IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Paris

Activity Report 2013

Project-Team CASCADE

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

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

RESEARCH CENTER
Paris - Rocquencourt

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team CASCADE

Keywords: Security, Cryptography, Privacy, Identification, Complexity

Creation of the Project-Team: 2008 July 01.

1. Members

Research Scientists

David Pointcheval [Team leader, CNRS, Senior Researcher, HdR]
Michel Ferreira Abdalla [CNRS, Researcher, HdR]
Vadim Lyubashevsky [Inria, Researcher]
Hoeteck Wee [CNRS, Researcher, from Oct 2013]

Faculty Members

Maribel Fernandez [ENS Paris, Associate Professor, until Dec 2013, HdR]
David Naccache [Univ. Paris II, Professor, HdR]
Damien Vergnaud [ENS Paris, Associate Professor]

Engineer

Mario Strefler [Inria, ANR BEST project, until Sep 2013]

PhD Students

Patrick Derbez [ENS Paris, until Aug 2013]
Léo Ducas-Binda [ENS Paris, until Sep 2013]
Aurore Guillevic [Thales, CIFRE, until Dec 2013]
Houda Ferradi [Morpho, CIFRE]
Simon Cogliani [CS Systems, CIFRE]
Jérémy Jean [ENS Paris, until Dec 2013]
Tancrède Lepoint [CryptoExperts, CIFRE]
Diana Maimut
Sylvain Ruhault [Oppida]
Olivier Sanders [France Telecom, CIFRE]
Sonia Belaid [Thales]
Thomas Prest [Thales, CIFRE]
Fabrice Ben Hamouda [ENS Paris]
Alain Passelègue [ENS Paris, from Oct 2013]
Mario Cornejo Ramirez [Inria, from Dec 2013]
Adrian Thillard [ANSSI, from Oct 2013]

Post-Doctoral Fellows

Sorina Ionica [ENS Paris, until Dec 2013]
Itai Dinur [ENS Paris, from Sep 2013]
Elizabeth Quaglia [Inria, ANR BEST project, until Dec 2013]

Administrative Assistants

Nathalie Gaudechoux [Inria]
Joëlle Isnard [CNRS, 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, but mainly in the public-key area:

1. Implementation of cryptographic and applied cryptography
2. Design and provable security
3. Theoretical and concrete attacks

2.2. Design of Provably Secure Primitives and Protocols

Since the beginning of public-key cryptography, with the seminal Diffie-Hellman paper, 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, based on the knapsack problem, which took more than 10 years to be totally broken by Serge Vaudenay, 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), 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 many years, more efficient reductions have been expected, under the denomination of either "exact security" or "concrete security", which provide more practical security results, with concrete efficiency properties.

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". Similarly, block ciphers are identified with families of truly random permutations in the "ideal cipher model". Another kind of idealization has also been 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", extended to the bilinear and multi-linear setting. Some works even require several ideal models together to provide some new validations.

But still, such idealization cannot be instantiated in practice, and so one prefers to get provable security, without such ideal assumptions, under new and possibly stronger computational assumptions. As a consequence, a cryptographer has to deal with the four following important steps, which are **all** our main goals:

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.

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 security models for many primitives and protocols;
- 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.

3. Research Program

3.1. Randomness in Cryptography

Randomness is a key ingredient for cryptography. Random bits are necessary not only for generating cryptographic keys, but are also often an part of steps of cryptographic algorithms. In some cases, probabilistic protocols make it possible to perform tasks that are impossible deterministically. In other cases, probabilistic algorithms are faster, more space efficient or simpler than known deterministic algorithms. Cryptographers usually assumes that parties have access to perfect randomness but in practice this assumption is often violated and a large body of research is concerned with obtaining such a sequence of random or pseudorandom bits.

One of the project-team research goals is to get a better understanding of the interplay between randomness and cryptography and to study the security of various cryptographic protocols at different levels (information-theoretic and computational security, number-theoretic assumptions, design and provable security of new and existing constructions).

Cryptographic literature usually pays no attention to the fact that in practice randomness is quite difficult to generate and that it should be considered as a resource like space and time. Moreover since the perfect randomness abstraction is not physically realizable, it is interesting to determine whether imperfect randomness is “good enough” for certain cryptographic algorithms and to design algorithms that are robust with respect to deviations of the random sources from true randomness.

The power of randomness in computation is a central problem in complexity theory and in cryptography. Cryptographers should definitely take these considerations into account when proposing new cryptographic schemes: there exist computational tasks that we only know how to perform efficiently using randomness but conversely it is sometimes possible to remove randomness from probabilistic algorithms to obtain efficient deterministic counterparts. Since these constructions may hinder the security of cryptographic schemes, it is of high interest to study the efficiency/security tradeoff provided by randomness in cryptography.

Quite often in practice, the random bits in cryptographic protocols are generated by a pseudorandom number generation process. When this is done, the security of the scheme of course depends in a crucial way on the quality of the random bits produced by the generator. Despite the importance, many protocols used in practice often leave unspecified what pseudorandom number generation to use. It is well-known that pseudorandom generators exist if and only if one-way functions exist and there exist efficient constructions based on various number-theoretic assumptions. Unfortunately, these constructions are too inefficient and many protocols used in practice rely on "ad-hoc" constructions. It is therefore interesting to propose more efficient constructions, to analyze the security of existing ones and of specific cryptographic constructions that use weak pseudorandom number generators.

The project-team undertakes research in these three aspects. The approach adopted is both theoretical and practical, since we provide security results in a mathematical frameworks (information theoretic or computational) with the aim to design protocols among the most efficient known.

3.2. Lattice Cryptography

The security of almost all public-key cryptographic protocols in use today relies on the presumed hardness of problems from number theory such as factoring and discrete log. This is somewhat problematic because these problems have very similar underlying structure, and its unforeseen exploit can render all currently used public key cryptography insecure. This structure was in fact exploited by Shor to construct efficient quantum algorithms that break all hardness assumptions from number theory that are currently in use. And so naturally, an important area of research is to build provably-secure protocols based on mathematical problems that are unrelated to factoring and discrete log. One of the most promising directions in this line of research is using lattice problems as a source of computational hardness —in particular since they also offer features that other alternative public-key cryptosystems (such as MQ-based, code-based or hash-based schemes) cannot provide.

