INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Cascade

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

Paris - Rocquencourt

THEME SYM

Table of contents

1. Team

Research Scientist

Michel Abdalla [CR, CNRS]
Phong 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

Charles Bouillaguet [Fondation EADS grant]
Céline Chevalier [AMN grant]
Cécile Delerablée [CIFRE grant – Orange Labs R&D]
Georg Fuchsbauer [EADS grant]
Nicolas Gama [AMN grant]
Malika Izabachène [University Paris 7 grant]
Serge Lefranc [DGA]
Gaëtan Leurent [DGA grant]
Eric Levieil [DGA grant]
Delphine Masgana [DGA]
Méhdi Tibouchi
Sébastien Zimmer [DGA]

Post-Doctoral Fellow

Aurélie Bauer [DGA grant]
Christophe de Cannière [Chaire ENS – France Télécom grant]
Julien Cathalo [Université Catholique de Louvain-la-Neuve, Belgique]
Orr Dunkelman [Chaire ENS – France Télécom grant]
Émeline Hufschmitt [ANR grant]

Administrative Assistant

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

2. Overall Objectives

2.1. Presentation

Cryptographic algorithms are the equivalent of locks, seals, security stamps and identification documents on the Internet. They are essential to protect our on-line bank transactions, credit cards, medical and personal information and to support e-commerce and e-government. They come in different flavors. Encryption algorithms are essential to protect sensitive information such as medical data, financial information and Personal Identification Numbers (PINs) from prying eyes. Digital signature algorithms (in combination with hash functions) replace hand-written signatures in electronic transactions. A similar role can be played by MAC algorithms. Identification protocols allow to securely verify the identity of the party at the other end of the line. Therefore, cryptology is a research area with a high strategic impact for industries, individuals, and for the society as a whole.

The research activity of the project-team CASCADE addresses the following topics, which cover almost all the domains that are currently active in the international cryptographic community:

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

2.2. Highlights

2.2.1. Foundation: Finding Short Lattice Vectors Within Mordell's Inequality

The shortest vector problem (SVP) in a lattice is a famous NP-hard problem of interest to both public-key cryptography and public-key cryptanalysis. Despite its importance, extremely few algorithms are known. This article presents the best polynomial-time algorithm known for approximating SVP. The algorithm, called slide reduction, has a natural interpretation: it can be viewed as an algorithmic version of a mathematical inequality proved by Mordell back in 1944.

The first polynomial-time algorithm for approximating SVP is the celebrated LLL algorithm, published by Lenstra, Lenstra and Lovász in 1982, and referenced by thousands of articles since: the historical applications of LLL were integer programming in fixed dimension, factoring polynomial with rational coefficients, and Diophantine approximation. The LLL algorithm is arguably best described as an algorithmic version of a mathematical inequality discovered by Hermite in 1850, which proved the existence of a constant related to lattice packings, now known as Hermite's constant. The principles and the worst-case output quality of the LLL algorithm are tightly related to Hermite's inequality.

In 1944, Mordell found a simple generalization of Hermite's inequality, which gave rise to better upper bounds on Hermite's constant. This article presents the first true algorithmic analogue of Mordell's inequality: the algorithm is to Mordell's inequality what LLL is to Hermite's inequality. As such, the new algorithm can be viewed as the "right" blockwise generalization of the LLL algorithm. Furthermore, it is simpler than previous blockwise generalizations of LLL, and a tight worst-case analysis is known.

2.2.2. Cryptanalysis: Cryptanalysis of SFLASH

Multivariate cryptography is a field of public-key cryptography which provides alternative schemes to RSA or Discrete-Log based schemes. The advantages of these schemes are twofold: they are extremely fast, even on low power devices since no cryptographic coprocessor is needed; and their security is related to a problem for which no quantum polynomial time algorithm is known. In 2003, the NESSIE project thus recommended the SFLASH signature scheme as a good scheme with high security level. This scheme has been proposed by Patarin, Goubin and Courtois in 2001. In multivariate cryptography, the public key is a system of multivariate polynomials over a small finite field. To sign a message with SFLASH, a trapdoor allows the legitimate user to invert the system, while the verification is very easy since it only requires to evaluate the system. The project-team CASCADE proposed in 2007 two attacks against SFLASH. These attacks are very efficient in practice since they require 3 minutes to break the parameters. The attacks allow an adversary to find a signature for any message. They only use linear and bilinear algebra and are based on some properties of the differential functions associated to the system of the public key. Studying the differential functions has also been proposed

by the project-team CASCADE in 2005 and allowed to cryptanalyze an encryption scheme whose security is related those of the SFLASH signature scheme. Finally, these attacks were recently extended and allow to recover equivalent secret keys on SFLASH and on other traitor tracing schemes based on other multivariate problems.

3. Scientific Foundations

3.1. Provable Security

Since the beginning of public-key cryptography, with the seminal Diffie-Hellman paper [69], many suitable algorithmic problems for cryptography have been proposed and many cryptographic schemes have been designed, together with more or less heuristic proofs of their security relative to the intractability of the underlying problems. However, many of those schemes have thereafter been broken. The simple fact that a cryptographic algorithm withstood cryptanalytic attacks for several years has often been considered as a kind of validation procedure, but schemes may take a long time before being broken. An example is the Chor-Rivest cryptosystem [68], based on the knapsack problem, which took more than 10 years to be totally broken [96], whereas before this attack it was believed to be strongly secure. The same happened more recently with multivariate cryptography [76], [88], [90], [89], [87], [71], [70] and [38]. In most of the recent cases, the project-team CASCADE was leading the cryptanalysis. 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) [75], 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" [86], 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 [72], 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" [80], [95]. 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 [94], [63], [91] which highlights the computational assumptions, and splits the analysis in small independent problems. We early adopted and developed this technique, and namely in [73].

