formelles aux robots humanoïdes* Univ. Bordeaux, 13 dec. 2012: David Naccache (reviewer)
- PhD: Amar Siad, *Protocoles de génération des clés pour le chiffrement basé sur de l'identité*, Univ. Paris 8, 17 dec. 2012: David Pointcheval, Duong-Hieu Phan
- PhD: Houssem Maghrebi *Masking Countermeasures against Higher-Order Side Channel Attacks: Security Evaluation and Enhancement by Specific Mask Encodings*, Telecom ParisTech, 21 dec. 2012: David Naccache
- HdR: Sylvain Guilley *Protection des Accélérateurs Matériels de Cryptographie Symétrique* TelecomParisTech, 20 dec. 2012: David Naccache

7.4. Invited Talks

7.4.1. At Conferences

- PKC 2012, Darmstadt, Germany (May): David Pointcheval
- NTCCS 2012, Oujda, Morocco (Avril): Damien Vergnaud
- LSFA 2012, Rio de Janeiro, Brazil (September): Maribel Fernandez
- ECC 2012, Queretaro, Mexico (October): Sorina Ionica
- ICCC 2012 Distinguished Lecturer, Paris (November): David Naccache
- ICISC 2012, Seoul Korea, (November): David Naccache
- CARDIS 2012, Graz (November): David Naccache
- SantaCrypt 2012, Prague (November): David Naccache

7.4.2. At Organized Schools

- Bar-Ilan Winter School on Cryptography. Ramat-Gan, Israel. February, 2012 : Vadim Lyubashevsky
- ECRYPT II Summer School on Lattices. Porto, Portugal. October, 2012 : Vadim Lyubashevsky

7.5. Scientific Animation

7.5.1. Organisation of Events

- ECRYPT II Summer School on Lattices, October 1 - 5, Porto Portugal: Michel Abdalla and Vadim Lyubashevsky
- a weekly seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html

7.5.2. Steering Committees of International Conferences

- steering committee of CANS: David Pointcheval
- steering committee of PKC: David Pointcheval, David Naccache
- steering committee of FDTC: David Naccache (chair)
- steering committee of PROOFS: David Naccache
- steering committee of LATINCRYPT: Michel Abdalla

7.5.3. Board of International Organizations

- Board of the *International Association for Cryptologic Research* (IACR): David Naccache (2010 – 2012), David Pointcheval (2008–2013)
- Scientific Board of the *Electronic Colloquium on Computational Complexity* (ECCC): Oded Regev

7.5.4. French Research Community

- Recruitment committee at Université Paris VII (PR 27): David Pointcheval
- Recruitment committee at Université of Lyon (PR 27): David Pointcheval
- Recruitment committee at Université de Caen (MC 25): Damien Vergnaud
- Recruitment committee at Université de Montpellier (MC 27): Damien Vergnaud
- Appointed member of the *Conseil National des Universités* (CNU): Damien Vergnaud

8. 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] 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.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[13] O. BLAZY. *Preuves de connaissances interactives et non-interactives*, Université Paris VII, 2012.

[14] R. LESCUYER. *Outils cryptographiques pour les accréditations anonymes*, Université Paris VII, 2012.

[15] D. MASGANA LERESTEUX. *Injection de fautes et de logiciels sur les implémentations cryptographiques*, Université Paris VII, 2012.

Articles in International Peer-Reviewed Journals

[16] M. ABDALLA, A. DE CARO, D. H. PHAN. *Generalized Key Delegation for Wildcarded Identity-Based and Inner-Product Encryption*, in "IEEE Transactions on Information Forensics & Security", 2012, vol. 7, n^{o} 6, p. 1695–1706.

[17] A. BARENGHI, L. BREVEGLIERI, I. KOREN, D. NACCACHE. *Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures*, in "Proceedings of the IEEE", 2012, vol. 100, n^{o} 11, p. 3056-3076.

[18] C. BOUILLAGUET, P. DERBEZ, O. DUNKELMAN, P.-A. FOUQUE, N. KELLER, V. RIJMEN. *Low-Data Complexity Attacks on AES*, in "IEEE Transactions on Information Theory", 2012, vol. 58, n^{o} 11, p. 7002-7017.

[19] E. BRIER, W. FANG, D. NACCACHE. *How to Scatter a Secret?*, in "Cryptologia", 2012, vol. 36, n^{o} 1, p. 46-54.