At its very core, secure communication rests on two foundations: authenticity and secrecy. Authenticity assures the communicating parties that they are indeed communicating with each other and not with some potentially malicious outside party. Secrecy is necessary so that no one except the intended recipient of a message is able to deduce anything about its contents.

Lattice cryptography might find applications towards constructing practical schemes for resolving essential cryptographic problems —in particular, guaranteeing authenticity. On this front, our team is actively involved in pursuing the following two objectives:

1. Construct, implement, and standardize a practical public key digital signature scheme that is secure against quantum adversaries.
2. Construct, implement, and standardize a symmetric key authentication scheme that is secure against side channel attacks and is more efficient than the basic scheme using AES with masking.

Despite the great progress in constructing fairly practical lattice-based encryption and signature schemes, efficiency still remains a very large obstacle for advanced lattice primitives. While constructions of identity-based encryption schemes, group signature schemes, functional encryption schemes, and even fully-homomorphic encryption schemes are known, the implementations of these schemes are extremely inefficient.

Fully Homomorphic Encryption (FHE) is a very active research area. Let us just give one example illustrating the usefulness of computing on encrypted data: Consider an on-line patent database on which firms perform complex novelty queries before filing patents. With current technologies, the database owner might analyze the queries, infer the invention and apply for a patent before the genuine inventor. While such frauds were not reported so far, similar incidents happen during domain name registration. Several websites propose "registration services" preceded by "availability searches". These queries trigger the automated registration of the searched domain names which are then proposed for sale. Algorithms allowing arbitrary computations without disclosing their inputs (and/or their results) are hence of immediate usefulness.

In 2009, IBM announced the discovery of a FHE scheme by Craig Gentry. The security of this algorithm relies on worst-case problems over ideal lattices and on the hardness of the sparse subset sum problem. Gentry's construction is an ingenious combination of two ideas: a somewhat homomorphic scheme (capable of supporting many "logical or" operations but very few "ands") and a procedure that refreshes the homomorphically processed ciphertexts. Gentry's main conceptual achievement is a "bootstrapping" process in which the somewhat homomorphic scheme evaluates its own decryption circuit (self-reference) to refresh (recrypt) ciphertexts.

Unfortunately, it is safe to surmise that if the state of affairs remains as it is in the present, then despite all the theoretical efforts that went into their constructions, these schemes will never be used in practical applications.

Our team is looking at the foundations of these primitives with the hope of achieving a breakthrough that will allow them to be practical in the near future.

3.3. Security amidst Concurrency on the Internet

Cryptographic protocols that are secure when executed in isolation, can be completely insecure when multiple such instances are executed concurrently (as is unavoidable on the Internet) or when used as a part of a larger protocol. For instance, a man-in-the-middle attacker participating in two simultaneous executions of a cryptographic protocol might use messages from one of the executions in order to compromise the security of the second – Lowe's attack on the Needham-Schroeder authentication protocol and Bleichenbacher's attack on SSL work this way. Our research addresses security amidst concurrent executions in secure computation and key exchange protocols.

Secure computation allows several mutually distrustful parties to collaboratively compute a public function of their inputs, while providing the same security guarantees as if a trusted party had performed the computation. Potential applications for secure computation include anonymous voting as well as privacy-preserving auctions and data-mining. Our recent contributions on this topic include

1. new protocols for secure computation in a model where each party interacts only once, with a single centralized server; this model captures communication patterns that arise in many practical settings, such as that of Internet users on a website,
2. and efficient constructions of universally composable commitments and oblivious transfer protocols, which are the main building blocks for general secure computation.

In key exchange protocols, we are actively involved in designing new password-authenticated key exchange protocols, as well as the analysis of the widely-used SSL/TLS protocols.

4. Application Domains

4.1. Privacy for the Cloud

Many companies have already started the migration to the Cloud and many individuals share their personal informations on social networks. While some of the data are public information, many of them are personal and even quite sensitive. Unfortunately, the current access mode is purely right-based: the provider first authenticates the client, and grants him access, or not, according to his rights in the access-control list. Therefore, the provider itself not only has total access to the data, but also knows which data are accessed, by whom, and how: privacy, which includes secrecy of data (confidentiality), identities (anonymity), and requests (obliviousness), should be enforced. Moreover, while high availability can easily be controlled, and thus any defect can immediately be detected, failures in privacy protection can remain hidden for a long time. The industry of the Cloud introduces a new implicit trust requirement: nobody has any idea at all of where and how his data are stored and manipulated, but everybody should blindly trust the providers. The providers will definitely do their best, but this is not enough. Privacy-compliant procedures cannot be left to the responsibility of the provider: however strong the trustfulness of the provider may be, any system or human vulnerability can be exploited against privacy. This presents too huge a threat to tolerate. *The distribution of the data and the secrecy of the actions must be given back to the users. It requires promoting privacy as a global security notion.*

In order to protect the data, one needs to encrypt it. Unfortunately, traditional encryption systems are inadequate for most applications involving big, complex data. Recall that in traditional public key encryption, a party encrypts data to a single known user, which lacks the expressiveness needed for more advanced data sharing. In enterprise settings, a party will want to share data with groups of users based on their credentials. Similarly, individuals want to selectively grant access to their personal data on social networks as well as documents and spreadsheets on Google Docs. Moreover, the access policy may even refer to users who do not exist in the system at the time the data is encrypted. Solving this problem requires an entirely new way of encrypting data.

A first natural approach would be **fully homomorphic encryption** (FHE, see above), but a second one is also **functional encryption**, that is an emerging paradigm for public-key encryption: it enables more fine-grained access control to encrypted data, for instance, the ability to specify a decryption policy in the ciphertext so that only individuals who satisfy the policy can decrypt, or the ability to associate keywords to a secret key so that it can only decrypt documents containing the keyword. Our work on functional encryption centers around two goals:

1. to obtain more efficient pairings-based functional encryption;
2. and to realize new functionalities and more expressive functional encryption schemes.

