IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Paris

Activity Report 2014

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 Abdalla [CNRS, Researcher, HdR]
Vadim Lyubashevsky [Inria, Researcher]
Hoeteck Wee [CNRS, Researcher]

Faculty Members

David Naccache [Univ. Paris II, Professor, HdR]
Damien Vergnaud [ENS, Associate Professor, HdR]

PhD Students

Sonia Belaid [Thales]
Fabrice Ben Hamouda [ENS, Fondation CFM]
Florian Bourse [CNRS, ERC CryptoCloud, from October 2014]
Jérémie Clément [Crocus, CIFRE]
Simon Cogliani [CS Systems, CIFRE]
Mario Cornejo Ramirez [Inria]
Geoffroy Couteau [CNRS, ERC CryptoCloud, from October 2014]
Rafael Del Pino [Inria, FUI CryptoComp, from October 2014]
Houda Ferradi [ENS, ANR Simpatic]
Rémi Géraud [Ingenico, CIFRE, from November 2014]
Tancrède Lepoint [CryptoExperts, CIFRE, until June 2014]
Diana Maimut [Advanced Technology Institute, Bucharest, Romania]
Pierrick Méaux [Inria, ANR CLE, from October 2014]
Thierry Mefenza [ENS, ANR ROMAnTIC, from October 2014]
Alain Passelègue [ENS, DGA & ANR Prince]
Thomas Prest [Thales, CIFRE]
Sylvain Ruhault [Oppida]
Olivier Sanders [Orange Labs, CIFRE]
Adrian Thillard [ANSSI]

Post-Doctoral Fellows

Angelo de Caro [ENS, ANR Simpatic]
Itai Dinur [ENS, FSMP]
Thomas Peters [CNRS, ERC CryptoCloud, from October 2014]

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 assume 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.

3.4. Symmetric Key Cryptanalysis

Symmetric key cryptographic primitives play a very important role in secure communications. For example, block ciphers and stream ciphers are used to protect the privacy of cellular phone users from eavesdroppers, while MACs (message authentication codes) ensure that active attackers cannot interfere with cellular communication without being detected.

Since there is no method of formally proving that a complex modern symmetric key cipher is secure, there is no choice but to consider it secure if there are no known attacks against it. Thus, a symmetric key cipher should undergo an extensive cryptanalytic effort to evaluate its resistance against both well-known and new types of attacks. The goal of cryptanalytic is thus to ensure that only the strongest symmetric key cryptographic primitives are deployed and used in practice.

The team contributes to this field by proposing new cryptanalytic techniques and applying them to both new and existing secret key primitives, helping to understand their security.

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.

5. New Results

5.1. Results

All the results of the team have been published in journals or conferences (see the list of publications). They are all related with the research program (see before) and the research projects (see after):

- More efficient constructions with lattices
- New constructions from pairings
- Delegation of computations
- Analysis of pseudo-random generators
- Advanced primitives for the privacy in the cloud
- Cryptanalysis of symmetric primitives
- New leakage-resilient primitives
- Stronger security with related-key security

6. Partnerships and Cooperations

6.1. National Initiatives with Industrials

- **ANR ARPEGE PRINCE: Proven Resilience against Information leakage in Cryptographic Engineering.**
  Participants: Michel Ferreira Abdalla, Sonia Belaid, Fabrice Ben Hamouda, Alain Passelègue, David Pointcheval.

  From December 2010 to May 2015.
  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.

- **ANR INS SIMPATIC: SIM and PAiring Theory for Information and Communications security.**
  Participants: Angelo de Caro, Houda Ferradi, David Pointcheval, Olivier Sanders, Damien Vergnaud.

  From February 2013 to July 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.
- **FUI CryptoComp.**
  Participants: Rafael Del Pino, Vadim Lyubashevsky.

  From October 2014 to September 2017.
  Partners: CEA, UVSQ, CryptoExperts, Dictao, XLIM, ViAccess Orca, CNRS, Bertin Technologies, KalRay, Gemalto
  We aim at studying delegation of computations to the cloud, in a secure way.

6.2. National Collaborations within Academics

- **ANR JCJC ROMAnTIC: Randomness in Mathematical Cryptography.**
  Participants: Thierry Mefenza, David Pointcheval, Sylvain Ruhault, Adrian Thillard, Damien Vergnaud.