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 [74], [81], [82], [83], 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 [93], [92], [78], [79], [77], 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], [97], [98], [99], [100], [102], [101] 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 just 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 just started (the call has been sent November 2nd, 2007, for submission before the end of 2008). In the first step, cryptographers had to build and analyze their own candidate; in a second step, cryptanalysts will be solicited, in order to analyze and break all the proposals. The conclusion is planned for 2012.

However, the main problem for hash functions is to identify the required security properties. Since they are used for many purposes, too many properties are often implicitly assumed, but not clearly stated, and clearly not satisfied. A lot of work has thus to be done one this topic of hash functions.

4.2. Stream Ciphers

Right after the selection of AES, research on block ciphers decreased: a strong block cipher is now available, with various security levels. However, AES does not solve the whole symmetric encryption problem, since encrypting streams of data, audio, video, etc requires *stream ciphers*. Modes of operation can of course be used, but they are often too costly. The eStream project has thus been launched by ECRYPT to address this lack of schemes. Now that the project is closed, stream ciphers remain a major issue in cryptography.

4.3. Anonymity and Privacy

Even if cryptography has been famous for addressing the problems of authenticity and confidentiality, by now, one of the main concerns of people is *privacy*. How can we live in this digital world, with bigger and bigger databases, really taking advantage of them, without the threat of “big brother”. Privacy and anonymity is thus one of the main challenges for the next years.

4.4. 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.

4.5. 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, he 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.

4.6. 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 Nguyen.

Finding Short Lattice Vectors Within Mordell's Inequality, STOC '08

The shortest vector problem (SVP) in a lattice is a famous NP-hard problem of interest to both public-key cryptography and public-key cryptanalysis. Despite its importance, extremely few algorithms are known. This article presents the best polynomial-time algorithm known for approximating SVP. The algorithm, called slide reduction, has a natural interpretation: it can be viewed as an algorithmic version of a mathematical inequality proved by Mordell back in 1944.

The first polynomial-time algorithm for approximating SVP is the celebrated LLL algorithm, published by Lenstra, Lenstra and Lovász in 1982, and referenced by thousands of articles since: the historical applications of LLL were integer programming in fixed dimension, factoring polynomial with rational coefficients, and Diophantine approximation. The LLL algorithm is arguably best described as an algorithmic version of a mathematical inequality discovered by Hermite in 1850, which proved the existence of a constant related to lattice packings, now known as Hermite's constant. The principles and the worst-case output quality of the LLL algorithm are tightly related to Hermite's inequality.

In 1944, Mordell found a simple generalization of Hermite's inequality, which gave rise to better upper bounds on Hermite's constant. This article presents the first true algorithmic analogue of Mordell's inequality: the algorithm is to Mordell's inequality what LLL is to Hermite's inequality. As such, the new algorithm can be viewed as the "right" blockwise generalization of the LLL algorithm. Furthermore, it is simpler than previous blockwise generalizations of LLL, and a tight worst-case analysis is known.

Predicting Lattice Reduction, EUROCRYPT '08

Despite their popularity, lattice reduction algorithms remain mysterious cryptanalytical tools. Though it has been widely reported that they behave better than their proved worst-case theoretical bounds, no precise assessment has ever been given. Such an assessment would be very helpful to predict the behaviour of lattice-based attacks, as well as to select keysizes for lattice-based cryptosystems. The goal of this paper is to provide such an assessment, based on extensive experiments performed with the NTL library. The experiments suggest several conjectures on the worst case and the actual behaviour of lattice reduction algorithms. We believe the assessment might also help to design new reduction algorithms overcoming the limitations of current algorithms.

Sieve Algorithms for the Shortest Vector Problem are Practical, Journal of Mathematical Cryptology 2008

We assess the practicality of the best (theoretical) algorithm known for exact SVP in low dimension: the sieve algorithm proposed by Ajtai, Kumar and Sivakumar (AKS) in 2001. AKS is a randomized algorithm of time and space complexity $2^{O(n)}$, which is theoretically much lower than the super-exponential complexity of all alternative SVP algorithms. Surprisingly, no implementation and no practical analysis of AKS has ever been reported. It was in fact widely believed that AKS was impractica. In this paper, we show that AKS can actually be made practical: we present a heuristic variant of AKS whose running time is $(4/3+\varepsilon)^n$ polynomial-time operations, and whose space requirement is $(4/3+\varepsilon)^{n/2}$ polynomially many bits. Our implementation can experimentally find shortest lattice vectors up to dimension 50, but is slower than classical alternative SVP algorithms in these dimensions

5.2. Cryptanalysis (Mathematical)

Participants: Vivien Dubois, Pierre-Alain Fouque, Phong Nguyen, Jacques Stern.

Cryptanalysis of SFLASH with Slightly Modified Parameters, EUROCRYPT '07

Practical Cryptanalysis of SFLASH, CRYPTO '07
Key Recovery on Hidden Monomial Multivariate Schemes, EUROCRYPT '08

Multivariate cryptography is a field of public-key cryptography which provides alternative schemes to RSA or Discrete-Log based schemes. The advantages of these schemes are two-folded: they are extremely fast, even on low power devices since no cryptographic coprocessor is needed; and their security is related to a problem for which no quantum polynomial time algorithm is known. In 2003, the NESSIE project thus recommended the SFLASH signature scheme as a good scheme with high security level. This scheme has been proposed by Patarin, Goubin and Courtois in 2001. In multivariate cryptography, the public key is a system of multivariate polynomials over a small finite field. To sign a message with SFLASH, a trapdoor allows the legitimate user to invert the system, while the verification is very easy since it only requires to evaluate the system. The project-team CASCADE proposed in 2007 two attacks against SFLASH. These attacks are very efficient in practice since they require 3 minutes to break the parameters. The attacks allow an adversary to find a signature for any message. They only use linear and bilinear algebra and are based on some properties of the differential functions associated to the system of the public key. Studying the differential functions has also been proposed by the project-team in 2005 and allowed to cryptanalyze an encryption scheme whose security is related those of the SFLASH signature scheme. Finally, these attacks were recently extended and allow to recover equivalent secret keys on SFLASH and on other traitor tracing schemes based on other multivariate problems.

Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures, Journal of Cryptology 2008

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.

5.3. Cryptanalysis (Symmetric)

Participants: Charles Bouillaguet, Pierre-Alain Fouque, Gaëtan Leurent, Phong Nguyen, Sébastien Zimmer.

Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5, CRYPTO '07
Message Freedom in MD4 and MD5 Collisions: Application to APOP, FSE '07
Second Preimage Attacks on Dithered Hash Functions, EUROCRYPT '08
MD4 is Not One-Way, SAC '08
Cryptanalysis of Tweaked Versions of SMASH and Reparation, SAC '08
Analysis of the Collision Resistance of Radiogatun using Algebraic Techniques, SAC '08
Cryptanalysis of a Hash Function Based on Quasi-Cyclic Codes, CT RSA '08

Since the attacks of Wang against the MD4 hash functions family in 2004, this area of research has been very active. At Crypto 2007, we showed how to adapt these attacks to break Message Authentication Code functions based on MD4 and MD5 and to break an authentication protocol used in the POP protocol at FSE.

This year, we showed that second preimage attacks can be mounted on a specific mode of operation designed by Ron Rivest to withstand generic second preimage attack on the Merkle-Damgard mode of operation at Eurocrypt '08. We also attack a hash function based on Coding Theory at CT RSA '08, another one proposed by Knudsen at SAC '08, and finally how to find preimage on MD4. Moreover, we show that Gröbner bases can be used on a recent hash function called Radiogatun to find colliding messages more efficiently than the technique proposed by the authors.

5.4. Cryptanalysis (Side-Channel)

Participant: Pierre-Alain Fouque.

The Carry Leakage on the Randomized Exponent Countermeasure, CHES '08
Fault Attack on Elliptic Curve with Montgomery Ladder, FDTC '08

At CHES 2008, we show that a very important countermeasure against DPA attacks, the randomization of the secret exponent using a multiple of $\varphi(N)$ or the order of the elliptic curve, can be attacked using a side channel attack that recovers the carry used in the addition of the secret key with a random value. The carry is leaked since such addition used large number, say 1024 bits packed in block of 8, 16 or 32 bits. Using statistic methods, we show that the carry of the addition of a fixed and secret value with a random value gives information on the secret.

At FDTC, we show that a fault attack on the abscissae of a compressed point on an elliptic curve cannot be detected and the Montgomery ladder works as the point were on the curve. However, with probability one half, the point lies on the twisted of the original elliptic curve and if the group order of the twisted is not prime, then a classical Pohlig-Hellman algorithm can be used to recover the secret scalar. This is the first attack on the Montgomery ladder with compressed representation and this algorithm has been promoted by various people as one of the most secure algorithm that computes the scalar multiplication on elliptic curve.

5.5. New Primitives

Participants: Michel Abdalla, Céline Chevalier, Cécile Delerablée, Georg Fuchsbauer, Malika Izabachène, David Pointcheval, Damien Vergnaud.

Unidirectional chosen-ciphertext secure proxy re-encryption, PKC '08
Tracing malicious proxies in proxy re-encryption, Pairing '08
Multi-use unidirectional proxy re-signatures, ACM CCS '08
Anonymous Proxy Signatures, SCN '08

In 1998, Blaze, Bleumer and Strauss put forth a cryptographic primitive, termed *proxy re-encryption*, whose goal is to securely enable the translation of ciphertexts from one party to another. In such systems, a proxy transforms – without being able to infer any information on the corresponding plaintext – a ciphertext computed under Alice's public key into one that can be opened using Bob's secret key. Recently, the project-team CASCADE has focused its research on delegation of rights: proxy re-encryption, as described above, and proxy signatures, which is the analogous delegation property for the signing rights.

New Anonymity Notions for Identity-Based Encryption, SCN '08
Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange, CANS '08

This year, anonymity has become a major topic, together with traceability (revokable anonymity). It thus shows some links with the group-oriented cryptography.

Dynamic Threshold Public-Key Encryption, CRYPTO '08

This paper deals with an efficient scheme which allows for some groups to decrypt documents. Dynamicity is also an important property in practice: the users can dynamically join the system (by opposition to static systems), authorized people in the groups can evolve dynamically too.

Multi-Factor Authenticated Key Exchange, ACNS '08
A Formal Study of the Privacy Concerns in Biometric-based Remote Authentication Schemes, ISPEC '08
Efficient Two-Party Password-Based Key Exchange Protocols in the UC Framework, CT-RSA '08

In these papers, we deal with various ways of authentication (password-based and biometrics).

Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Journal of Cryptology, 2008

There has recently been interest in various forms of “searchable encryption” in the literature. In this paper, we further explore one of the variants of this goal, namely public-key encryption with keyword search (PEKS) as introduced by Boneh, Di Crescenzo, Ostrovsky and Persiano in Eurocrypt 2004. A PEKS scheme allows the owner of a secret decryption key to give away pieces of trapdoor information based on this key that allows a third party to check whether a certain keyword is encrypted in a given ciphertext, without leaking any other information about the encrypted message however. The main application of PEKS schemes is to allow the intelligent routing of encrypted email containing certain keywords over a low-bandwidth connection. The user sends the trapdoor corresponding to the keyword to the mail server, who can then independently check encrypted emails for presence of that keyword.

In this paper, we identify and fill some gaps with regard to consistency (the extent to which false positives are produced) for PEKS. We define computational and statistical relaxations of the existing notion of perfect consistency, show that the scheme of Boneh et al. in Eurocrypt 2004 is computationally consistent, and provide a new scheme that is statistically consistent. We also provide a transform of an anonymous identity-based encryption (IBE) scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally, we suggest three extensions of the basic notions, namely anonymous hierarchical identity-based encryption, public-key encryption with temporary keyword search, and identity-based encryption with keyword search.