Another approach is **secure multi-party computation protocols**, where interactivity might provide privacy in a more efficient way. Recent implicit interactive proofs of knowledge can be a starting point. But stronger properties are first expected for improving privacy. They can also be integrated into new ad-hoc broadcast systems, in order to distribute the management among several parties, and eventually remove any trust requirements.

Strong privacy for the Cloud would have a huge societal impact since it would revolutionize the trust model: users would be able to make safe use of outsourced storage, namely for personal, financial and medical data, without having to worry about failures or attacks of the server.

4.2. Hardware Security

Cryptography is only one component of information security, but it is a crucial component. Without cryptography, it would be impossible to establish secure communications between users over insecure networks like the Internet. In particular, public-key cryptography (invented by Diffie and Hellman in 1976) enables to establish secure communications between users who have never met physically before. One can argue that companies like E-Bay or Amazon could not exist without public-key cryptography. Since 30 years the theory of cryptography has developed considerably. However cryptography is not only a theoretical science; namely at some point the cryptographic algorithms must be implemented on physical devices, such as PCs, smart cards or RFIDs. Then problems arise: in general smart cards and RFIDs have limited computing power and leak information through power consumption and electro-magnetic radiations. Similarly a PC can be exposed to various computer viruses which can leak private informations to a remote attacker. Such information leakage can be exploited by an attacker; this is called a **side-channel attack**. It is well known that a cryptographic algorithm which is perfectly secure in theory can be completely insecure in practice if improperly implemented.

In general, countermeasures against side-channel attacks are heuristic and can only make a particular implementation resist particular attacks. Instead of relying on ad-hoc security patches, a better approach consists in working in the framework of **provable security**. The goal is to prove that a cryptosystem does not only resist specific attacks but can resist any possible side-channel attack. As already demonstrated with cryptographic protocols, this approach has the potential to significantly increase the security level of cryptographic products. Recently the cryptography research community has developed new security models to take into account these practical implementation attacks; the most promising such model is called the **leakage-resilient model**.

Therefore, our goal is to define new security models that take into account any possible side-channel attack, and then to design new cryptographic schemes and countermeasures with a proven security guarantee against side-channel attacks.

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.

5. Partnerships and Cooperations

5.1. ANR Projects with Industrials

- **SAPHIR-II** *(Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes)*
  Security and analysis of innovating and recent hashing primitives.
  Participants: Patrick Derbez, Jérémy Jean.

  From April 2009 to March 2013.
  Partners: France Telecom R&D, Gemalto, EADS, SAGEM, DCSSI, Cryptolog, Inria/Secret, UVSQ, XLIM, CryptoExperts.
- **BEST: Broadcast Encryption for Secure Telecommunications.**
  Participants: David Pointcheval, Elizabeth Quaglia, Mario Strefler, Damien Vergnaud, Aurore Guillevic, Sorina Ionica.

  From December 2009 to December 2013.
  Partners: Thales, Nagra, CryptoExperts, Univ. Paris 8.
  This project aims at studying broadcast encryption and traitor tracing, with applications to the Pay-TV and geolocalisation services.
- **PRINCE: Proven Resilience against Information leakage in Cryptographic Engineering.**
  Participants: Fabrice Ben Hamouda, Sonia Belaid, Alain Passelègue, Michel Ferreira Abdalla, David Pointcheval.

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

  From February 2013 to August 2016.
  Partners: Orange Labs,INVIA, Oberthur Technologies, STMicroelectronics, Université Bordeaux 1, Université de Caen Basse-Normandie, Université de Paris VIII
  We aim at providing the most possible efficient and secure hardware/software implementation of a bilinear pairing in a SIM card.

5.2. ANR Projects within Academics

- **ProSe: Security protocols : formal model, computational model, and implementations.**
  Participant: David Pointcheval.

  From December 2010 to November 2014.
  Partners: ENS Cachan-Inria/Secsi, LORIA-Inria/Cassis, Inria/Prosecco, Verimag.
  The goal of the project is to increase the confidence in security protocols, and in order to reach this goal, provide security proofs at three levels: the symbolic level, in which messages are terms; the computational level, in which messages are bitstrings; the implementation level: the program itself.
- **ROMAnTIC: Randomness in Mathematical Cryptography.**
  Participants: Damien Vergnaud, David Pointcheval, Adrian Thillard, Sylvain Ruhault.

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

  From October 2013 to September 2017.
  Partners: UVSQ, Univ. Paris 8, Inria/SECRET.
  The main objective of this project is to explore the potential practical implications of the Learning with Errors problem and its variants. The plan is to focus on the constructions of essential primitives whose use is prevalent in the real world. Toward the end of the project, the hope is to propose and standardize several public key and symmetric key schemes that have specific advantages over ones that are currently deployed.

5.3. European Initiatives

- **ECRYPT-II: Network of Excellence in Cryptology.**
  From August 2008 to July 2013.
  There are three virtual labs that focus on the following core research areas: symmetric key algorithms (STVL), public key algorithms and protocols (MAYA), and secure and efficient implementations (VAMPIRE).
  ENS/Inria/CASCADE leads the MAYA virtual lab.
- **SecFuNet: Security for Future Networks.**
  From July 2011 to April 2014.
  The goal of the SECFUNET project is to design and develop a coherent security architecture for virtual networks and cloud accesses.