[20] J. BRIET, A. NAOR, O. REGEV. *Locally decodable codes and the failure of cotype for projective tensor products*, in "Electronic Research Announcements in Mathematical Sciences", 2012, vol. 19, p. 120–130.

[21] H. BUHRMAN, O. REGEV, G. SCARPA, R. DE WOLF. *Near-Optimal and Explicit Bell Inequality Violations*, in "Israel Journal of Mathematics", 2012, To appear.

[22] A. CHAKRABARTI, O. REGEV. *An Optimal Lower Bound on the Communication Complexity of Gap Hamming Distance*, in "SIAM Journal on Computing", 2012, To appear.

[23] E. DOMENJOUD, D. JAMET, D. VERGNAUD, L. VUILLON. *Enumeration formula for (2, n)-cubes in discrete planes*, in "Discrete Applied Mathematics", 2012, vol. 160, n^{o} 15, p. 2158-2171.

[24] I. HAVIV, O. REGEV. *Entropy-based Bounds on Dimension Reduction in L_1*, in "Israel Journal of Mathematics", 2012, To appear.

[25] I. HAVIV, O. REGEV. *Tensor-based Hardness of the Shortest Vector Problem to within Almost Polynomial Factors*, in "Theory of Computing", 2012, To appear.

[26] A. NAOR, O. REGEV. *Krivine schemes are optimal*, in "Proceedings of the AMS", 2012, To appear.

[27] H. Q. NGO, D. H. PHAN, D. POINTCHEVAL. *Black-box Trace&Revoke Codes*, in "Algorithmica", 2012, To appear, http://hal.inria.fr/hal-00763979.

[28] O. REGEV, T. VIDICK. *Elementary Proofs of Grothendieck Theorems for Completely Bounded Norms*, in "Journal of Operator Theory", 2012, To appear.

International Conferences with Proceedings

[29] M. ABDALLA, D. FIORE, V. LYUBASHEVSKY. *From Selective to Full Security: Semi-generic Transformations in the Standard Model*, in "Public Key Cryptography (PKC '12)", Darmstadt, Germany, M. FISCHLIN, J. BUCHMANN, M. MANULIS (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7293, p. 316-333.

[30] M. ABDALLA, P.-A. FOUQUE, V. LYUBASHEVSKY, M. TIBOUCHI. *Tightly-Secure Signatures from Lossy Identification Schemes*, in "Advances in Cryptology – Proc. EUROCRYPT 2012", D. POINTCHEVAL, T. JOHANSSON (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7237, p. 572-590.

[31] M. ABDALLA, J.-J. VIE. *Leakage-Resilient Spatial Encryption*, in "Second International Conference on Cryptology and Information Security (Latincrypt '12)", Santiago, Chile, A. HEVIA, G. NEVEN (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7533, p. 78–99.

[32] M. ABDALLA, A. DE CARO, K. MOCHETTI. *Lattice-Based Hierarchical Inner Product Encryption*, in "Second International Conference on Cryptology and Information Security (Latincrypt '12)", Santiago, Chile, A. HEVIA, G. NEVEN (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7533, p. 121–138.

[33] G. BARTHE, D. POINTCHEVAL, S. ZANELLA-BÉGUELIN. *Verified Security of Redundancy-Free Encryption from Rabin and RSA*, in "Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS '12)", Raleigh, NC, USA, T. YU, G. DANEZIS, V. D. GLIGOR (editors), ACM Press, 2012, p. 724–735, http://hal.inria.fr/hal-00764871.

[34] A. BAUER, D. VERGNAUD, J.-C. ZAPALOWICZ. *Inferring Sequences Produced by Nonlinear Pseudorandom Number Generators Using Coppersmith's Methods*, in "Public Key Cryptography (PKC '12)", Darmstadt, Germany, M. FISCHLIN, J. BUCHMANN, M. MANULIS (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7293, p. 609-626.

[35] O. BLAZY, D. POINTCHEVAL, D. VERGNAUD. *Compact Round-Optimal Partially-Blind Signatures*, in "The 8th Conference on Security in Communication Networks (SCN '12)", Amalfi, Italy, I. VISCONTI, R. DE PRISCO (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7485, p. 95–112, http://hal.inria.fr/hal-00764863.

[36] O. BLAZY, D. POINTCHEVAL, D. VERGNAUD. *Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions*, in "9th Theory of Cryptography Conference (TCC '12)", Taormina, Italy, R. CRAMER (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7194, p. 94–111, http://hal.inria.fr/hal-00672939.