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

  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.
- **ANR JCJC EnBiD: Encryption for Big Data.**
  Participant: Hoeteck Wee.

  From October 2014 to September 2018.
  Partners: Univ. Paris 2, Univ. Paris 8.
  The main objective of this project is to study techniques for efficient and expressive functional encryption schemes. Functional encryption is a novel paradigm for public-key encryption that enables both fine-grained access control and selective computation on encrypted data, as is necessary to protect big, complex data in the cloud.

6.3. European Initiatives

- **SecFuNet: Security for Future Networks.**
  Participants: Michel Ferreira Abdalla, Vadim Lyubashevsky, David Pointcheval.

  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.
- **ICT COST CryptoAction: Cryptography for Secure Digital Interaction**
  Participant: Vadim Lyubashevsky.

  From April 2014 to April 2018.
  The aim of this COST Action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments.
- **ERC CryptoCloud: Cryptography for the Cloud.**
  Participants: Michel Ferreira Abdalla, Florian Bourse, Fabrice Ben Hamouda, Geoffroy Couteau, Thomas Peters, David Pointcheval, Hoeteck Wee.

  From June 2014 to May 2019.

6.4. Other Grants

- **Google: Google Research Award.**
  Participant: Hoeteck Wee.

  On the security of TLS. The goal of this project is to initiate a formal cryptographic treatment of new mechanisms and proposals for reducing the latency in the TLS Handshake Protocol and to enhance our cryptographic understanding of the TLS Handshake Protocol.

6.5. International Research Visitors

- Hugo Krawczyk (IBM)
- Serdar Pehlivanoğlu (Zirve University, Turkey)
- Kai-Min Chung (Academia Sinicia, Taiwan)
- Daniel Wichs (Northeastern)
- Mehdi Tibouchi (NTT)
- Vinod Vaikuntanathan (MIT)
- Kenny Paterson (RHUL)
- Tal Malkin (Columbia)
- David Cash (Rutgers)
- Igor Shparlinski
- Zvika Brakerski (Weizmann)
- Elette Boyle (Technion)
- Giuseppe Persiano (Salerno)
- Yuval Ishai (Technion)
- Eike Kiltz (RUB)

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific Events Organisation

7.1.1.1. Organisation of Events

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

7.1.1.2. 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 (chair)
- steering committee of PAIRING: Michel Abdalla

7.1.1.3. Board of International Organisations

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

7.1.2. Scientific Events Selection

7.1.2.1. Program Committee Chair

- Africacrypt – 28-30 May (Marrakesh, Morocco): David Pointcheval, Damien Vergnaud
- WISTP – 30 June-2 July (Heraklion, Greece): David Naccache
- SCN – 3-5 September (Amalfi, Italy): Michel Abdalla

7.1.2.2. Program Committee Member

- CS2 – 20 January (Amsterdam, Netherlands): David Naccache
- WAHC – 7 March (Rockley, Christ Church, Barbados, West Indies): David Naccache
- PKC – 26-28 March (Buenos Aires, Argentina): Michel Abdalla, Vadim Lyubashevsky
- POST – 5-13 April (Grenoble, France): David Pointcheval
- HOST – 6-7 May (Austin, TX, USA): David Naccache
- ECSaR – 27-31 May (Stanford, USA): David Naccache
- ASIACCS – 3-6 June (Kyoto, Japan): David Naccache
- HASP – 15 June (Minneapolis, MN, USA): David Naccache
- WISTP – 30 June-2 July (Heraklion, Greece): David Pointcheval
- NFSP – 3 July (Madrid, Spain): David Naccache
- IWSEC – 27-29 August (Hirosaki, Japan): Damien Vergnaud
- SCN – 3-5 September (Amalfi, Italy): Damien Vergnaud
- ESORICS – 7-11 September (Wroclaw, Poland): David Naccache
- LATINCRYPT – 17-19 September (Florianopolis, Brazil): Michel Abdalla
- ICDF2C – 18-20 September (Seoul, South Korea): David Naccache
- PQC – 1-3 October (Waterloo, Canada): Vadim Lyubashevsky
- SPACE – 18-22 October (Pune, India): David Naccache
- CANS – 22-24 October (Heraklion, Greece): Itai Dinur
- WNCS – 7-9 November (Dubai, UAE): David Naccache