5.4. International Research Visitors

- Mario Cornejo (Ms student) – Chile
- Nuttapong Attrapadung – The National Institute of Advanced Industrial Science and Technology, Japan
- Yu Long – Shanghai Jiao Tong University, China

6. Dissemination

6.1. Editorial Boards

Editor-in-Chief

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

Associate Editor

  - of *Security and Communication Networks*: David Naccache (editor)
  - of *Journal of Cryptographic Design*: David Naccache (editor)
  - of *Encyclopedia of Cryptography and Security*: David Naccache (editor)
  - of *Journal of Computer Security, IOS Press*: David Naccache (associate editor)
  - of *Open Journal of Information Security and Applications, SOP*: David Naccache (editor)
  - of *Cryptologia* – Taylor & Francis: David Naccache (editor)
  - of *Information Processing Letters* – Elsevier: David Pointcheval
  - of *IEEE Transactions on Information Forensics and Security*: Michel Abdalla
  - of *IET Information Security*: Michel Abdalla

Columnist (in charge of the bi-monthly CryptoCorner)

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

6.2. Program Committees

- FIC - January, Lille, France: David Naccache
- ComManTel - January, Ho Chi Minh City, Vietnam: David Naccache
- PKC - February, Nara, Japan: David Naccache
- CT-RSA - February, San Francisco, USA: Michel Abdalla
- IIT - March, Al Ain, UAE: David Naccache
- WAHC - April, Okinawa, Japan: David Naccache
- LightSec - May, Gebze, Turkey: David Pointcheval
- Eurocrypt - May, Athens, Greece: Vadim Lyubashevsky
- ASIACCS - May, Hangzhou, China: David Naccache
- HOST - June, Austin, Texas, US: David Naccache
- ACISP - July, Brisbane, Australia: Michel Abdalla
- SECRYPT - July, Reykjavik, Iceland: David Naccache
- Indocrypt - July, Mumbai, India: David Naccache
- Crypto - August, Santa Barbara, USA: Vadim Lyubashevsky
- ICACCI (SSCC) - August, Mysore, India: David Naccache
- CHES - August, Santa Barbara, CA, USA: David Naccache
- SPACE - October, Kharagpur, India: David Naccache
- IWSEC - November, Okinawa, Japan: Damien Vergnaud
- RIVF - November, Hanoi, Vietam: David Naccache
- ICICS - November, Beijing, China: David Pointcheval, David Naccache
- Pairing - November, Beijing, China: Damien Vergnaud
- ISC - November, Dallas, Texas: David Naccache
- SBSeg - November, Manaus, Brazil: Michel Abdalla (Program Chair)
- ACM CCS - November, Berlin, Germany: David Naccache
- CANS - November, Paraty, Brazil: Michel Abdalla (Program Chair), Damien Vergnaud
- CARDIS - November, Berlin, Germany: David Naccache

- Asiacrypt - December, Bengaluru, India: Michel Abdalla, David Pointcheval, Hoeteck Wee
- IMACC - December, Oxford, UK: David Naccache
- Botconf - December, Nantes, France: David Naccache

6.3. Teaching - Supervision - Juries

6.3.1. Teaching

- Licence: David Naccache, Introduction to computer science, L1, Univ. Paris II
- Master: David Naccache, Scientific programming through practice, M1, ENS
- Master: David Naccache, Jacques Stern, Damien Vergnaud, Introduction to Cryptology, M1, ENS
- Master: Michel Abdalla, David Pointcheval, Vadim Lyubashevsky, Cryptography, M2, MPRI
- Master: David Naccache, Computer Security, M2, Univ. Paris II
- Master: David Naccache, Computer Security, M2, Beijing Jiaotong University
- Master: David Naccache, Risk Management, M2, Univ. Paris II
- Master: David Naccache, Computer Forensics, M2, Univ. Paris II
- Master: David Naccache, Computer Security, M2, University of Luxembourg
- Master: David Pointcheval, Cryptography, M2, ESIEA

6.3.2. Supervision

- PhD: Jérémy Jean, Cryptanalyse de primitives symétriques basées sur le chiffrement AES, September 24th 2013, Pierre-Alain Fouque
- PhD: Mario Strefler, Diffusion chiffrée avec traçage de traîtres, ENS, September 26th 2013, David Pointcheval
- PhD: Léo Ducas, Signatures fondées sur les réseaux euclidiens: attaques, analyses et optimisations, Univ. Paris 7, November 12th 2013, Phong Nguyen
- PhD: Patrick Derbez, Attaques par rencontre par le milieu sur l'AES, ENS, December 9th 2013, Pierre-Alain Fouque
- PhD: Aurore Guillevic, Étude de l'arithmétique des couplages sur des courbes algébriques pour la cryptographie, ENS, December 20th 2013, Phong Nguyen & Damien Vergnaud
- PhD in progress: Tancrède Lepoint, Lattice-based cryptography, 2011, Vadim Lyubashevsky & David Pointcheval
- PhD in progress: Sylvain Ruhault, Randomness in cryptography, 2011, David Pointcheval & Damien Vergnaud
- PhD in progress: Sonia Belaid, Leakage-resilient cryptography, 2012, Michel Abdalla
- PhD in progress: Fabrice Ben Hamouda, Leakage of information in cryptography, 2012, Michel Abdalla & David Pointcheval
- PhD in progress: Diana Maimut, Fully Homomorphic Encryption, 2012, David Naccache
- PhD in progress: Thomas Prest, Lattice-based cryptography, 2012, Vadim Lyubashevsky & David Pointcheval
- PhD in progress: Olivier Sanders, Delegation of computations, 2012, David Pointcheval
- PhD in progress: Mario Cornejo, Security for the cloud, 2013, Michel Abdalla
- PhD in progress: Alain Passelègue, Security against related-key attacks , 2013, Michel Abdalla
- PhD in progress: Adrian Thillard, Counter-measures against side-channel attacks and secure multi-party computation, 2013, Damien Vergnaud
- PhD in progress: Houda Ferradi, Biometric protocols and mobile security, 2013, David Naccache

- PhD in progress: Simon Cogliani, Authenticated Encryption, 2013, David Naccache

