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 ]
Phong Quang Nguyen [ DR, INRIA, HdR ]
David Pointcheval [ DR, CNRS, Team Leader, HdR ]

**Faculty Member**

Pierre-Alain Fouque [ Assistant Professor, ENS ]
David Naccache [ Professor, University Paris II, HdR ]
Jacques Stern [ Professor, ENS, On leave, HdR ]
Damien Vergnaud [ Assistant Professor, ENS ]
Jean Vuillemin [ Professor, ENS, HdR ]

**PhD Student**

Olivier Blazy [ University Paris 7 grant ]
Charles Bouillaguet [ Fondation EADS grant ]
Céline Chevalier [ AMN grant ]
Léo Ducas [ ENS ]
Georg Fuchsbauer [ EADS grant ]
Nicolas Gama [ AMN grant ]
Malika Izabachène [ University Paris 7 grant ]
Gaëtan Leurent [ DGA grant ]
Mario Strefler [ INRIA ]
Mehdi Tibouchi [ Ingenico & NTT ]

**Post-Doctoral Fellow**

Aurélie Bauer [ DGA grant ]
Orr Dunkelman [ Chaire ENS – France Télécom 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

## 2.2. Highlights

### *2.2.1. SIMD: Selected for the second round of the NIST SHA-3 Competition*

Since the recent attacks on many hash functions such as MD4, MD5, SHA-0, and SHA-1, the NIST has decided to launch a competition to choose the next standardized hash function. Among the 51 hash functions presented in february 2009 at the first NIST hash function workshop, only 14 have passed the first round in august 2009, including 3 hash functions designed by french groups: one of them is the SIMD hash function designed by our team.

Since the recent attacks use differential cryptanalysis, we tried to secure SIMD against such attacks by using a strong message expansion with a high minimal distance. SIMD also provides new ideas by tweaking the Davies-Meyer mode for constructing compression function in a special way to avoid undesiderable properties such as fixed points. The performances of SIMD are especially interesting for processors with SIMD instructions, since SIMD is highly parallelizable.

### *2.2.2. Password-based Cryptography*

To be used in practice, cryptography must be efficient on both the machine and the user points of view. Computational cost has been a major concern for a long time, with various successes. This is still important to keep efficiency in mind. However, the security of the system is at most that of the weakest part. And this weakest part is quite often the human being: if intricate techniques have to be used, the latter will not use them.

Password-based cryptography can provide a good trade-off, if well specified. Of course, we cannot expect the same security as with a 128-bit secret key, but reasonable security levels can be reached, even with small passwords, easily memorable by users: on-line dictionary attacks only are possible for the adversary, which means that one password only can be tested per active attack.

Last year, we provided the first analysis of a 2-party key exchange, secure against adaptive adversaries, in the random oracle model. This year, we provided the first efficient scheme provably secure in the standard model. To this aim, we extended a theoretical tool, the *smooth projective hash system*, in order to build conditionally extractable commitments. Moreover, we studied group key exchange, in the random oracle model, with an additional property. The *contributiveness* means that until the adversary has not corrupted too many parties, it has no chance to bias the key the group will agree on.

Traditional wisdom says that it is impossible to do public-key cryptography from short passwords. This is because any low-entropy private key will quickly succumb to an off-line dictionary attack, made possible by the very publication of the public key, which can thus be used as a non-interactive test function. Since off-line attacks are very effective against weak secrets, it is imperative that the private keys in public-key systems be highly random and complex, but that makes them hopelessly impossible to be remembered by humans. We have thus introduced the notion of distributed password-based public-key cryptography, where a virtual high-entropy private key is implicitly defined as a concatenation of low-entropy passwords held in separate locations. The users can jointly perform private-key operations by exchanging messages over an arbitrary channel, based on their respective passwords, without ever sharing their passwords or reconstituting the key.

# 3. Scientific Foundations

## 3.1. Provable Security

Since the beginning of public-key cryptography, with the seminal Diffie-Hellman paper [70], many suitable algorithmic problems for cryptography have been proposed and many cryptographic schemes have been designed, together with more or less heuristic proofs of their security relative to the intractability of the underlying problems. However, many of those schemes have thereafter been broken. The simple fact that a cryptographic algorithm withstood cryptanalytic attacks for several years has often been considered as a kind of validation procedure, but schemes may take a long time before being broken. An example is the Chor-Rivest cryptosystem [68], based on the knapsack problem, which took more than 10 years to be totally broken [86], 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) [74], without considering practicality. Therefore, they just needed to design a scheme with polynomial-time algorithms, and to exhibit polynomial reductions from the basic mathematical assumption on the hardness of the underlying problem into an attack of the security notion, in an asymptotic way. However, such a result has no practical impact on actual security. Indeed, even with a polynomial reduction, one may be able to break the cryptographic protocol within a few hours, whereas the reduction just leads to an algorithm against the underlying problem which requires many years. Therefore, those reductions only prove the security when very huge (and thus maybe unpractical) parameters are in use, under the assumption that no polynomial time algorithm exists to solve the underlying problem.

For a few years, more efficient reductions have been expected, under the denomination of either "exact security" [65] or "concrete security" [79], which provide more practical security results. The perfect situation is reached when one is able to prove that, from an attack, one can describe an algorithm against the underlying problem, with almost the same success probability within almost the same amount of time: "tight reductions". We have then achieved "practical security" [61]. Unfortunately, in many cases, even just provable security is at the cost of an important loss in terms of efficiency for the cryptographic protocol. Thus, some models have been proposed, trying to deal with the security of efficient schemes: some concrete objects are identified with ideal (or black-box) ones. For example, it is by now usual to identify hash functions with ideal random functions, in the so-called "random-oracle model", informally introduced by Fiat and Shamir [71], and later formalized by Bellare and Rogaway [64]. Similarly, block ciphers are identified with families of truly random permutations in the "ideal cipher model" [62]. A few years ago, another kind of idealization was introduced in

cryptography, the black-box group, where the group operation, in any algebraic group, is defined by a black-box: a new element necessarily comes from the addition (or the subtraction) of two already known elements. It is by now called the "generic model" [78], [85]. Some works even require several ideal models together to provide some new validations [67].