5.6. Hardware

Participants: Florian Praden, Jean Vuillemin.

Our experimental compiler (from C source to FPGA) [84], [85] was developped and tested against half a dozen very challenging applications, derived from industrial partners. sustained the full version of our "motion estimation algorithm", a very complex hardware design, by any measure. The design was successfully transferred to LetItWave, as part of our ANR contract.

This year has seen more robust technology transfer (through key ANR contracts), to two (RealViz and LetItWave) successful French high-tech startups.

From a more cryptographic point of view, we are also implementing a prototype for our candidate SIMD to the NIST Competition SHA-3 on FPGA.

6. Contracts and Grants with Industry

6.1. Contracts with Industrial Partners

- **ECRYPT: Network of Excellence in Cryptology.**
  From February 2004 to July 2008.
  The ECRYPT research roadmap is motivated by the changing environment (evolving toward ambient intelligence) and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, by the need of strong foundations in the watermarking area and by the requirements of new applications and cryptographic implementations.
  The main objective of ECRYPT is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas.
  There are five virtual labs that focus on the following core research areas: symmetric key algorithms (STVL), public key algorithms (AZTEC), protocols (PROVILAB), secure and efficient implementations (VAMPIRE), and watermarking (WAVILA).
  ENS/INRIA/CASCADE leads the AZTEC virtual lab and the ECRYPT strategic committee.

- **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.
- **Wired Smart**
  From December 2005 to June 2008.
  Partners: RealViz, ENPC/CERTIS, Mokros Image.
  Hardware implementation of image and video processing algorithms for special effects.
- **SUPERES: Super Resolution**
  From 2006 to 2008.
  Partners: Analog Way, LetItWave, Mokros Image, Vitec multimédia.
  This project deals with FPGA design & implementation of a key real-time algorithm in video interpolation, from low quality TV to HDTV.
- **BACH: Biometric Authentication with Cryptographic Handling.**
  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.
  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.
  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.
  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.**
  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.**
  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.

6.2. Grants from Industry

- **Chaire ENS – France Télécom pour la sécurité des réseaux de télécommunications.**
  From January 2006 to December 2009.
  - Adi Shamir (The Weizmann Institute – Israel) – Invited Professor – 9 months, from September 2006 to December 2008
  - Christophe de Cannière (KU Leuven – Belgium) – Post-doc – from October 2007 to September 2008
  - Orr Dunkelman (KU Leuven – Belgium) – Post-doc – from April 2008 to March 2009
- **CIFRE Grant with France Télécom.**
  Cécile Delerablée, in PhD Thesis from November 2005 to October 2008
- **EADS Grant.**
  Georg Fuchsbauer, in PhD Thesis from January 2007 to December 2009
- **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.**
  From January 2007 to December 2008.
  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.**
  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.
  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.**
  Eric Levieil, in PhD Thesis from October 2005 to September 2008
- **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

7.3. 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 *Information Processing Letters* – Elsevier: David Pointcheval

Guest Editor

– of the *Journal of Universal Computer Science* – Springer-Verlag – Volume 14 – Issue 3 – 2008
Special Issue on Cryptography in Computer System Security: David Pointcheval.
– of the *IET - Information Security* – IET – Volume 2 – Issue 3 – September 2008
Special Issue on Group-Oriented Cryptographic Protocols: David Pointcheval

7.4. Program Committees

ASIACCS March 2008, Tokyo, Japan: Michel Abdalla

PKC March 2008, Barcelona, Spain: Michel Abdalla

EUROCRYPT April 2008, Istanbul, Turkey: Phong Nguyen

ACISP July 2008, Wollongong, Australia: Michel Abdalla

ICALP July 2008, Reykjavik, Iceland: David Pointcheval

SAC August 2008, Sackville, Canada: Orr Dunkelman

SCN September 2008, Amalfi, Italy: Phong Nguyen

IWSEC November 2008, Kagawa, Japan: Michel Abdalla, Phong Nguyen

CANS December 2008, Hong Kong, China: Michel Abdalla

ASIACRYPT December 2008, Melbourne, Australia: David Pointcheval

7.5. Responsibilities

7.5.1. Board of International Organizations

- 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

7.5.2. French Research Community

- Recruitment committee at ENS: Pierre-Alain Fouque, Phong Nguyen, David Pointcheval
- ANR expert: David Pointcheval
- AERES visiting committee: David Pointcheval

8. Dissemination

8.1. Teaching

M1 – Introduction to Cryptology (ENS) – Pierre-Alain Fouque Jacques Stern

M1 – Introduction to Cryptology (EPITA) – Phong Nguyen

M2 – Number theory and Cryptography (MPRI) – Pierre-Alain Fouque, Phong Nguyen, David Pointcheval

M2 – Synchronous Systems (MPRI) – Jean Vuillemin

M2 – Computer Security (ENSMSE) – David Naccache

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

M2 – Cryptolography (ESIEA) – David Pointcheval

8.2. Ph.D./Habilitation Committees

Nicolas Gama – Ph.D. – 13 nov. 2008 – Université Paris VII – France
Géométrie des nombres et cryptanalyse de NTRU
Phong Nguyen (supervisor), Jacques Stern (chair)

Thomas Peyrin – Ph.D. – 3 nov. 2008 – Université Paris VII – France
Analyse de fonctions de hachage cryptographiques
Pierre-Alain Fouque

Eric Levieil – Ph.D. – 29 sept. 2008 – Université Paris VII – France
Contributions à l'étude cryptographique de protocoles et de primitives à clé secrète
Pierre-Alain Fouque, David Pointcheval (chair), Jacques Stern (supervisor)

Thomas Sirvent – Ph.D. – 26 sep. 2008 – Université de Rennes I – France
Courbes elliptiques et applications à la diffusion numérique sécurisée
David Pointcheval (reviewer)