6.3.3. Juries

- PhD: Maria Christofi *Preuves de sécurité outillées d'implémentations cryptographiques* Univ. Versailles – Saint-Quentin, February 15th 2013: David Naccache
- PhD: Alfredo Rial, *Privacy-Preserving E-Commerce Protocols*, KU Leuven, Belgium, March 28th 2013: David Pointcheval
- HDR: Jessy Clédière *Treize années au Centre d'Evaluation de la Sécurité des Technologies de l'Information du CEA-Grenoble (CESTI-Léti)* Institut Néel (CNRS), Grenoble, June 19th 2013: David Naccache
- PhD: Alex Ruiz, *Contributions to Secret Sharing and Other Distributed Cryptosystems*, Univ. Politècnica de Catalunya, July 22nd 2013: Michel Abdalla
- PhD: David Oswald *Implementation Attacks: From Theory to Practice* Univ. Bochum, Germany, August 1st 2013: David Naccache
- HDR: Valérie Nachef *Cryptographie, Attaques génériques, Authentification* Univ. Cergy-Pontoise, September 25th 2013: David Naccache
- PhD: Mario Strefler, *Diffusion chiffrée avec traçage de traîtres*, ENS, September 26th 2013: David Pointcheval (supervisor), David Naccache
- PhD: Léo Ducas, *Signatures Fondées sur les Réseaux Euclidiens: Attaques, Analyses et Optimisations*, Univ. Paris 7, November 12th 2013: David Pointcheval, Vadim Lyubashevsky
- PhD: Jannik Dreier, *Formal Verification of Voting and Auction Protocols: From Privacy to Fairness and Verifiability*, Univ. Grenoble, November 25th 2013: David Pointcheval (chair)
- PhD: Sébastien Tiran *Side Channels in the Frequency Domain* Univ. Montpellier 2, December 11th 2013: David Naccache
- PhD: Patrick Derbez, *Attaques par Rencontre par le Milieu sur l'AES*, ENS, December 9th 2013: David Pointcheval
- PhD: Julien Devigne, *Protocoles de re-chiffrement pour le stockage de données*, Univ. de Caen – Basse-Normandie, December 13th 2013: Damien Vergnaud
- PhD: Viet Cuong Trinh, *Sécurité et efficacité des schémas de diffusion de données chiffrés*, Univ. Paris 8, December 19th 2013: Michel Abdalla, David Pointcheval
- PhD: Aurore Guillevic, *Étude de l'arithmétique des couplages sur les courbes algébriques pour la cryptographie*, ENS, December 20th 2013: David Pointcheval, Damien Vergnaud (advisor)

6.4. Invited Talks

6.4.1. At Conferences

- Vadim Lyubashevsky: "The LPN Problem in Cryptography" at the 14th IMA International Conference on Cryptography and Coding. Oxford, UK, December 2013
- David Naccache (common work with Roman Korkikian and Guilherme Ozari de Almeida:): "Instantaneous Frequency Analysis" at SECRYPT 2013, the 10th International Conference on Security and Cryptography. Reykjavik, Iceland, July, 2013
- David Naccache (common work with Eric Brier and Li-yao Xia): "How to Sign Paper Contracts? Conjectures & Evidence Related to Equitable & Efficient Collaborative Task Scheduling" at Open Problems in Mathematical and Computational Sciences Conference, Istanbul, Turkey, September 2013.
- David Naccache (common work with Hervé Chabanne, Jean-Michel Cioranesco, Vincent Despiegel and Jean-Christophe Fondeur) "Using Hamiltonian Totems as Passwords" at SantaCrypt 2013, Prague, Czech Republic, November 2013

6.4.2. At Organized Schools

- Vadim Lyubashevsky: “Lattice-Based Cryptography” at the Ecole de Printemps d’Informatique Theorique. Autrans, France, March 2013
- Vadim Lyubashevsky: “Lattice Cryptography” (5 hour course) at the Summer School on Lattices and FHE at Chongqing University. Chongqing, China, July 2013
- Vadim Lyubashevsky: “Lattice-Based Digital Signatures" at the Workshop on Lattice-Based Cryptography. Bangalore, India, December 2013

6.5. Scientific Animation

6.5.1. Organisation of Events

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

6.5.2. Steering Committees of International Conferences

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

6.5.3. Board of International Organizations

- Board of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2013 – 2015), David Pointcheval (2008–2016)

6.5.4. French Research Community

- Recruitment committee at Université of Rennes (PR 27): David Pointcheval
- Recruitment committee at Université of Versailles (MCF 27): Damien Vergnaud
- Recruitment committee at Université Paris 1 (PR 27): David Naccache
- Recruitment committee at Université Paris 2 (MCF 27): David Naccache
- Recruitment committee at Université Paris 2 (MCF 26): David Naccache
- Recruitment committee at École normale supérieure (MCF 27): Damien Vergnaud
- Recruitment committee at École normale supérieure (MCF 27): Damien Vergnaud
- Appointed member of the *Conseil National des Universités* (CNU): Damien Vergnaud
- Scientific board member, Agence pour les mathématiques en interaction avec l’entreprise et la société: David Naccache
- Scientific board member, Conseil supérieur de la formation et de la recherche stratégiques (CSFRS, a French government body): David Naccache
- Qualified Appointee, Banque de France’s Payment Security Observatory: David Naccache

7. Bibliography

Major publications by the team in recent years

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

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

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

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

[5] F. BENHAMOUDA, O. BLAZY, C. CHEVALIER, D. POINTCHEVAL, D. VERGNAUD. *New Techniques for SPHFs and Efficient One-Round PAKE Protocols*, in "CRYPTO (1)", R. CANETTI, J. A. GARAY (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8042, pp. 449-475

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

[7] J.-S. CORON, A. MANDAL, D. NACCACHE, M. TIBOUCHI. *Fully Homomorphic Encryption over the Integers with Shorter Public Keys*, in "Advances in Cryptology – Proceedings of CRYPTO '11", Lecture Notes in Computer Science, Springer, 2011, vol. 6841, pp. 487-504

[8] J.-S. CORON, D. NACCACHE, M. TIBOUCHI, R.-P. WEINMANN. *Practical Cryptanalysis of iso/iec 9796-2 and emv Signatures*, in "Advances in Cryptology – Proceedings of CRYPTO '09", Lecture Notes in Computer Science, Springer, 2009, vol. 5677, pp. 428-444