[37] S. BRIAIS, S. CARON, J.-M. CIORANESCO, J.-L. DANGER, S. GUILLEY, J.-H. JOURDAN, A. MILCHIOR, D. NACCACHE, T. PORTEBOEUF. *3D Hardware Canaries*, in "Cryptographic Hardware and Embedded Systems (CHES '12)", E. PROUFF, P. SCHAUMONT (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7428, p. 1-22.

[38] S. BRIAIS, J.-M. CIORANESCO, J.-L. DANGER, S. GUILLEY, D. NACCACHE, T. PORTEBOEUF. *Random Active Shield*, in "Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC '12)", G. BERTONI, B. GIERLICHS (editors), IEEE, 2012, p. 103-113.

[39] B. CHUNG, S. MARCELLO, A.-P. MIRBAHA, D. NACCACHE, K. SABEG. *Operand Folding Hardware Multipliers*, in "Cryptography and Security: From Theory to Applications", D. NACCACHE (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 6805, p. 319-328.

[40] G. CLARET, M. MATHIEU, D. NACCACHE, G. SEGUIN. *Physical Simulation of Inarticulate Robots*, in "Cryptography and Security: From Theory to Applications", D. NACCACHE (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 6805, p. 491-499.

[41] J.-S. CORON, D. NACCACHE, M. TIBOUCHI. *Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers*, in "Advances in Cryptology – Proc. EUROCRYPT 2012", D. POINTCHEVAL, T. JOHANSSON (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7237, p. 446-464.

[42] J. P. DEGABRIELE, A. LEHMANN, K. G. PATERSON, N. P. SMART, M. STREFLER. *On the Joint Security of Encryption and Signature in EMV*, in "Topics in Cryptology – Proc. CT-RSA 2012", San Francisco, CA, O. DUNKELMAN (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7178, p. 116–135.

[43] P. DERBEZ, P.-A. FOUQUE, J. JEAN. *Faster Chosen-Key Distinguishers on Reduced-Round AES*, in "INDOCRYPT '12", 2012, p. 225-243.

[44] R. DUBOIS, A. GUILLEVIC, M. SENGELIN LE BRETON. *Improved Broadcast Encryption Scheme with Constant-Size Ciphertext*, in "Pairing-Based Cryptography (Pairing '12)", Cologne, Germany, M. ABDALLA, T. LANGE (editors), Lecture Notes in Computer Science, Springer, 2012.

[45] L. DUCAS, A. DURMUS. *Ring-LWE in Polynomial Rings*, in "Public Key Cryptography (PKC '12)", Lecture Notes in Computer Science, Springer, 2012, vol. 7293, p. 34-51.

[46] L. DUCAS, P. Q. NGUYEN. *Faster Gaussian Lattice Sampling using Lazy Floating-Point Arithmetic*, in "Advances in Cryptology – Proc. ASIACRYPT '12", Lecture Notes in Computer Science, Springer, 2012, vol. 7658.

[47] L. DUCAS, P. Q. NGUYEN. *Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures*, in "Advances in Cryptology – Proc. ASIACRYPT '12", Lecture Notes in Computer Science, Springer, 2012, vol. 7658.

[48] J.-M. DUTERTRE, A.-P. MIRBAHA, D. NACCACHE, A.-L. RIBOTTA, A. TRIA, T. VASCHALDE. *Fault Round Modification Analysis of the advanced encryption standard*, in "IEEE International Symposium on Hardware-Oriented Security and Trust (HOST '12)", IEEE, 2012, p. 140-145.

[49] V. GRATZER, D. NACCACHE. *How to Read a Signature?*, in "Cryptography and Security: From Theory to Applications", D. NACCACHE (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 6805, p. 480-483.

[50] A. GUILLEVIC, D. VERGNAUD. *Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions.*, in "Pairing-Based Cryptography (Pairing '12)", Cologne, Germany, M. ABDALLA, T. LANGE (editors), Lecture Notes in Computer Science, Springer, 2012.

[51] T. GÜNEYSU, V. LYUBASHEVSKY, T. PÖPPELMANN. *Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems*, in "Cryptographic Hardware and Embedded Systems (CHES '12)", E. PROUFF, P. SCHAUMONT (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7428, p. 530-547.