- PriSec – 3-5 December (Sydney, Australia): David Naccache
- Botconf – 3-5 December (Paris, France): David Naccache
- ASIACRYPT – 7-11 December (Kaoshiung, Taiwan): Itai Dinur
- Indocrypt – 14-17 December (New Delhi, India): David Naccache
- INTRUST – 16-17 December (Beijing, China): David Naccache

7.1.3. Editorial Boards of Journals

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 Engineering*: David Naccache (editor)
- of *Encyclopedia of Cryptography and Security*: David Naccache (editor)
- of *Journal of Computer Security, IOS Press*: David Naccache
- of *Open Journal of Information Security and Applications, SOP*: David Naccache (editor)
- of *Cryptologia* – Taylor & Francis: David Naccache (editor)
- of *Computers & Security* – Elsevier: David Naccache
- 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

7.2. Teaching - Supervision - Juries

7.2.1. 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: Damien Vergnaud, Advanced Algebra and Applications to Cryptography, Ecole Centrale Paris
- Master: Hoeteck Wee, Randomness in Complexity, 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

7.2.2. Supervision

- PhD: Tancrède Lepoint, Design and Implementation of Lattice-Based Cryptography, ENS, June 30th, 2014, David Pointcheval

- PhD in progress: Sylvain Ruhault, Randomness in cryptography, from 2011, David Pointcheval & Damien Vergnaud
- PhD in progress: Sonia Belaid, Leakage-resilient cryptography, from 2012, Michel Abdalla
- PhD in progress: Fabrice Ben Hamouda, Leakage of information in cryptography, from 2012, Michel Abdalla & David Pointcheval
- PhD in progress: Diana Maimut, Fully Homomorphic Encryption, from 2012, David Naccache
- PhD in progress: Thomas Prest, Lattice-based cryptography, from 2012, Vadim Lyubashevsky & David Pointcheval
- PhD in progress: Olivier Sanders, Delegation of computations, from 2012, David Pointcheval
- PhD in progress: Jérémie Clément, Lightweight cryptography, from 2013, David Naccache
- PhD in progress: Simon Cogliani, Authenticated Encryption, from 2013, David Naccache
- PhD in progress: Mario Cornejo, Security for the cloud, from 2013, Michel Abdalla
- PhD in progress: Houda Ferradi, Biometric protocols and mobile security, from 2013, David Naccache
- PhD in progress: Alain Passelègue, Security against related-key attacks, from 2013, Michel Abdalla
- PhD in progress: Adrian Thillard, Counter-measures against side-channel attacks and secure multi-party computation, from 2013, Damien Vergnaud
- PhD in progress: Florian Bourse, Encryption Schemes for the Cloud, from 2014, Michel Abdalla & David Pointcheval
- PhD in progress: Geoffroy Couteau, Efficient secure two-party computation for the Cloud, from 2014, David Pointcheval & Hoeteck Wee
- PhD in progress: Rafael Del Pino, Lattice-Based Cryptography – Complexity and Ideal-Lattices, from 2014, Vadim Lyubashevsky
- PhD in progress: Rémi Géraud, Provable security in public-key cryptography, from 2014, David Naccache
- PhD in progress: Pierrick Meaux, Lattice-Based Cryptography – Advanced Features, from 2014, Vadim Lyubashevsky

7.2.3. Juries

- PhD Robert Künnemann. *On the Analysis of Security APIs and Stateful Protocols* – ENS Cachan – France, January 7th 2014: David Pointcheval
- HdR Emmanuel Prouff. *Analyse des Attaques par Canaux Auxiliaires et Preuves de Sécurité* – Université Pierre et Marie Curie, Paris – France, January 27th 2014: David Pointcheval
- PhD Thomas Peters. *Privacy Enhancing Cryptographic Mechanisms with Public Verifiability* – Université Catholique de Louvain – Belgium, April 2nd 2014: David Pointcheval
- PhD Alain Patey. *Techniques cryptographiques pour l'authentification et l'identification biométriques respectant la vie privée* – Telecom ParisTech – France, May 20th 2014: David Pointcheval (Chair)
- PhD Susan Thomson. *Public-Key Cryptography with Joint and Related-Key Security* – ENS – France, June 18th 2014: Michel Abdalla (Examiner)
- PhD Tancrède Lepoint. *Design and Implementation of Lattice-Based Cryptography* – ENS – France, June 30th 2014: David Naccache, David Pointcheval (Supervisor)
- HdR Damien Vergnaud. *Primitives et constructions en cryptographie asymétrique* – Ecole Normale Supérieure – France, July 1st 2014: Michel Abdalla, David Pointcheval
- PhD Slim Bettaieb. *Signature et identification pour l'anonymat, basées sur les réseaux* – Université de Limoges – France, September 26h 2014: Damien Vergnaud (Reviewer)