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

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

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

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

Publications of the year

Doctoral Dissertations and Habilitation Theses

[13] P. DERBEZ. , *Attaques par Rencontre par le Milieu sur l'AES*, Ecole Normale Supérieure de Paris - ENS Paris, December 2013, http://hal.inria.fr/tel-00918146

[14] A. GUILLEVIC. , *Étude de l'arithmétique des couplages sur les courbes algébriques pour la cryptographie*, Ecole Normale Supérieure de Paris - ENS Paris, December 2013, http://hal.inria.fr/tel-00921940

[15] J. JEAN. , *Cryptanalyse de primitives symetriques basees sur le chiffrement AES*, Ecole Normale Supérieure de Paris - ENS Paris, September 2013, http://hal.inria.fr/tel-00911049

[16] M. STREFLER. , *Diffusion chiffrée avec traçage de traîtres*, Ecole Normale Supérieure de Paris - ENS Paris, September 2013, http://hal.inria.fr/tel-00870910

Articles in International Peer-Reviewed Journals

[17] O. BLAZY, G. FUCHSBAUER, D. POINTCHEVAL, D. VERGNAUD. *Short Blind Signatures*, in "Journal of Computer Security", November 2013, vol. 21, n^{o} 5, pp. 627-661 [*DOI :* 10.3233/JCS-130477], http://hal.inria.fr/hal-00921915

[18] J.-M. CIORANESCO, H. FERRADI, D. NACCACHE. *Communicating Covertly through CPU Monitoring*, in "IEEE Security & Privacy", 2013, vol. 11, n^{o} 6, pp. 71-73 [*DOI :* 10.1109/MSP.2013.140], http://hal.inria.fr/hal-00934347

[19] J.-L. DANGER, S. GUILLEY, P. HOOGVORST, C. MURDICA, D. NACCACHE. *A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards*, in "Journal of Cryptographic Engineering", 2013, vol. 3, n^{o} 4, pp. 241-265 [*DOI :* 10.1007/s13389-013-0062-6], http://hal.inria.fr/hal-00934333

[20] M. FERREIRA ABDALLA, D. CATALANO, D. FIORE. *Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions*, in "Journal of Cryptology", May 2013 [*DOI :* 10.1007/s00145-013-9153-x], http://hal.inria.fr/hal-00915548

[21] S. IONICA. *Pairing-based algorithms for Jacobians of genus 2 curves with maximal endomorphism ring*, in "Journal of Number Theory", July 2013, vol. 133, pp. 3755-3770 [*DOI :* 10.1016/j.jnt.2013.04.023], http://hal.inria.fr/hal-00675045

[22] J. JEAN, M. NAYA-PLASENCIA, T. PEYRIN. *Improved Cryptanalysis of AES-like Permutations*, in "Journal of Cryptology", July 2013, http://hal.inria.fr/hal-00907706

[23] V. LYUBASHEVSKY, C. PEIKERT, O. REGEV. *On Ideal Lattices and Learning with Errors over Rings*, in "Journal of the ACM", November 2013, vol. 60, n^{o} 6 [*DOI :* 10.1145/2535925], http://hal.inria.fr/hal-00921792

[24] H. Q. NGO, D. H. PHAN, D. POINTCHEVAL. *Black-Box Trace&Revoke Codes*, in "Algorithmica", November 2013, vol. 67, n^{o} 3, pp. 418-448 [*DOI :* 10.1007/s00453-012-9702-y], http://hal.inria.fr/hal-00763979

[25] D. H. PHAN, D. POINTCHEVAL, S. FAYYAZ SHAHANDASHTI, M. STREFLER. *Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts*, in "International Journal of Information Security", August 2013, vol. 12, n^{o} 4, pp. 251-265 [*DOI :* 10.1007/s10207-013-0190-0], http://hal.inria.fr/hal-00864357

Invited Conferences

[26] E. BRIER, D. NACCACHE, L.-Y. XIA. *How to Sign Paper Contracts? Conjectures & Evidence Related to Equitable & Efficient Collaborative Task Scheduling*, in "Open Problems in Mathematical and Computational Sciences Conference", Istanbul, Turkey, 2013, http://hal.inria.fr/hal-00934345

[27] C. CHEVALIER, D. GAUMONT, D. NACCACHE. *How to (Carefully) Breach a Service Contract?*, in "Open Problems in Mathematical and Computational Sciences Conference", Istambul, Turkey, 2013, http://hal.inria.fr/hal-00934343

[28] R. KORKIKIAN, D. NACCACHE, G. OZARI DE ALMEIDA. *Instantaneous Frequency Analysis*, in "DCNET/ICE-B/OPTICS 2013: IS-11 - 4th International Conference on Data Communication Networking, 10th International Conference on e-Business and 4th International Conference on Optical Communication Systems", Reykjavík, Iceland, SciTePress, 2013, http://hal.inria.fr/hal-00934340

International Conferences with Proceedings

[29] F. BENHAMOUDA, O. BLAZY, C. CHEVALIER, D. POINTCHEVAL, D. VERGNAUD. *Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages*, in "Public-Key Cryptography - PKC 2013", Nara, Japan, K. KUROSAWA, G. HANAOKA (editors), LNCS, Springer, February 2013, vol. 7778, pp. 272-291 [*DOI :* 10.1007/978-3-642-36362-7_18], http://hal.inria.fr/hal-00790633

[30] F. BENHAMOUDA, O. BLAZY, C. CHEVALIER, D. POINTCHEVAL, D. VERGNAUD. *New Techniques for SPHFs and Efficient One-Round PAKE Protocols*, in "CRYPTO 2013 - 33rd Annual Cryptology Conference", Santa Barbara, CA, United States, R. CANETTI, J. A. GARAY (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8042, pp. 449-475 [*DOI :* 10.1007/978-3-642-40041-4_25], http://hal.inria.fr/hal-00864345

[31] O. BLAZY, C. CHEVALIER, D. POINTCHEVAL, D. VERGNAUD. *Analysis and Improvement of Lindell's UC-Secure Commitment Schemes*, in "ACNS 2013 - 11th International Conference Applied Cryptography and Network Security", Banff, Canada, M. JACOBSON, M. LOCASTO, P. MOHASSEL, R. SAFAVI-NAINI (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7954, pp. 534-551 [*DOI :* 10.1007/978-3-642-38980-1_34], http://hal.inria.fr/hal-00865612