Sébastien Zimmer – Ph.D. – 22 sep. 2008 – École polytechnique – France
Mécanismes cryptographiques pour la génération de clefs et l'authentification
Pierre-Alain Fouque, David Pointcheval (supervisor), Jacques Stern (chair)

Aurélie Bauer – Ph.D. – 15 sep. 2008 – Université Versailles Saint-Quentin-en-Yvelines – France
Vers une généralisation rigoureuse des méthodes de Coppersmith pour la recherche de petites racines de polynômes
Phong Nguyen, Jacques Stern (chair)

Hervé Chabanne – Habiliation – 27 apr. 2008 – Université Paris VII – France
Application de techniques cryptographiques à l'authentication biométrique
David Pointcheval, Jacques Stern (supervisor)

8.3. Participation to Workshops and Conferences

FSE February 2008, Lausanne, Switzerland, participants: Pierre-Alain Fouque, Phong Nguyen, Damien Vergnaud; Charles Bouillaguet, Gaëtan Leurent; Christophe de Cannière

PKC Marc 2008, Barcelona, Spain, participants: Damien Vergnaud; Emeline Hufschmitt

AsiaCCS March 2008, Tokyo, Japan, participants: Sébastien Zimmer

TCC March 2008, New-York, USA, participants: Michel Abdalla; Georg Fuchsbauer

CT-RSA April 2008, San Francisco, California, USA, participants: Michel Abdalla; Gaëtan Leurent; Orr Dunkelman

Eurocrypt April 2008, Istanbul, Turkey, participants: Pierre-Alain Fouque, David Naccache, Phong Nguyen, David Pointcheval, Damien Vergnaud; Charles Bouillaguet, Céline Chevalier, Cécile Delerablée, Georg Fuchsbauer, Nicolas Gama, Malika Izabachène, Sébastien Zimmer; Christophe de Cannière, Orr Dunkelman, Emeline Hufschmitt

STOC May 2008, Victoria, Canada, participants: Phong Nguyen; Nicolas Gama

ACNS June 2008, New-York, USA, participants: Sébastien Zimmer

SAC August 2008, Sackvill, Canada, participants: Charles Bouillaguet, Gaëtan Leurent, Sébastien Zimmer; Orr Dunkelman

Crypto August 2008, Santa-Barbara, California, USA, participants: Michel Abdalla, Pierre-Alain Fouque, David Pointcheval; Charles Bouillaguet, Céline Chevalier, Cécile Delerablée, Gaëtan Leurent; Christophe de Cannière

Pairing September 2008, London, UK, participants: Damien Vergnaud

SCN September 2008, Amalfi, Italy, participants: Georg Fuchsbauer, Malika Izabachène

CANS December 2008, Hong-Kong, participants: Malika Izabachène

Asiacrypt December 2008, Melbourne, Australia, participants: Damien Vergnaud; Nicolas Gama; Orr Dunkelman

Indocrypt December 2008, Kharagpur, India, participants: Orr Dunkelman

Franco-Japanese Computer Security Workshop , December 2008, Tokyo, Japan, participants: Phong Nguyen; Georg Fuchsbauer

8.4. Seminar Presentations

Georgia Tech , March, Atlanta, USA: Georg Fuchsbauer

ECRYPT Summer School , May 2008, Crete, Greece: Michel Abdalla

Rennes , June, Rennes, France: Orr Dunkelman

Leuven , July, Leuven, Belgium: Orr Dunkelman

IMDEA , July 2008, Madrid, Spain: Michel Abdalla

ENPC , September, Marne la Vallée, France: David Pointcheval

UFF Univ. , October 2008, Niterói, Rio de Janeiro, Brazil: Michel Abdalla

Tsinghua Univ. , October, Beijing, China: David Pointcheval

Univ. Bristol , November, Bristol, UK: Georg Fuchsbauer

Wollongong , December, Wollongong, Australia: Orr Dunkelman

8.5. Distinctions

- Jean Stern has been distinguished “Doctor Honoris Causa” from the Military Technical Academy at Bucharest, in Romania
- Jean Stern has been distinguished “Officier de la Légion d’Honneur”
- Jean Vuillemin received from the Academy of Sciences the “Prix de la fondation EADS pour les sciences de l’informatique et de leurs applications”

8.6. Visiting Researchers

Xavier Boyen Voltage Inc., California, USA

Dario Catalano Univ. Catania, Italy

Jonathan Katz Univ. Maryland, USA

Adam O’Neill (Ph.D. Student) Georgia Tech., Atlanta, USA

Oded Regev Univ. Tel Aviv, Israel

Sharmila Devaselvi Selvaraj (Ph.D. Student) IIT Madras, India

Adi Shamir Weizmann Inst., Rehovot, Israel

Sreevivek Sivanandam (Ph.D. Student) IIT Madras, India

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] 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.

[3] D. CATALANO, D. POINTCHEVAL, T. PORNIN. *Trapdoor-Hard-to-Invert Isomorphism and their Application to Password-based Authentication*, in "Journal of Cryptology", vol. 20, n^{o} 1, 2007, p. 115–149.

[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 "Advances in Cryptology – Proceedings of EUROCRYPT '06", Lecture Notes in Computer Science, vol. 4004, Springer, 2006, p. 215–233.

[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

Articles in International Peer-Reviewed Journal

[13] M. ABDALLA, J. H. AN, M. BELLARE, C. NAMPREMPRE. *From Identification to Signatures via the Fiat-Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security*, in "IEEE Transactions on Information Theory", vol. 54, n^{o} 8, August 2008, p. 3631–3646.

[14] 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.

[15] M. ABDALLA, E. KILTZ, G. NEVEN. *Generalized Key Delegation for Hierarchical Identity-Based Encryption*, in "IET Information Security", vol. 2, n^{o} 3, September 2008, p. 67–78.