- PhD Adeline Langlois. *Lattice-Based Cryptography: Security Foundations and Constructions* – ENS Lyon – France, October 17 2014: Vadim Lyubashevsky (Jury member)
- HdR: Duong Hieu Phan. *Some Advances in Broadcast Encryption and Traitor Tracing* – Ecole Normale Supérieure – France, November 19th 2014: Michel Abdalla, David Pointcheval (Supervisor)
- PhD Cédric Murdica. *Sécurité Physique de la Cryptographie sur Courbes Elliptiques* – Télécom ParisTech – France, February 13th 2014: David Naccache (Supervisor)
- PhD Thomas Souvignet. *L'expertise et la lutte contre la fraude monétique* Université Panthéon-Assas Paris 2 – France, December 18th 2014: David Naccache (Supervisor)
- PhD Jean-Michel Cioranesco. *Nouvelles contre-mesures pour la protection de circuit intégrés* – Université Panthéon-Sorbonne Paris 1 – France, December 18th 2014: David Naccache (Supervisor)
- PhD Guillaume Bouffard. *A Generic Approach for Protecting Java Card Smart Card Against Software Attacks* Université de Limoges – France, October 10th 2014: David Naccache (Reviewer)
- PhD Emmanuel Volte. *Miroirs, cubes et Feistel dissymétrique* – Université Cergy-Pontoise – France, November 28th 2014: David Pointcheval (Chair)
- PhD Rodolphe Lampe. *Preuves de sécurité en cryptographie symétrique à l'aide de la technique du coupling* – Université de Versailles Saint-Quentin en Yvelines – France, December 2nd 2014: David Pointcheval, David Naccache (Reviewer)

8. Bibliography

Major publications by the team in recent years

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, H. Shi. *Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions*, in "Journal of Cryptology", July 2008, vol. 21, n^{o} 3, 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] T. LEPOINT. *Design and Implementation of Lattice-Based Cryptography*, Ecole Normale Supérieure de Paris - ENS Paris, June 2014, https://tel.archives-ouvertes.fr/tel-01069864

[14] D. VERGNAUD. *Primitives et constructions en cryptographie asymétrique*, Ecole normale supérieure, July 2014, Habilitation à diriger des recherches, https://hal.inria.fr/tel-01089163

Articles in International Peer-Reviewed Journals

[15] M. ABDALLA, D. CATALANO, D. FIORE. *Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions*, in "Journal of Cryptology", July 2014, vol. 27, n^o 3, pp. 544-593 [*DOI :* 10.1007/S00145-013-9153-X], https://hal.inria.fr/hal-00915548

[16] S. BELAID, V. GROSSO, F.-X. STANDAERT. *Masking and leakage-resilient primitives: One, the other(s) or both?*, in "Cryptography and Communications", 2014, 25 p. [*DOI :* 10.1007/S12095-014-0113-6], https://hal.inria.fr/hal-01093883

[17] J. JEAN, M. NAYA-PLASENCIA, T. PEYRIN. *Improved Cryptanalysis of AES-like Permutations*, in "Journal of Cryptology", 2014, pp. 772–798, https://hal.inria.fr/hal-01092270

Invited Conferences

[18] M. ABDALLA. *Password-Based Authenticated Key Exchange: An Overview*, in "PROVSEC 2014", Hong Kong, China, S. S. M. CHOW, J. K. LIU, L. C. K. HUI, S. M. YIU (editors), Springer, October 2014, vol. 8782, pp. 1-9 [*DOI :* 10.1007/978-3-319-12475-9_1], https://hal.inria.fr/hal-01071313