[32] S. CANARD, D. POINTCHEVAL, O. SANDERS. *Efficient Delegation of Zero-Knowledge Proofs of Knowledge in a Pairing-Friendly Setting*, in "17th International Conference on Practice and Theory in Public-Key Cryptography (PKC '14)", Buenos Aires, Argentina, H. KRAWCZYK (editor), LNCS, Springer, March 2014, vol. 8383, pp. 167-183, http://hal.inria.fr/hal-00940045

[33] H. CHABANNE, J.-M. CIORANESCO, V. DESPIEGEL, J.-C. FONDEUR, D. NACCACHE. *Using Hamiltonian Totems as Passwords*, in "SantaCrypt 2013", Prague, Czech Republic, 2013, http://hal.inria.fr/hal-00934341

[34] J. CHEON, J.-S. CORON, J. KIM, M. LEE, T. LEPOINT, M. TIBOUCHI, A. YUN. *Batch Fully Homomorphic Encryption over the Integers*, in "EUROCRYPT - 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques - 2013", Athens, Greece, T. JOHANSSON, P. Q. NGUYEN (editors), Lecture Notes in Computer Science, Springer, May 2013, vol. 7881, pp. 315-335 [*DOI :* 10.1007/978-3-642-38348-9_20], http://hal.inria.fr/hal-00864327

[35] C. DELERABLÉE, T. LEPOINT, P. PAILLIER, M. RIVAIN. *White-Box Security Notions for Symmetric Encryption Schemes*, in "SAC 2013 - Conference Selected Areas in Cryptography", Burnaby, British Columbia, Canada, August 2013, http://hal.inria.fr/hal-00872841

[36] P. DERBEZ, P.-A. FOUQUE, J. JEAN. *Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting*, in "EUROCRYPT 2013", Athens, Greece, May 2013, Publié à EUROCRYPT 2013, http://hal.inria.fr/hal-00870449

[37] Y. DODIS, D. POINTCHEVAL, S. RUHAULT, D. VERGNAUD, D. WICHS. *Security Analysis of Pseudo-Random Number Generators with Input: /dev/random is not Robust*, in "ACM CCS 2013 - 20th ACM Conference on Computer and Communications Security", Berlin, Germany, ACM, November 2013 [*DOI :* 10.1145/2508859.2516653], http://hal.inria.fr/hal-00864431

[38] L. DUCAS, A. DURMUS, T. LEPOINT, V. LYUBASHEVSKY. *Lattice signatures and bimodal Gaussians*, in "CRYPTO 2013 - 33rd Annual Cryptology Conference", Santa Barbara, United States, R. CANETTI, J. A. GARAY (editors), Lecture Notes in Computer Science, Springer, August 2013, vol. 8042, pp. 40-56 [*DOI :* 10.1007/978-3-642-40041-4_3], http://hal.inria.fr/hal-00864298

[39] M. FERREIRA ABDALLA, S. BELAID, P.-A. FOUQUE. *Leakage-Resilient Symmetric Encryption via Re-keying*, in "Cryptographic Hardware and Embedded Systems - CHES 2013", Santa Barbara, United States, G. BERTONI, J.-S. CORON (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8086, pp. 471-488 [*DOI :* 10.1007/978-3-642-40349-1_27], http://hal.inria.fr/hal-00870955

[40] M. FERREIRA ABDALLA, F. BENHAMOUDA, O. BLAZY, C. CHEVALIER, D. POINTCHEVAL. *SPHF-Friendly Non-Interactive Commitments*, in "ASIACRYPT 2013", Bangalore, India, K. SAKO, P. SARKAR (editors), Lecture Notes in Computer Science, Springer, December 2013, vol. 8269, pp. 214-234 [*DOI :* 10.1007/978-3-642-42033-7_12], http://hal.inria.fr/hal-00915542

[41] M. FERREIRA ABDALLA, F. BENHAMOUDA, D. POINTCHEVAL. *Tighter Reductions for Forward-Secure Signature Scheme*, in "Public-Key Cryptography (PKC 2013)", Nara, Japan, K. KUROSAWA, G. HANAOKA (editors), LNCS, Springer, February 2013, vol. 7778, pp. 292-311 [*DOI :* 10.1007/978-3-642-36362-7_19], http://hal.inria.fr/hal-00790626

[42] P.-A. FOUQUE, J. JEAN, T. PEYRIN. *Structural Evaluation of AES and Chosen-Key Distinguisher of 9-round AES-128*, in "CRYPTO 2013", Santa Barbara, United States, August 2013, Publié à CRYPTO 2013, http://hal.inria.fr/hal-00870453

[43] P.-A. FOUQUE, D. VERGNAUD, J.-C. ZAPALOWICZ. *Time/Memory/Data Tradeoffs for Variants of the RSA Problem*, in "Computing and Combinatorics, 19th International Conference, COCOON 2013", Hangzhou, China, D.-Z. DU, G. ZHANG (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7936, pp. 651-662 [*DOI :* 10.1007/978-3-642-38768-5_57], http://hal.inria.fr/hal-00871319

[44] A. GUILLEVIC. *Comparing the Pairing Efficiency over Composite-Order and Prime-Order Elliptic Curves*, in "ACNS - 11th International Conference on Applied Cryptography and Network Security - 2013", Banff, Canada, April 2013, http://hal.inria.fr/hal-00812960

[45] A. GUILLEVIC, S. IONICA. *Four-Dimensional GLV via the Weil Restriction*, in "Asiacrypt - 19th Annual International Conference on the Theory and Application of Cryptology and Information Security", Bengalore, India, K. SAKO, P. SARKAR (editors), Springer, September 2013, http://hal.inria.fr/hal-00864966

[46] A. GUILLEVIC, D. VERGNAUD. *Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions*, in "Pairing-Based Cryptography - Pairing 2012", Cologne,