[16] T. CLAVEIROLE, M. DIAS DE AMORIM, M. ABDALLA, Y. VINIOTIS. *Securing Wireless Sensor Networks Against Aggregator Compromises*, in "IEEE Communications Magazine", vol. 46, n^{o} 4, April 2008, p. 134–141.

[17] D. COPPERSMITH, J.-S. CORON, F. GRIEU, S. HALEVI, C. S. JUTLA, D. NACCACHE, J. P. STERN. *Cryptanalysis of ISO/IEC 9796-1*, in "Journal of Cryptology", vol. 21, n^{o} 1, 2008, p. 27–51.

[18] O. DUNKELMAN, N. KELLER. *Treatment of the Initial Value in Time-Memory-Data Tradeoff Attacks on Stream Ciphers*, in "Information Processing Letters", vol. 107, n^{o} 5, 2008, p. 133–137.

[19] G. LEURENT. *Practical key-recovery attack against APOP, an MD5-based challenge-response authentication*, in "International Journal of Applied Cryptography", vol. 1, n^{o} 1, 2008, p. 32–46.

[20] P. Q. NGUYEN, O. REGEV. *Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures*, in "J. of Cryptology", Published online: 11 November 2008. Printed version to appear, 2008.

[21] P. Q. NGUYEN, D. STEHLÉ. *Low-Dimensional Lattice Basis Reduction Revisited*, in "ACM Transactions on Algorithms", To appear, 2008.

[22] P. Q. NGUYEN, T. VIDICK. *Sieve Algorithms for the Shortest Vector Problem are Practical*, in "J. of Mathematical Cryptology", vol. 2, n^{o} 2, 2008.

[23] D. VERGNAUD. *Mesure d'indépendance linéaire de carrés de périodes et quasi-périodes de courbes elliptiques.*, in "J. Number Theory", To appear, 2008.

[24] D. VERGNAUD. *New Extensions of Pairing-based Signatures into Universal (Multi) Designated Verifier Signatures.*, in "Int. J. Found. Comput. Sci.", To appear, 2008.

International Peer-Reviewed Conference/Proceedings

[25] M. ABDALLA, D. CATALANO, C. CHEVALIER, D. POINTCHEVAL. *Efficient Two-Party Password-Based Key Exchange Protocols in the UC Framework*, in "The Cryptographers' Track at RSA Conference '08 (CT-RSA '08)", Lecture Notes in Computer Science, vol. 4964, Springer, 2008, p. 335–351.

[26] M. ABDALLA, M. IZABACHÈNE, D. POINTCHEVAL. *Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange*, in "The 7th International Conference on Cryptology and Network Security (CANS '08)", Lecture Notes in Computer Science, vol. 5339, Springer, 2008, p. 133–148.

[27] 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.

[28] C. BOUILLAGUET, P.-A. FOUQUE. *Analysis of the Collision Resistance of Radiogatun using Algebraic Techniques*, in "Selected Area in Cryptography '08 (SAC '08)", Lecture Notes in Computer Science, Springer, 2008, -.

[29] E. BRESSON, J. MONNERAT, D. VERGNAUD. *Separation Results on the "One-More" Computational Problems*, in "Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008,

San Francisco, CA, USA, April 8-11, 2008. Proceedings", T. MALKIN (editor), Lecture Notes in Computer Science, vol. 4964, Springer, 2008, p. 71-87.

[30] C. DE CANNIÈRE, Ö. KÜÇÜK, B. PRENEEL. *Analysis of Grain's Initialization Algorithm*, in "Proceedings of AFRICACRYPT '08", Lecture Notes in Computer Science, vol. 5023, Springer, 2008, p. 276–289.

[31] C. DE CANNIÈRE, C. RECHBERGER. *Preimages for Reduced SHA-0 and SHA-1*, in "Advances in Cryptology - Proceedings of CRYPTO '08", Lecture Notes in Computer Science, vol. 5157, Springer, 2008, p. 179–202.

[32] 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.

[33] O. DUNKELMAN, S. INDESTEEGE, N. KELLER. *Differential-Linear Attack on 12-Round Serpent*, in "Proceedings of INDOCRYPT '08", Lecture Notes in Computer Science, springer, 2008.

[34] O. DUNKELMAN, N. KELLER. *A New Attack on the LEX Stream Cipher*, in "Advances in Cryptology - Proceedings of ASIACRYPT '08", Lecture Notes in Computer Science, springer, 2008.

[35] O. DUNKELMAN, N. KELLER. *An Improved Impossible Differential Attack on MISTY1*, in "Advances in Cryptology - Proceedings of ASIACRYPT '08", Lecture Notes in Computer Science, springer, 2008.

[36] P.-A. FOUQUE, G. LEURENT. *Cryptanalysis of a Hash Function Based on Quasi-cyclic Codes*, in "The Cryptographers' Track at RSA Conference '08 (CT-RSA '08)", Lecture Notes in Computer Science, vol. 4964, Springer, 2008, p. 19–35.

[37] P.-A. FOUQUE, G. MACARIO-RAT, L. PERRET, J. STERN. *Total Break of the l-IC Signature Scheme*, in "Conference on Practice and Theory in Public-Key Cryptography (PKC '08)", Lecture Notes in Computer Science, vol. 4939, Springer, 2008, p. 1–17.

[38] 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.

[39] P.-A. FOUQUE, G. MARTINET, F. VALETTE, S. ZIMMER. *On the Security of the CCM Encryption Mode and of a Slight Variant*, in "Conference on Applied Cryptography and Network Security (ACNS '08)", Lecture Notes in Computer Science, vol. 5037, Springer, 2008, p. 411–428.

[40] P.-A. FOUQUE, D. POINTCHEVAL, S. ZIMMER. *HMAC is a Randomness Extractor and Applications to TLS*, in "Proceedings of the 3rd ACM Symposium on InformAtion, Computer and Communications Security (AsiaCCS '08)", ACM Press, 2008, p. 21–32.