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

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

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

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

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

**security proof**, which consists in exhibiting a reduction.

For a long time, the security proofs by reduction used classical techniques from complexity theory, with a direct description of the reduction, and then a long and quite technical analysis for providing the probabilistic estimates. Such analysis is unfortunately error-prone. Victor Shoup proposed a nice way to organize the proofs, and eventually obtain the probabilities, using a sequence of games [84], [63], [80] which highlights the computational assumptions, and splits the analysis in small independent problems. We early adopted and developed this technique, and namely in [72].

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.

## 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 [82], [81], [76], [77], [75], which are an essential primitive in many protocols, received a lot of attention: they were initially used for improving efficiency in signature schemes, hence the requirement of collision-resistance. But afterwards, hash functions have been used for many purposes, such as key derivation, random generation, and random functions (random oracles [64]). Recently, a bunch of attacks [66], [87], [88], [89], [90], [92], [91] 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 [59] 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 [83]. 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. New Results

## 5.1. Foundations

**Participants:** Nicolas Gama, Phong Quang Nguyen.

**An LLL Algorithm with Quadratic Complexity (SIAM J. Computing, 2009)**

LLL is a celebrated algorithm published by Lenstra, Lenstra and Lovász in 1982. This algorithm was the first polynomial-time algorithm that provably finds short vectors in a lattice, which has many applications: given as input a finite number of integral vectors, LLL finds a reasonably short integral linear combination of the input vectors.

This can be viewed as a geometric generalization of the problem of computing greatest common divisors: given as input two integers $a$ and $b$, Euclid's algorithm computes in quadratic time the gcd of $a$ and $b$, that is, the nonzero integral linear combination of $a$ and $b$ that is both positive and smallest.

However, the natural analogy between LLL and Euclid's algorithm was not fully satisfactory until now, at least from a computational point of view. Indeed, while the running time of Euclid's algorithm is quadratic without fast integer arithmetic, all LLL-type algorithms known had a cubic running time without fast integer arithmetic, in the sense that their polynomial-time complexity was at least cubic in the bit-size of the largest norm of the input vectors: here, we ignore the additional polynomial term depending on the lattice dimension.

This article [17] presents the first LLL algorithm whose running time is provably quadratic in the bit-size of the largest norm of the input vectors, which makes it similar to Euclid's algorithm. This result was inspired by [18], which studied low-dimensional lattice reduction.

**The LLL Algorithm: Surveys and Applications (Springer book, 2009)**

This book [57], published by Springer, is a follow-up to the 2007 conference that took place in Caen, celebrating the 25th anniversary of the publication of the LLL algorithm. It surveys the foundations and the main applications of LLL and lattice algorithms in computer science and mathematics: for instance, [54] introduces lattices and presents the main provable lattice algorithms. The surveys are written by the invited speakers of the conference.

## 5.2. Cryptanalysis (Mathematical)

**Participants:** Gaëtan Leurent, David Naccache, Phong Quang Nguyen, Mehdi Tibouchi.

**Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures (Journal of Cryptology, 2009)**

Lattice-based signature schemes following the Goldreich-Goldwasser-Halevi (GGH) design have the unusual property that each signature leaks information on the signer's secret key, but this does not necessarily imply that such schemes are insecure. We present a practical and provable method to attack signature schemes à la GGH, by studying the following learning problem: given many random points uniformly distributed over an unknown $n$-dimensional parallelepiped, recover the parallelepiped or an approximation thereof. We transform this problem into a multivariate optimization problem that can provably be solved by a gradient descent. Our approach is very effective in practice: we present the first successful key-recovery experiments on NTRUsign-251 without perturbation, as proposed in half of the parameter choices in NTRU standards under consideration by IEEE P1363.1. Experimentally, 400 signatures are sufficient to recover the NTRUsign-251 secret key, thanks to symmetries in NTRU lattices. We are also able to recover the secret key in the signature analogue of all the GGH encryption challenges.

**Factoring $pq^2$ with Quadratic Forms: Nice Cryptanalyses (ASIACRYPT '09)**

Factoring integers remains the most famous hard computational problem used in cryptology. Yet, there are many open questions regarding the complexity of factoring. For instance, we do not even know if numbers of the form $N = pq$ where $p$ and $q$ are distinct primes are easier or harder to factor than numbers of the form $N = pq^2$. The former numbers are used in RSA. The latter numbers are used in many public-key cryptosystems, such as the ESIGN signature scheme, because their structure allows special properties such as improved efficiency or unusual features. This article [30] presents a new algorithm to factor numbers of the form $N = pq2$ when special properties are met, related to the so-called NICE family of public-key cryptosystems based on quadratic fields, that was introduced in the 1990s. The main member of the NICE family was recently broken at EUROCRYPT '09, but this article presents an alternative attack which can apply to the whole NICE family. In particular, the article presents a heuristic algorithm to obtain a squarefree factorization $N = pq^2$ when the regulator of $\mathbb{Q}(\sqrt{p})$ is small, and this algorithm is works very well in practice. The results are based on combining Lagrange's classical reduction of quadratic forms with a well-known cryptanalysis technique to find small roots of polynomial equations, due to Coppersmith.

**Factoring Unbalanced Moduli with Known Bits (ICISC '09)**

In the particular case where $n = pq > q^3$, we describe an LLL-based method allowing to factor $n$ given $2\log_2 q$ contiguous bits of $p$, irrespective to their position. A second method is presented, which needs fewer bits but whose length depends on the position of the known bit pattern. Finally, we introduce a somewhat surprising ad hoc method where two different known bit chunks, totalling $\frac{3}{2}\log_2 q$ bits suffice to factor $n$.

**Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms (Cryptography and Coding, 2009)**

This paper extends Joux-Naccache-Thomé's $e$-th root algorithm [73] to the static Diffie-Hellman problem (SDHP). The new algorithm can be adapted to diverse finite fields by customizing it with an NFS-like core or an FFS-like core. In both cases, after a number of SDHP oracle queries, the attacker builds-up the ability to solve new SDHP instances unknown before the query phase. While sub-exponential, the algorithm is still significantly faster than all currently known DLP and SDHP resolution methods. We explore the applicability of the technique to various cryptosystems. The attacks were implemented in $\mathbb{F}_{2^{1025}}$ and also in $\mathbb{F}_p$, for a 516-bit $p$.

**How Risky is the Random-Oracle Model? (CRYPTO '09)**

The Random-Oracle Model (ROM) is a widespread methodology popularized by Bellare and Rogaway in 1993 to prove security properties by modeling hash functions as random oracles: several standardized RSA schemes are provably secure in the ROM. There are well-known pros and cons to the ROM, but this article [45] presents new issues. The first contribution is to show that the random-oracle instantiations proposed in the litterature for the special case of long hash output (as required in certain RSA signature schemes) are not satisfactory: in particular, the 1993 proposal by Bellare and Rogaway is completely insecure. The second contribution is to highlight the lack of granularity of the ROM: the article shows that the security of certain recent cryptographic schemes provably secure in the ROM completely collapses with the slightest defect in the hash function; for instance, a hash collision may suffice to disclose the secret key. This is however not the case for most schemes

secure in the ROM, which implies that a ROM security proof alone is insufficient to compare the actual security guarantees of schemes.

**Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures (CRYPTO '09)**

In 1999, Coron, Naccache and Stern [69] discovered an existential signature forgery for two popular RSA signature standards, ISO/IEC 9796-1 and 2. Following this attack ISO/IEC 9796-1 was withdrawn. ISO/IEC 9796-2 was amended by increasing the message digest to at least 160 bits. Attacking this amended version required at least $2^{61}$ operations. In this paper, we exhibit algorithmic refinements allowing to attack the amended (currently valid) version of ISO/IEC 9796-2 for all modulus sizes. A practical forgery was computed in only two days using 19 servers on the Amazon EC2 grid for a total cost of US$800. The forgery was implemented for $e = 2$ but attacking odd exponents will not take longer. The forgery was computed for the RSA-2048 challenge modulus, whose factorization is still unknown.

The new attack blends several theoretical tools. These do not change the asymptotic complexity of Coron et al.'s technique but significantly accelerate it for parameter values previously considered beyond reach.

While less efficient (US$45,000), the acceleration also extends to EMV signatures. EMV is an ISO/IEC 9796-2-compliant format with extra redundancy. Luckily, this attack does not threaten any of the 730 million EMV payment cards in circulation for operational reasons.

Costs are per modulus: after a first forgery for a given modulus, obtaining more forgeries is virtually immediate.

## 5.3. Cryptanalysis (Symmetric)

**Participants:** Charles Bouillaguet, Pierre-Alain Fouque, Gaëtan Leurent.

- **Herding, Second Preimage and Trojan Message Attacks Beyond Merkle-Damgaard (SAC '09)**
- **Practical Electromagnetic Template Attack on HMAC (CHES '09)**

Besides the design of a hash function, have also attacked some schemes: such as Edon-R (recovering an equivalent key when the MAC function is $H(k||m)$) and we have the best attacks on the Lesamnta hash function.

Following the work of Eurocrypt last year [60] on cryptanalysis of mode of operation for hash functions, some new attacks have been proposed at SAC [25]. Finally, in order to attack some standards such as HMAC-SHA1, we have used side channel attacks [39].

## 5.4. Cryptanalysis (Side-Channel)

**Participant:** David Naccache.

**Fault Attacks on RSA Signatures with Partially Unknown Messages (CHES '09)**

This paper exhibits a fault attack against RSA signatures with partially known messages: it allows factoring the public modulus $N$. While the size of the unknown message part increases with the number of faulty signatures available, the complexity of the attack increases exponentially with the number of faulty signatures.

**Deconvolving Protected Signals (ARES '09)**

The variable clock (VC) side-channel countermeasure consists in clocking a chip with an internal oscillator whose parameters (frequency, duty cycle, shape, etc.) vary randomly in time. In this paper, we use parametric deconvolution to process VC-power consumption curves. We also analyze experimental results in order to show its efficiency.

## 5.5. New Primitives (Key Exchange)

**Participants:** Michel Ferreira Abdalla, Céline Chevalier, David Pointcheval.

- **Distributed Public-Key Cryptography from Weak Secrets (PKC '09)**
- **Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness (AfricaCrypt '09)**

These two papers propose new schemes that allow key generation, with password authentication of the players. The main goal of password-based cryptography is to guarantee that the on-line dictionary attack is the best attack: each on-line active interaction just allows the adversary to test one password.

- **Smooth Projective Hashing for Conditionally Extractable Commitments (CRYPTO '09)**
- **Optimal Randomness Extraction from a Diffie-Hellman Element (EUROCRYPT '09)**

These two papers present tools to be used for efficient key exchange protocols: the former leads to the first efficient password-based key exchange protocol secure against adaptive adversaries in the UC framework, in the standard model. The latter explains that if one truncates the representation of a random group element (in a finite field or an elliptic curve), this leads to a random bit string.

## 5.6. New Primitives (Anonymity)

**Participants:** Michel Ferreira Abdalla, Georg Fuchsbauer, Malika Izabachène, David Pointcheval, Damien Vergnaud.

- **Fair E-Cash: Be Compact, Spend Faster (ISC '09)**
- **Transferable Anonymous Constant-Size Fair E-Cash (CANS '09)**

We focused on the specific topic of anonymous electronic money: e-cash can be spent and even transfered (to an other user) in an anonymous way. However, in case of double-spending, a trusted third party is able to open the identity of the defrauder. Efficiency (computation and communication) is also considered.

- **Provably Secure Code-Based Threshold Ring Signatures (Cryptography and Coding '09)**
- **Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model (CANS '09)**

Signing in the name of a group of players is a fundamental primitive in cryptography: ring signatures allow to do so in a perfect anonymous way; group signatures provide the ability to open the identity of the actual signer in case of abuse.