[52] S. HEYSE, E. KILTZ, V. LYUBASHEVSKY, C. PAAR, K. PIETRZAK. *Lapin: An Efficient Authentication Protocol Based on Ring-LPN*, in "Fast Software Encryption (FSE '12)", A. CANTEAUT (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7549, p. 346-365.

[53] J. JEAN, M. NAYA-PLASENCIA, T. PEYRIN. *Improved Rebound Attack on the Finalist Grøstl*, in "Fast Software Encryption (FSE '12)", A. CANTEAUT (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 7549, p. 110-126.

[54] M. JOYE, T. LEPOINT. *Partial key exposure on RSA with private exponents larger than N*, in "Information Security Practice and Experience (ISPEC '12)", Hangzhou, China, M. D. RYAN, B. SMYTH, G. WANG (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7232, p. 369–380.

[55] V. LYUBASHEVSKY. *Lattice Signatures without Trapdoors*, in "Advances in Cryptology – Proc. EUROCRYPT 2012", D. POINTCHEVAL, T. JOHANSSON (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7237, p. 738-755.

[56] C. MURDICA, S. GUILLEY, J.-L. DANGER, P. HOOGVORST, D. NACCACHE. *Same Values Power Analysis Using Special Points on Elliptic Curves*, in "Constructive Side-Channel Analysis and Secure Design (COSADE '12)", W. SCHINDLER, S. A. HUSS (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7275, p. 183-198.

[57] D. NACCACHE, D. POINTCHEVAL. *Autotomic Signatures*, in "Cryptography and Security: From Theory to Applications", D. NACCACHE (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 6805, p. 143–155.

[58] D. H. PHAN, D. POINTCHEVAL, S. F. SHAHANDASHTI, M. STREFLER. *Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts*, in "The 17th Australasian Conference on Information Security and Privacy (ACISP '12)", Wollongong, Australia, W. SUSILO, Y. MU, J. SEBERRY (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7372, p. 308–321, http://hal.inria.fr/hal-00764852.

[59] D. H. PHAN, D. POINTCHEVAL, M. STREFLER. *Decentralized Dynamic Broadcast Encryption*, in "The 8th Conference on Security in Communication Networks (SCN '12)", Amalfi, Italy, I. VISCONTI, R. DE PRISCO (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7485, p. 166–183, http://hal.inria.fr/hal-00764847.

[60] D. H. PHAN, D. POINTCHEVAL, M. STREFLER. *Message-based Traitor Tracing with Optimal Ciphertext Rate*, in "Second International Conference on Cryptology and Information Security (LatinCrypt '12)", Santiago, Chile, A. HEVIA, G. NEVEN (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7533, p. 56–77, http://hal.inria.fr/hal-00764842.

[61] D. POINTCHEVAL. *Password-Based Authenticated Key Exchange*, in "Conference on Practice and Theory in Public-Key Cryptography (PKC '12)", Darmstadt, Germany, M. FISCHLIN, J. BUCHMANN, M. MANULIS (editors), Lecture Notes in Computer Science, Springer, 2012, vol. 7293, p. 390–397, http://hal.inria.fr/hal-00764515.

Scientific Books (or Scientific Book chapters)

[62] M. ABDALLA, T. LANGE (editors). *The 5th International Conference on Pairing-Based Cryptography (Pairing 2012)*, Lecture Notes in Computer Science, Springer, Cologne, Germany, 2012, vol. 7708.

[63] O. BLAZY, D. POINTCHEVAL. *Traceable Signature with Stepping Capabilities*, in "Cryptography and Security: From Theory to Applications", D. NACCACHE (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 6805, p. 108–131.

Books or Proceedings Editing

[64] D. NACCACHE (editor). *Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday*, Lecture Notes in Computer Science, Springer, 2012, vol. 6805.

[65] D. POINTCHEVAL, T. JOHANSSON (editors). *The 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt '12)*, Lecture Notes in Computer Science, Springer, Cambridge, UK, 2012, vol. 7237, http://hal.inria.fr/hal-00766147.

References in notes

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

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

[74] 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.

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

[76] 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.

[77] 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.

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

[79] NIST. *Descriptions of SHA–256, SHA–384, and SHA–512*, October 2000, Federal Information Processing Standards PUBlication 180–3, http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

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

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

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

[83] 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.

[84] 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).

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

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

[87] 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.

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

[89] 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.

[90] 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.

[91] 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.

[92] 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.

[93] 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.

[94] 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.

[95] 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.

[96] 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.