[41] P.-A. FOUQUE, D. RÉAL, F. VALETTE, M. DRISSI. *The Carry Leakage on the Randomized Exponent Countermeasure*, in "Cryptographic Hardware and Embedded Systems '08 (CHES '08)", Lecture Notes in Computer Science, vol. 5154, Springer, 2008, p. 198-213.

[42] P.-A. FOUQUE, J. STERN, S. ZIMMER. *Cryptanalysis of Tweaked Versions of SMASH and Reparation*, in "Selected Area in Cryptography '08 (SAC '08)", Lecture Notes in Computer Science, Springer, 2008, -.

[43] G. FUCHSBAUER, D. POINTCHEVAL. *Anonymous Proxy Signatures*, in "The 6th Conference on Security in Communication Networks (SCN '08)", Lecture Notes in Computer Science, vol. 5229, Springer, 2008, p. 201–217.

[44] 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.

[45] N. GAMA, P. Q. NGUYEN. *Predicting Lattice Reduction*, in "Advances in Cryptology - Proc. EUROCRYPT '08", Lecture Notes in Computer Science, vol. 4965, Springer, 2008, p. 31-51.

[46] M. IZABACHÈNE, D. POINTCHEVAL. *New Anonymity Notions for Identity-Based Encryption*, in "The 6th Conference on Security in Communication Networks (SCN '08)", Lecture Notes in Computer Science, vol. 5229, Springer, 2008, p. 375–391.

[47] N. K. JIQIANG LU, J. KIM. *New Impossible Differential Attacks on AES*, in "Proceedings of INDOCRYPT '08", Lecture Notes in Computer Science, springer, 2008.

[48] G. LEURENT. *MD4 is Not One-Way*, in "FSE '08", Lecture Notes in Computer Science, vol. 5086, Springer, 2008, p. 412–428.

[49] E. LEVIEIL, D. NACCACHE. *Cryptographic Test Correction*, in "Public Key Cryptography (PKC '08)", vol. 4939, Springer, 2008, p. 85-100.

[50] B. LIBERT, D. VERGNAUD. *Multi-use unidirectional proxy re-signatures.*, in "Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008", P. NING, P. F. SYVERSON, S. JHA (editors), ACM, 2008, p. 511–520.

[51] B. LIBERT, D. VERGNAUD. *Tracing Malicious Proxies in Proxy Re-Encryption.*, in "Pairing-Based Cryptography (Pairing '08)", Lecture Notes in Computer Science, vol. 5209, Springer, 2008, p. 332–353.

[52] B. LIBERT, D. VERGNAUD. *Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption*, in "Public Key Cryptography (PKC '08)", Lecture Notes in Computer Science, vol. 4939, Springer, 2008, p. 360-379.

[53] D. POINTCHEVAL, S. ZIMMER. *Multi-Factor Authenticated Key Exchange*, in "Conference on Applied Cryptography and Network Security (ACNS '08)", Lecture Notes in Computer Science, vol. 5037, Springer, 2008, p. 277–295.

[54] Q. TANG, J. BRINGER, H. CHABANNE, D. POINTCHEVAL. *A Formal Study of the Privacy Concerns in Biometric-based Remote Authentication Schemes*, in "The 4th Information Security Practice and Experience Conference (ISPEC '08)", Lecture Notes in Computer Science, vol. 4991, Springer, 2008, p. 56–70.

Scientific Books (or Scientific Book chapters)

[55] P. Q. NGUYEN. *Public-Key Cryptanalysis*, I. LUENGO (editor), Contemporary Mathematics, To appear, AMS–RSME, 2008.

Other Publications

[56] O. DUNKELMAN. *Hash Functions — As You Like It*, in "TaiWan Information Security Center (TWISC) 2008", 2008.

[57] O. DUNKELMAN. *Hash Functions — Much Ado about Something*, in "Elliptic Curves Cryptography 2008", 2008.

[58] O. DUNKELMAN. *New Hash Function Proposals*, in "TaiWan Information Security Center (TWISC) 2008", 2008.

[59] O. DUNKELMAN. *Re-visiting HAIFA and why you should visit too*, in "Hash functions in cryptology: theory and practice (Lorentz Center)", 2008.

[60] O. DUNKELMAN. *Related-Key Attacks*, in "3rd ECRYPT PhD SUMMER SCHOOL Advanced Topics in Cryptography", 2008.

References in notes

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

[62] M. BELLARE, D. POINTCHEVAL, P. ROGAWAY. *Authenticated Key Exchange Secure against Dictionary Attacks*, in "Advances in Cryptology – EUROCRYPT 2000, Bruges, Belgium", B. PRENEEL (editor), Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, Berlin, Germany, May 14–18, 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 2006, St. Petersburg, Russia", S. VAUDENAY (editor), Lecture Notes in Computer Science, vol. 4004, Springer-Verlag, Berlin, Germany, May 28 – June 1, 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, Fairfax, Virginia, USA", V. ASHBY (editor), ACM Press, November 3–5, 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, Saragossa, Spain", U. M. MAURER (editor), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, Berlin, Germany, May 12–16, 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 "Eurocrypt '05", LNCS 3494, Springer-Verlag, Berlin, 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, Santa Barbara, CA, USA", G. R. BLAKLEY, D. CHAUM (editors), Lecture Notes in Computer Science, vol. 196, Springer-Verlag, Berlin, Germany, August 19–23, 1985, p. 54–65.

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

[70] 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, Submitted, Springer, 2007.

[71] V. DUBOIS, P. A. FOUQUE, J. STERN. *Cryptanalysis of SFLASH with Slightly Modified Parameters*, in "Advances in Cryptology – Proceedings of EUROCRYPT '07", Lecture Notes in Computer Science, To appear, Springer, 2007.