- **Anonymous Consecutive Delegation of Signing Rights: Unifying Group and Proxy Signatures (Formal to Practical Security)**
- **Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures (Pairing '09)**

These papers develop models and tools in order to delegate some rights, in such a way that the delegatee's signature is indistinguishable from the delegator's signature: anonymity is guaranteed, except for the delegator who can recover the identity of the actual delegatee who signed in his name.

## 5.7. New Primitives (Identity-Based Encryption)

**Participants:** Michel Ferreira Abdalla, Malika Izabachène, David Pointcheval, Damien Vergnaud.

- **New Anonymity Notions for Identity-Based Encryption (Formal to Practical Security)**
- **Adaptive-ID Secure Revocable Identity-Based Encryption (CT-RSA '09)**
- **Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys (PKC '09)**
- **Verifiable Random Functions from Identity based Key Encapsulation (EUROCRYPT '09)**

Identity-based encryption makes public-key cryptography much easier since the public key is simply the identity of the recipient: no certification of the public key is needed anymore. We studied several tools related to this primitive.

# 6. Contracts and Grants with Industry

## 6.1. Contracts with Industrial Partners

- **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.*
- **BACH: Biometric Authentication with Cryptographic Handling.**
  **Participants:** Michel Ferreira Abdalla, Malika Izabachène, David Pointcheval.

  From November 2005 to December 2009.
  Partners: Sagem, Cryptolog.
  *This project studies how to combine biometric data and cryptographic protocols, in order to preserve privacy.*
- **SAPHIR** *(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.

  From November 2005 to March 2009.
  Partners: France Telecom R&D, Gemalto, DCSSI, Cryptolog.
  *This project aims at improving recent attacks against hash functions, but also at designing new (provably secure) hash functions.*
- **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.

  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.**
  **Participant:** 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:** Georg Fuchsbauer, Malika Izabachène, David Pointcheval, 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, Céline Chevalier, Malika Izabachène, 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:** 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.*

## 6.2. Grants from Industry

- **Chaire ENS – France Télécom pour la sécurité des réseaux de télécommunications.**
  From January 2006 to December 2010.
  - Adi Shamir (The Weizmann Institute – Israel) – Invited Professor – 10 months, from September 2006 to September 2009
  - Mihir Bellare (UC San Diego – California – USA) – Invited Professor – 1 month, in June-July 2009
  - Orr Dunkelman – Post-doc – from April 2008 to September 2009
- **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

# 7. Other Grants and Activities

## 7.1. National Initiatives

- DGA/CELAR (Centre d'Electronique de l'Armement): **Provable security of cryptosystems.**
  **Participants:** Pierre-Alain Fouque, Georg Fuchsbauer, Gaëtan Leurent, David Pointcheval.

  From January 2007 to April 2009.
  *The goal of the contract is to make a survey on the methods and techniques used in provable security, for both cryptographic primitives and protocols.*

- **ARA FORMACRYPT: Formal security proofs for cryptographic protocols.**
  **Participant:** David Pointcheval.

  From January 2006 to December 2009.
  Partners: INRIA/Abstraction, INRIA/Secsi, INRIA/Cassis.
  *The verification of cryptographic protocols is a very active research area. Most works on this topic use either the computational approach, in which messages are bit strings, or the formal approach, in which messages are terms. The computational approach is more realistic but more difficult to automate. The goal of our project is to bridge the gap between these two approaches.*
- **ARA CrySCoE** *(Cryptographie pour la Sécurité des Codes Embarqués)*
  **Cryptography for the security of embedded systems.**
  **Participants:** David Naccache, David Pointcheval.

  From January 2006 to June 2009.
  Partners: UVSQ/Prism, Univ. Bordeaux I/LaBRI.
  *The goal of this project is to provide security and confidence to embedded systems: privacy of the code (obfuscation), integrity and authenticity of the code, security proof of correctness of the code (formal methods).*

## 7.2. National Grants

- **PhD DGA Grant.**
  Gaëtan Leurent, in PhD Thesis from October 2007 to September 2010
- **Post-Doc DGA Grant.**
  Aurélie Bauer, as a Post-doc from October 2008 to September 2009

# 8. Dissemination

## 8.1. Scientific Animation

- the CASCADE project-team organized the 7th Internal Conference on Applied Cryptography and Network Security, in June 2009
- we organized a workshop in honor of the 60th birthday of Jacques Stern, in September 2009: http://www.di.ens.fr/JS60.html
- a weekly seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html

## 8.2. Editorial Boards

Editor-in-Chief

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

Associate Editor

- of the *Journal of Cryptology*: Phong Nguyen
- of the *Journal of Mathematical Cryptology*: Phong Nguyen
- of *IET - Information Security*: David Naccache, David Pointcheval
- 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

## 8.3. Program Committees

- FSE – February 2009, Leuven, Belgium: Orr Dunkelman (chair)
- PKC – March 2009, Irvine, CA, USA: David Pointcheval
- CT-RSA – April 2009, San Francisco, CA, USA: Michel Abdalla
- EUROCRYPT – April 2009, Cologne, Germany: Pierre-Alain Fouque
- ACNS – June 2009, Paris, France: Michel Abdalla; David Pointcheval (co-chairs)
- AFRICACRYPT – June 2009, Gammarth, Tunisia: Michel Abdalla
- ISCC – July 2009, Sousse, Tunisia: David Naccache
- ACISP – July 2009, Brisbane, Australia: Michel Abdalla
- WEWoRC – July 2009, Graz, Austria: David Naccache
- PAIRING – August 2009, Palo Alto, CA, USA: Michel Abdalla
- CRYPTO – August 2009, Santa-Barbara, CA, USA: Phong Nguyen
- ICDF2C – September 2009, Albany, NY, USA: David Naccache
- FDTC – September 2009, Lausanne, Switzerland: David Naccache (co-chair), Mehdi Tibouchi, Damien Vergnaud
- SBSEG – September 2009, Campinas, SP, Brazil: Michel Abdalla (Keynote Speech and Tutorial Chair)
- NSS – October 2009, Gold Coast, Australia: David Pointcheval
- IWSEC – October 2009, Toyama, Japan: David Naccache
- ProvSec – November 2009, Guangzhou , China: Damien Vergnaud
- WISSEC – November 2009, Louvain-la-Neuve, Belgium: Damien Vergnaud
- IWISA – November 2009, Qingdao, China: David Naccache
- ASIACRYPT – December 2009, Tokyo, Japan: Phong Nguyen and David Pointcheval
- ICISC – December 2009, Seoul, South Korea: David Naccache
- WIFS – December 2009, London, UK: David Naccache (co-chair)
- MPIS – December 2009, Jeju island, Korea: David Naccache
- INTRUST – December 2009, Beijing, China: David Naccache