Germany, M. FERREIRA ABDALLA, T. LANGE (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7708, pp. 234-253, http://hal.inria.fr/hal-00871327

[47] J. JEAN, M. NAYA-PLASENCIA, T. PEYRIN. *Multiple Limited-Birthday Distinguishers and Applications*, in "Selected Areas in Cryptography - SAC 2013", Vancouver, Canada, August 2013, To appear, http://hal.inria.fr/hal-00870452

[48] J. JEAN, I. NIKOLIC, T. PEYRIN, L. WANG, S. WU. *Security Analysis of PRINCE*, in "FSE 2013", Singapore, Singapore, March 2013, Publié à FSE 2013, http://hal.inria.fr/hal-00870448

[49] T. LEPOINT, J.-S. CORON, M. TIBOUCHI. *Practical Multilinear Maps over the Integers*, in "CRYPTO 2013 - 33rd Annual Cryptology Conference Advances in Cryptology", Santa-Barbara, United States, R. CANETTI, J. A. GARAY (editors), Lecture Notes in Computer Science, Springer, August 2013, vol. 8042, pp. 476-493 [*DOI :* 10.1007/978-3-642-40041-4_26], http://hal.inria.fr/hal-00872773

[50] T. LEPOINT, P. PAILLIER. *On the Minimal Number of Bootstrappings in Homomorphic Circuits*, in "Workshop on Applied Homomorphic Cryptography", Okinawa, Japan, A. A. ADAMS, M. BRENNER, M. SMITH (editors), Lecture Notes in Computer Science, Springer, April 2013, vol. 7862, pp. 189-200 [*DOI :* 10.1007/978-3-642-41320-9_13], http://hal.inria.fr/hal-00872833

[51] T. LEPOINT, M. RIVAIN, Y. DE MULDER, B. PRENEEL, P. ROELSE. *Two Attacks on a White-Box AES Implementation*, in "SAC 2013 - Conference Selected Areas in Cryptography", Burnaby, British Columbia, Canada, August 2013, http://hal.inria.fr/hal-00872844

[52] V. LYUBASHEVSKY, D. MASNY. *Man-in-the-Middle Secure Authentication Schemes from LPN and Weak PRFs*, in "CRYPTO 2013 - 33rd Annual Cryptology Conference", Santa Barbara, United States, R. CANETTI, J. A. GARAY (editors), Lecture Notes in Computer Science, Springer, August 2013, vol. 8043, pp. 308-325 [*DOI :* 10.1007/978-3-642-40084-1_18], http://hal.inria.fr/hal-00864299

[53] V. LYUBASHEVSKY, C. PEIKERT, O. REGEV. *A toolkit for Ring-LWE cryptography*, in "EUROCRYPT - 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques - 2013", Athens, Greece, T. JOHANSSON, P. Q. NGUYEN (editors), Lecture Notes in Computer Science, Springer, May 2013, vol. 7881, pp. 35-54 [*DOI :* 10.1007/978-3-642-38348-9_3], http://hal.inria.fr/hal-00864284

[54] D. MAIMUT, C. MURDICA, D. NACCACHE, M. TIBOUCHI. *Fault Attacks on Projective-to-Affine Coordinates Conversion*, in "COSADE 2013 - 4th International Workshop Constructive Side-Channel Analysis and Secure Design", Paris, France, Springer, 2013, pp. 46-61 [*DOI :* 10.1007/978-3-642-40026-1_4], http://hal.inria.fr/hal-00934335

[55] D. H. PHAN, D. POINTCHEVAL, V. C. TRINH. *Multi-channel broadcast encryption*, in "ASIA CCS '13 Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security", Hangzhou, China, ACM, 2013, pp. 277-286 [*DOI :* 10.1145/2484313.2484348], http://hal.inria.fr/hal-00864356

Conferences without Proceedings

[56] S. BELAID, L. BETTALE, E. DOTTAX, L. GENELLE, F. RONDEPIERRE. *Differential Power Analysis of HMAC SHA-2 in the Hamming Weight Model*, in "SECRYPT 2013 - 10th International Conference on Security and Cryptography", Reykjavik, Iceland, July 2013, http://hal.inria.fr/hal-00872410

Books or Proceedings Editing

[57] M. FERREIRA ABDALLA, T. LANGE (editors). , *Pairing-Based Cryptography - PAIRING 2012*, Lecture Notes in Computer Science, Springer, 2013, vol. 7708, 333 p. [*DOI :* 10.1007/978-3-642-36334-4], http://hal.inria.fr/hal-00915796

[58] M. FERREIRA ABDALLA, C. NITA-ROTARU, R. DAHAB (editors). , *CANS 2013*, Lecture Notes in Computer Science, Springer, November 2013, vol. 8257, 349 p. [*DOI :* 10.1007/978-3-319-02937-5], http://hal.inria.fr/hal-00915711

Research Reports

[59] E. BRIER, D. NACCACHE, L.-Y. XIA. , *How to Sign Paper Contracts? Conjectures & Evidence Related to Equitable & Efficient Collaborative Task Scheduling*, 2013, n° IACR Cryptology ePrint Archive 2013: 432 (2013), http://hal.inria.fr/hal-00934338

[60] H. CHABANNE, J.-M. CIORANESCO, V. DESPIEGEL, J.-C. FONDEUR, D. NACCACHE. , *Using Hamiltonian Totems as Passwords*, 2013, n° IACR Cryptology ePrint Archive 2013: 751 (2013), http://hal.inria.fr/hal-00934337

[61] J.-L. DANGER, S. GUILLEY, P. HOOGVORST, C. MURDICA, D. NACCACHE. , *Dynamic Countermeasure Against the Zero Power Analysis*, 2013, n° IACR Cryptology ePrint Archive 2013: 764 (2013), http://hal.inria.fr/hal-00934336

[62] R. KORKIKIAN, D. NACCACHE, G. OZARI DE ALMEIDA. , *Instantaneous Frequency Analysis*, 2013, n° IACR Cryptology ePrint Archive 2013: 320 (2013), http://hal.inria.fr/hal-00934334