[72] A. FIAT, A. SHAMIR. *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, in "Advances in Cryptology – CRYPTO'86, Santa Barbara, CA, USA", A. M. ODLYZKO (editor), Lecture Notes in Computer Science, vol. 263, Springer-Verlag, Berlin, Germany, August 1987, p. 186–194.

[73] 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.

[74] N. GAMA, N. HOWGRAVE-GRAHAM, H. KOY, P. Q. NGUYEN. *Rankin's Constant and Blockwise Lattice Reduction*, in "Advances in Cryptology – Proceedings of CRYPTO '06", Lecture Notes in Computer Science, vol. 4117, Springer, 2006, p. 112-130.

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

[76] T. MATSUMOTO, H. IMAI. *Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption*, in "Advances in Cryptology – EUROCRYPT'88, Davos, Switzerland", C. G. GÜNTHER (editor), Lecture Notes in Computer Science, vol. 330, Springer-Verlag, Berlin, Germany, May 25–27, 1988, p. 419–453.

[77] NIST. *Descriptions of SHA–256, SHA–384, and SHA–512*, October 2000, http://www.nist.gov/sha/.

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

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

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

[81] P. Q. NGUYEN, D. STEHLÉ. *Floating-Point LLL Revisited*, in "Advances in Cryptology – Proceedings of EUROCRYPT '05", Lecture Notes in Computer Science, vol. 3494, Springer, 2005, p. 215–233.

[82] P. Q. NGUYEN, D. STEHLÉ. *Low-dimensional lattice basis reduction revisited*, in "Proceedings of the 6th International Algorithmic Number Theory Symposium, (ANTS-VI)", Lecture Notes in Computer Science, vol. 3076, Springer, 2004, p. 338–357.

[83] 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.

[84] J.-B. NOTE, J. VUILLEMIN. *Compiling synchronous kahn networks to efficient reconfigurable hardware*, Symposium in memory of Gilles Kahnn, Springer Verlag, 2007.

[85] J.-B. NOTE, J. VUILLEMIN. *Towards automatically compiling efficient fpga hardware*, International Workshop on Design and Functional Languages, IEEE, 2007, p. 115–124.

[86] K. OHTA, T. OKAMOTO. *On Concrete Security Treatment of Signatures Derived from Identification*, in "Advances in Cryptology – CRYPTO'98, Santa Barbara, CA, USA", H. KRAWCZYK (editor), Lecture Notes in Computer Science, vol. 1462, Springer-Verlag, Berlin, Germany, August 23–27, 1998, p. 354–369.

[87] J. PATARIN, L. GOUBIN, N. COURTOIS. *C^*_{-+} and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai*, in "Advances in Cryptology – ASIACRYPT'98, Beijing, China", K. OHTA, D. PEI (editors), Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, Berlin, Germany, October 18–22, 1998, p. 35–49.

[88] J. PATARIN. *Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*, in "Advances in Cryptology – CRYPTO'95, Santa Barbara, CA, USA", D. COPPERSMITH (editor), Lecture Notes in Computer Science, vol. 963, Springer-Verlag, Berlin, Germany, August 27–31, 1995, p. 248–261.

[89] J. PATARIN. *Asymmetric Cryptography with a Hidden Monomial*, in "Advances in Cryptology – CRYPTO'96, Santa Barbara, CA, USA", N. KOBLITZ (editor), Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, Berlin, Germany, August 18–22, 1996, p. 45–60.

[90] J. PATARIN. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, in "Advances in Cryptology – EUROCRYPT'96, Saragossa, Spain", U. M. MAURER (editor), Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, Berlin, Germany, May 12–16, 1996, p. 33–48.

[91] D. POINTCHEVAL. *« Provable Security for Public-Key Schemes »*, in "Advanced Course on Contemporary Cryptology", Advanced Courses CRM Barcelona, ISBN: 3-7643-7294-X (248 pages), Birkhäuser Publishers, Basel, June 2005, p. 133–189.

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

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

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

[95] V. SHOUP. *Lower Bounds for Discrete Logarithms and Related Problems*, in "Advances in Cryptology – EUROCRYPT'97, Konstanz, Germany", W. FUMY (editor), Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, Berlin, Germany, May 11–15, 1997, p. 256–266.

[96] S. VAUDENAY. *Cryptanalysis of the Chor-Rivest Cryptosystem*, in "Advances in Cryptology – CRYPTO'98, Santa Barbara, CA, USA", H. KRAWCZYK (editor), Lecture Notes in Computer Science, vol. 1462, Springer-Verlag, Berlin, Germany, August 23–27, 1998, p. 243–256.

[97] X. WANG, X. LAI, D. FENG, H. CHEN, X. YU. *Cryptanalysis of the Hash Functions MD4 and RIPEMD*, in "Eurocrypt '05", LNCS 3494, Springer-Verlag, Berlin, 2005, p. 1–18.

[98] X. WANG, Y. L. YIN, H. YU. *Finding Collisions in the Full SHA-1*, in "Crypto '05", LNCS 3621, Springer-Verlag, Berlin, 2005, p. 17–36.

[99] X. WANG, H. YU. *How to Break MD5 and Other Hash Functions*, in "Eurocrypt '05", LNCS 3494, Springer-Verlag, Berlin, 2005, p. 19–35.

[100] X. WANG, H. YU, Y. L. YIN. *Efficient Collision Search Attacks on SHA-0*, in "Crypto '05", LNCS 3621, Springer-Verlag, Berlin, 2005, p. 1–16.

[101] H. YU, X. WANG, A. YUN, S. PARK. *Cryptanalysis of the Full HAVAL with 4 and 5 Passes*, in "FSE '06", LNCS 4047, Springer-Verlag, Berlin, 2006, p. 89–110.

[102] H. YU, G. WANG, G. ZHANG, X. WANG. *The Second-Preimage Attack on MD4*, in "CANS '05", LNCS 3810, Springer-Verlag, Berlin, 2005, p. 1–12.