## 8.4. Responsibilities

### *8.4.1. Board of International Organizations*

- Chair of the Program Committee of FSE – Orr Dunkelman
- Chairs of the Program Committee of ACNS – Michel Abdalla and David Pointcheval
- General Chairs of ACNS – Pierre-Alain Fouque and Damien Vergnaud
- Board of the *International Association for Cryptologic Research* (IACR) – David Pointcheval – 2008–2010
- Selected Areas in Cryptography workshop board in Canada – Orr Dunkelman – 2008–2010
- 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

### *8.4.2. French Research Community*

- Recruitment committee at ENS: Jean Vuillemin, Pierre-Alain Fouque
- Foreign student recruitment committee at ENS: Pierre-Alain Fouque and Phong Nguyen
- INRIA-Rocquencourt seminar committee: Phong Nguyen

## 8.5. 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): David Pointcheval

M2 – Synchronous Systems (MPRI): Jean Vuillemin

M2 – Computer Security (ENSMSE): David Naccache

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

M2 – Cryptography (ESIEA): David Pointcheval

## 8.6. Ph.D/Habilitation Defenses

- Céline Chevalier – Ph.D. – 3 dec. 2009 – Université Paris VII – France
  *Étude de protocoles cryptographiques à base de mots de passe* [13]
- Malika Izabachène – Ph.D. – 1 oct. 2009 – Université Paris VII – France
  *L'anonymat dans les protocoles cryptographiques* [15]
- Cécile Delerablée – Ph.D. – 1 jul. 2009 – Université Paris VII – France
  *Cryptographie dans les groupes* [14]

## 8.7. Ph.D/Habilitation Committees

- Céline Chevalier – Ph.D. – 3 dec. 2009 – Université Paris VII – France
  *Étude de protocoles cryptographiques à base de mots de passe*
  David Pointcheval (supervisor), Jacques Stern (chair)
- Sébastien Canard – Habilitation – 2 dec. 2009 – Université de Caen – France
  *La Cryptographie au Service the la Protection de la Vie Privée*
  David Pointcheval (reviewer and chair)
- María Naya Plasencia – Ph.D. – 16 nov. 2009 – Université Paris VI – France
  *Chiffrements à flot et fonctions de hachage : conception et cryptanalyse*
  Pierre-Alain Fouque
- Assia Tria – Habilitation – 13 nov. 2009 – Ecole des Mines de Saint-Etienne – France
  *Sécurité des architectures matérielles*
  David Naccache
- Iwen Coisel – Ph.D. – 9 oct. 2009 – Université de Caen – France
  *Authentification et anonymat à bas-coût : modèles et protocoles*
  David Pointcheval

- Malika Izabachène – Ph.D. – 1 oct. 2009 – Université Paris VII – France
  *L'anonymat dans les protocoles cryptographiques*
  David Pointcheval (supervisor), David Naccache, Damien Vergnaud
- Guomin Yang – Ph.D. – 24 jul. 2009 – CU of Hong Kong
  *Security and Privacy in Wireless and Roaming Networks*
  David Pointcheval (reviewer)
- Yannick Seurin – Ph.D. – 1 jul. 2009 – UVSQ – France
  *Primitives et protocoles cryptographiques à sécurité prouvée*
  David Pointcheval (reviewer), Pierre-Alain Fouque
- Cécile Delerablée – Ph.D. – 1 jul. 2009 – Université Paris VII – France
  *Cryptographie dans les groupes*
  David Pointcheval (supervisor), Jacques Stern (chair)
- Sylvain Pasini – Ph.D. – 17 jun. 2009 – EPFL – Switzerland
  *Secure Communication Using Authenticated Channels*
  David Pointcheval (reviewer)
- Konstantin Hypponen – Ph.D. – 13 Mar. 2009 – Univ. of Kuopio – Finland
  *Open Mobile Identity - Secure identity management and mobile payments using Hand-Held Devices*
  David Naccache

## 8.8. Participation to Workshops and Conferences

FSE – February 2009, Leuven, Belgium: Charles Bouillaguet, Orr Dunkelman, Pierre-Alain Fouque, Gaëtan Leurent

The First SHA-3 Candidate Conference – February 2009, Leuven, Belgium: Orr Dunkelman, Gaëtan Leurent

TCC – March 2009, San Francisco, California, USA: Céline Chevalier, Georg Fuchsbauer, Damien Vergnaud

PKC – March 2009, Irvine, California, USA: Céline Chevalier, Georg Fuchsbauer, David Naccache, Damien Vergnaud

Franco-Japanese Computer Security Workshop – April 2009, Atagawa, Japan: Phong Nguyen, David Pointcheval

CT-RSA – April 2009, San Francisco, California, USA: Orr Dunkelman, Damien Vergnaud

Eurocrypt – April 2009, Cologne, Germany: Michel Abdalla, Aurélie Bauer, Charles Bouillaguet, Céline Chevalier, Léo Ducas, Pierre-Alain Fouque, David Naccache, Mehdi Tibouchi

Ecrypt hash function retreat – May 2009, Graz, Austria: Orr Dunkelman, Gaëtan Leurent

WPK – May 2009, Bertinoro, Italy: Michel Abdalla

ACNS – June 2009, Paris, France: Michel Abdalla, Aurélie Bauer, Pierre-Alain Fouque, Georg Fuchsbauer, Malika Izabachène, Phong Nguyen, David Pointcheval, Mehdi Tibouchi, Damien Vergnaud

AfricaCrypt – June 2009, Gammarth, Tunisia: Céline Chevalier

MITACS – June 2009, Grenoble, France: Michel Abdalla

VETO – June 2009, Grenoble, France: Damien Vergnaud

CIAA – July 2009, Sydney, Australia: Nicolas Gamma

ISSAC – July 2009, South Korea: Phong Nguyen

SAC – August 2009, Calgary, Canada: Charles Bouillaguet, Orr Dunkelman, Gaëtan Leurent

Pairing – August 2009, Stanford Univ, Palo Alto, California, USA: Michel Abdalla, Olivier Blazy, Georg Fuchsbauer, Malika Izabachène, Mehdi Tibouchi

Crypto – August 2009, Santa-Barbara, California, USA: Michel Abdalla, Olivier Blazy, Charles Bouillaguet, Orr Dunkelman, Georg Fuchsbauer, Malika Izabachène, Gaëtan Leurent, Phong Nguyen, David Pointcheval, Mehdi Tibouchi

SBSEG – September 2009, Campinas, SP, Brazil: Michel Abdalla

Journées C2 – October 2009, Fréjus, France: Aurélie Bauer, Olivier Blazy, Charles Bouillaguet, Damien Vergnaud

SEDAN – October 2009, Enschede, The Netherlands: Michel Abdalla

Ecrypt Hash$^3$ Worskop – November 2009, Tenerife, Spain: Gaëtan Leurent

WIFS – December 2009, London, UK : David Naccache

Asiacrypt – December 2009, Tokyo, Japan: Michel Abdalla, Léo Ducas, Pierre-Alain Fouque, Phong Nguyen, Mehdi Tibouchi, Damien Vergnaud

CANS – December 2009, Kanazawa, Ishikawa, Japan: Mehdi Tibouchi, Damien Vergnaud

ICISC – December 2009, Seoul, South Korea: Michel Abdalla, Mehdi Tibouchi

## 8.9. Invited Talks

- Franco-Japanese Computer Security Workshop, Atagawa, Japan (April): David Pointcheval
- MITACS, Grenoble, France (June): Michel Abdalla
- RSA Japan Conference, Japan (June): Phong Nguyen
- VETO 2009, Grenoble, France (June) : Damien Vergnaud
- XI Congress on Applied Mathematics, Spain (September): Phong Nguyen
- Journées C2, Fréjus, France (October): Aurélie Bauer
- SEDAN, Enschede, The Netherlans (October): Michel Abdalla
- ICISC, Seoul, South Korea (December): Michel Abdalla

## 8.10. Seminar Presentations

- NTT, Tokyo, Japan (April): David Pointcheval
- Univ. Catania, Italy (April): David Pointcheval
- Univ. Caen, France (May): Georg Fuchsbauer
- EPFL, Lausanne, Switzerland (June): David Pointcheval
- University of Bochum, Germany (July): Aurélie Bauer
- EWHA Univ. and Korea Univ., South Korea (July): Phong Nguyen
- Imperial College London, UK (August): Phong Nguyen
- UC San Diego, USA (August): Georg Fuchsbauer
- ENPC, Marne la Vallée, France (September): David Pointcheval
- Journées C2, Fréjus, France (Octobre): Olivier Blazy
- NTT, Tokyo, Japan (October): Phong Nguyen
- Royal Holloway, Univ. of London, Egham, UK (November): Georg Fuchsbauer

## 8.11. Visiting Researchers

- Mihir Bellare – UC San Diego, California, USA
- Xavier Boyen – Stanford Univ., California, USA

- Dennis Hofheinz – CWI, The Netherlands
- Vadim Lyubashevsky – Tel-Aviv Univ., Israel
- Adi Shamir – Weizmann Inst., Rehovot, Israel

# 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", vol. 21, n$^{o}$ 3, July 2008, 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, vol. 5677, Springer, 2009, 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, vol. 4117, Springer, 2006, 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, vol. 5157, Springer, 2008, 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, vol. 4622, Springer, 2007, 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, vol. 4622, Springer, 2007, 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, vol. 4965, Springer, 2008, p. 19–30.

[8] E. FUJISAKI, T. OKAMOTO, D. POINTCHEVAL, J. STERN. *RSA–OAEP is Secure under the RSA Assumption*, in "Journal of Cryptology", vol. 17, n$^{o}$ 2, 2004, 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. SMART, J. STERN. *Projective Coordinates Leak*, in "Advances in Cryptology – Proceedings of EUROCRYPT '04", Lecture Notes in Computer Science, vol. 3027, Springer, 2004, p. 257–267.

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

[12] P. Q. NGUYEN, D. STEHLÉ. *LLL on the Average*, in "Proceedings of the 7th International Algorithmic Number Theory Symposium (ANTS-VII)", Lecture Notes in Computer Science, vol. 4076, Springer, 2006, p. 238–256.

# Year Publications

## Doctoral Dissertations and Habilitation Theses

[13] C. CHEVALIER. *Étude de protocoles cryptographiques à base de mots de passe*, Université Paris VII, 2009, Ph. D. Thesis.

[14] C. DELERABLÉE. *Cryptographie dans les groupes*, Université Paris VII, 2009, Ph. D. Thesis.

[15] M. IZABACHÈNE. *L'anonymat dans les protocoles cryptographiques*, Université Paris VII, 2009, Ph. D. Thesis.

## Articles in International Peer-Reviewed Journal

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

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

[18] P. Q. NGUYEN, D. STEHLÉ. *Low-Dimensional Lattice Basis Reduction Revisited*, in "ACM Transactions on Algorithms", vol. 5, n$^{o}$ 4, 2009 AU .

[19] D. VERGNAUD. *Mesure d'indépendance linéaire de carrés de périodes et quasi-périodes de courbes elliptiques*, in "J. Number Theory", vol. 129, 2009, p. 1212-1233.

[20] D. VERGNAUD. *New Extensions of Pairing-based Signatures into Universal (Multi) Designated Verifier Signatures.*, in "Int. J. Found. Comput. Sci.", vol. 20, 2009, p. 109-133, To appear.

## International Peer-Reviewed Conference/Proceedings

[21] M. ABDALLA, X. BOYEN, C. CHEVALIER, D. POINTCHEVAL. *Distributed Public-Key Cryptography from Weak Secrets*, in "Conference on Practice and Theory in Public-Key Cryptography (PKC '09)", Lecture Notes in Computer Science, vol. 5443, Springer, 2009, p. 139–159 US .

[22] M. ABDALLA, D. CATALANO, C. CHEVALIER, D. POINTCHEVAL. *Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness*, in "Second African International Conference on Cryptology (AfricaCrypt '09)", Lecture Notes in Computer Science, vol. 5580, Springer, 2009, p. 254–271 IT .

[23] M. ABDALLA, D. CATALANO, D. FIORE. *Verifiable Random Functions from Identity based Key Encapsulation*, in "Advances in Cryptology – Proceedings of EUROCRYPT '09", Lecture Notes in Computer Science, vol. 5479, Springer, 2009, p. 554–571 IT .

[24] 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, vol. 5677, Springer, 2009, p. 671–689.

[25] E. ANDREEVA, C. BOUILLAGUET, O. DUNKELMAN, J. KELSEY. *Herding, Second Preimage and Trojan Message Attacks Beyond Merkle-Damgaard*, in "Advances in Cryptology – Proceedings of SAC'09", Lecture Notes in Computer Science, vol. 5867, Springer, 2009, p. 393–414 BE IL US .

[26] J.-P. AUMASSON, O. DUNKELMAN, S. INDESTEEGE, B. PRENEEL. *Cryptanalysis of Dynamic SHA(2)*, in "Proceedings of Selected Areas in Cryptography 2009", Lecture Notes in Computer Science, vol. 5867, Springer, 2009, p. 415-432 BE CH .

[27] J.-P. AUMASSON, O. DUNKELMAN, F. MENDEL, C. RECHBERGER, S. S. THOMSEN. *Cryptanalysis of Vortex*, in "Proceedings of Africacrypt 2009", Lecture Notes in Computer Science, vol. 5580, Springer, 2009, p. 14-28 CH AT DK .

[28] E. BRIER, D. NACCACHE, M. TIBOUCHI. *Factoring unbalanced moduli with known bits*, in "The 12th Annual International Conference on Information Security and Cryptology (ICISC '09)", Lecture Notes in Computer Science, Springer, 2009, To appear.

[29] S. CANARD, C. DELERABLÉE, A. GOUGET, E. HUFSCHMITT, F. LAGUILLAUMIE, H. SIBERT, J. TRAORÉ, D. VERGNAUD. *Fair E-Cash: Be Compact, Spend Faster*, in "Information Security, 12th International Conference, ISC 2009", Lecture Notes in Computer Science, Springer, 2009, p. 294-309.

[30] G. CASTAGNOS, A. JOUX, F. LAGUILLAUMIE, P. Q. NGUYEN. *Factoring $pq^2$ with Quadratic Forms: Nice Cryptanalyses*, in "Advances in Cryptology – Proceedings of ASIACRYPT '09", Lecture Notes in Computer Science, vol. 5912, Springer, 2009.

[31] J. CATHALO, D. NACCACHE, J.-J. QUISQUATER. *Comparing With RSA*, in "Cryptography and Coding, 12th IMA International Conference", Lecture Notes in Computer Science, Springer, 2009, To appear BE .

[32] C. CHEVALIER, P.-A. FOUQUE, D. POINTCHEVAL, S. ZIMMER. *Optimal Randomness Extraction from a Diffie-Hellman Element*, in "Advances in Cryptology – Proceedings of EUROCRYPT '09", Lecture Notes in Computer Science, vol. 5479, Springer, 2009, p. 572–589 IT .

[33] J.-S. CORON, A. JOUX, I. KIZHVATOV, D. NACCACHE, P. PAILLIER. *Fault Attacks on RSA Signatures with Partially Unknown Messages*, in "Cryptographic Hardware and Embedded Systems (CHES '09)", Lecture Notes in Computer Science, vol. 5747, Springer, 2009, p. 444-456 LU .

[34] J.-S. CORON, D. NACCACHE, M. TIBOUCHI, R.-P. WEINMANN. *Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures*, in "Advances in Cryptology - CRYPTO '09", Lecture Notes in Computer Science, vol. 5677, Springer, 2009, p. 428-444 LU .

[35] L. DALLOT, D. VERGNAUD. *Provably Secure Code-Based Threshold Ring Signatures*, in "Cryptography and Coding, 12th IMA International Conference", Lecture Notes in Computer Science, Springer, 2009, To appear.

[36] C. DE CANNIÈRE, O. DUNKELMAN, M. KNEZEVIC. *KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers*, in "Proceedings of CHES 2009", Lecture Notes in Computer Science, vol. 5747, Springer, 2009, p. 272-288 BE .

[37] O. DUNKELMAN, E. FLEISCHMANN, M. GORSKI, S. LUCKS. *Related-Key Rectangle Attack of the Full 80-Round HAS-160 Encryption Mode*, in "Proceedings of INDOCRYPT '09", Lecture Notes in Computer Science, Springer, 2009, To appear BE .

[38] O. DUNKELMAN, N. KELLER. *Cryptanalysis of CTC2*, in "Proceedings of CT-RSA 2009", Lecture Notes in Computer Science, vol. 5473, Springer, 2009, p. 226-239 IL .

[39] P.-A. FOUQUE, G. LEURENT, D. RÉAL, F. VALETTE. *Practical Electromagnetic Template Attack on HMAC*, in "Cryptographic Hardware and Embedded Systems (CHES '09)", Lecture Notes in Computer Science, vol. 5747, Springer, 2009, p. 66-80 US .

[40] G. FUCHSBAUER, D. POINTCHEVAL. *Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures*, in "Third International Conference on Pairing-based Cryptography (Pairing 2009)", Lecture Notes in Computer Science, vol. 5671, Springer, 2009, p. 132-149.

[41] G. FUCHSBAUER, D. POINTCHEVAL, D. VERGNAUD. *Transferable Anonymous Constant-Size Fair E-Cash*, in "The 8th International Workshop on Cryptology and Network Security (CANS '09)", Lecture Notes in Computer Science, Springer, 2009, To appear.

[42] M. IZABACHÈNE, D. POINTCHEVAL. *New Anonymity Notions for Identity-Based Encryption*, in "Formal to Practical Security", Lecture Notes in Computer Science, vol. 5458, Springer, 2009, p. 138–157.

[43] A. JOUX, R. LERCIER, D. NACCACHE, E. THOMÉ. *Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms*, in "Cryptography and Coding, 12th IMA International Conference", Lecture Notes in Computer Science, Springer, 2009, To appear.

[44] M. KAFI, S. GUILLEY, S. MARCELLO, D. NACCACHE. *Deconvolving Protected Signals*, in "Availability, Reliability and Security (ARES '09)", IEEE, 2009, p. 687-694.

[45] G. LEURENT, P. Q. NGUYEN. *How Risky Is the Random-Oracle Model?*, in "Advances in Cryptology – Proceedings of CRYPTO '09", Lecture Notes in Computer Science, vol. 5677, Springer, 2009, p. 445-464.

[46] B. LIBERT, D. VERGNAUD. *Adaptive-ID Secure Revocable Identity-Based Encryption*, in "Topics in Cryptology - CT-RSA 2009", Lecture Notes in Computer Science, Springer, 2009, p. 1-15 BE .

[47] B. LIBERT, D. VERGNAUD. *Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model*, in "The 8th International Workshop on Cryptology and Network Security (CANS '09)", Lecture Notes in Computer Science, Springer, 2009, To appear BE .

[48] B. LIBERT, D. VERGNAUD. *Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys*, in "Public Key Cryptography (PKC '09)", Lecture Notes in Computer Science, Springer, 2009, p. 235-255 BE .

[49] D. NACCACHE, R. STEINWANDT, M. YUNG. *Reverse Public Key Encryption*, in "Biometrics and Electronic Signatures - Research and Applications (BIOSIG '09)", Lecture Notes in Informatics, GI, vol. 155, Springer, 2009, To appear US .

[50] J. VUILLEMIN, N. GAMA. *Compact normal form for regular languages as xor automata*, in "14th International Conference on Implementation and Application of Automata (CIAA '09)", Lecture Notes in Computer Science, vol. 5642, Springer, 2009, p. 24–33.

[51] J. VUILLEMIN. *Efficient data structure and algorithms for sparse integers, sets and predicates*, in "19th IEEE Symposium on Computer Arithmetic", IEEE, 2009, p. 7–14.

### Scientific Books (or Scientific Book chapters)

[52] G. FUCHSBAUER, D. POINTCHEVAL. *Anonymous Consecutive Delegation of Signing Rights: Unifying Group and Proxy Signatures*, in "Formal to Practical Security", Lecture Notes in Computer Science, vol. 5458, Springer, 2009, p. 95–116.

[53] P. Q. NGUYEN. *Public-Key Cryptanalysis*, in "Recent Trends in Cryptography", I. LUENGO (editor), Contemporary Mathematics, vol. 477, AMS–RSME, 2009.

[54] 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, 2009, To appear.

### Books or Proceedings Editing

[55] M. ABDALLA, D. POINTCHEVAL, P.-A. FOUQUE, D. VERGNAUD (editors). *The 7th International Conference on Applied Cryptography and Network Security (ACNS '09)*, Lecture Notes in Computer Science, vol. 5536, Springer, 2009.

[56] O. DUNKELMAN (editor). *The 16th International Workshop Fast Software Encryption (FSE '09)*, Lecture Notes in Computer Science, vol. 5665, Springer, 2009.

[57] P. Q. NGUYEN, B. VALLÉE (editors). *The LLL Algorithm: Survey and Applications*, Information Security and Cryptography, Springer, 2009, To appear.

### Other Publications

[58] B. COURCELLE, G. KAHN, J. VUILLEMIN. *Algorithms for equivalence and reduction to minimal form for a class of simple recursive equations*, in "From Semantics to Computer Science, Essays in Honour of Gilles Kahn", Cambridge University Press, 2009.

## References in notes

[59] 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.

[60] E. ANDREEVA, C. BOUILLAGUET, P.-A. FOUQUE, J. J. HOCH, J. KELSEY, A. SHAMIR, S. ZIMMER. *Second Preimage Attacks on Dithered Hash Functions*, in "Advances in Cryptology - Proceedings of EUROCRYPT '08", Lecture Notes in Computer Science, vol. 4965, Springer, 2008, p. 270–288.

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

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

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

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

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

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

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

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

[69] J.-S. CORON, D. NACCACHE, J. P. STERN. *On the Security of RSA Padding*, in "Advances in Cryptology – CRYPTO '99", Lecture Notes in Computer Science, vol. 1666, Springer, 1999, p. 1-18.

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

[71] 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, vol. 263, Springer, 1987, p. 186–194.

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

[73] A. JOUX, D. NACCACHE, E. THOMÉ. *When e-th Roots Become Easier Than Factoring*, in "Advances in Cryptology - Proceedings of ASIACRYPT '07", Lecture Notes in Computer Science, vol. 4833, Springer, 2007, p. 13-28.

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

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

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

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

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

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

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

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

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

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

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

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

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

[87] 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, vol. 3494, Springer, 2005, p. 1–18.

[88] 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, vol. 3621, Springer, 2005, p. 17–36.

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

[90] 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, vol. 3621, Springer, 2005, p. 1–16.

[91] 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, vol. 4047, Springer, 2006, p. 89–110.

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