[19] M. ABDALLA, H. CHABANNE, H. FERRADI, J. JAINSKI, D. NACCACHE. *Improving Thomlinson-Walker's Software Patching Scheme Using Standard Cryptographic and Statistical Tools*, in "ISPEC 2014", Fuzhou, China, X. HUANG, J. ZHOU (editors), Lecture Notes in Computer Science, Springer, May 2014, vol. 8434, pp. 8-14 [*DOI :* 10.1007/978-3-319-06320-1_2], https://hal.inria.fr/hal-01071319

[20] H. WEE. *Functional Encryption and Its Impact on Cryptography*, in "Security and Cryptography for Networks (SCN 2014)", Amalfi, Italy, September 2014 [*DOI :* 10.1007/978-3-319-10879-7_18], https://hal.inria.fr/hal-01094712

International Conferences with Proceedings

[21] M. ABDALLA, F. BENHAMOUDA, A. PASSELÈGUE, K. G. PATERSON. *Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier*, in "CRYPTO 2014", Santa Barbara, United States, J. A. GARAY, R. GENNARO (editors), August 2014, vol. 8616, pp. 77-94 [*DOI :* 10.1007/978-3-662-44371-2_5], https://hal.inria.fr/hal-01068388

[22] A. BAR-ON, I. DINUR, O. DUNKELMAN, N. KELLER, V. LALLEMAND, B. TSABAN. *Cryptanalysis of SP Networks with Partial Non-Linear Layers*, in "Advances in Cryptology - Eurocrypt 2015", Sofia, Bulgaria, April 2015, https://hal.inria.fr/hal-01108331

[23] S. BELAID, B. GÉRARD, P.-A. FOUQUE. *Side-Channel Analysis of Multiplications in* $GF(2^{128})$, in "Asiacrypt 2014", Kaohsiung, Taiwan, Lecture Notes in Computer Science, Springer, December 2014, vol. 8874 [*DOI :* 10.1007/978-3-662-45608-8_17], https://hal.inria.fr/hal-01093865

[24] F. BENHAMOUDA, J. CAMENISCH, S. KRENN, V. LYUBASHEVSKY, G. NEVEN. *Better Zero-Knowledge Proofs for Lattice Encryption and Their Application to Group Signatures*, in "ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security", Kaohsiung, Taiwan, P. SARKAR, T. IWATA (editors), LNCS - Lecture Notes in Computer Science, Springer, December 2014, vol. 8873, pp. 551-572 [*DOI :* 10.1007/978-3-662-45611-8_29], https://hal.archives-ouvertes.fr/hal-01084737

[25] T. BOURGEAT, J. BRINGER, H. CHABANNE, R. CHAMPENOIS, J. CLÉMENT, H. FERRADI, M. HEINRICH, P. MELOTTI, D. NACCACHE, A. VOIZARD. *New Algorithmic Approaches to Point Constellation Recognition*, in "IFIP SEC 2014", Marrakech, Morocco, IFIP SEC 2014, March 2014, https://hal.inria.fr/hal-01098401

[26] S. CANARD, J. DEVIGNE, O. SANDERS. *Delegating a Pairing Can Be Both Secure and Efficient*, in "Applied Cryptography and Network Security (ACNS) 2014", Lausanne, Switzerland, June 2014 [*DOI :* 10.1007/978-3-319-07536-5_32], https://hal.inria.fr/hal-01091145

[27] 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), Springer, March 2014, vol. 8383, pp. 167-183, https://hal.inria.fr/hal-00940045

[28] J.-M. CIORANESCO, J.-L. DANGER, T. GRABA, S. GUILLEY, Y. MATHIEU, D. NACCACHE, X. T. NGO. *Cryptographically secure shields*, in "IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)", Arlington, VA, United States, Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on, IEEE, May 2014, 6 p. [*DOI :* 10.1109/HST.2014.6855563], https://hal.inria.fr/hal-01098383

[29] S. Cogliani, D.-S. Maimut, D. Naccache, R. Portella, R. Reyhanitabar, S. Vaudenay, D. Vizár. *OMD: A Compression Function Mode of Operation for Authenticated Encryption*, in "Selected Areas in Cryptography 2014", Montreal, Quebec, Canada, Selected Areas in Cryptography 2014, Springer, August 2014, vol. Lecture Notes in Computer Science 2014 [*DOI :* 10.1007/978-3-319-13051-4_7], https://hal.inria.fr/hal-01098397

[30] M. Cornejo, S. Ruhault. *Characterization of Real-Life PRNGs under Partial State Corruption*, in "CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security", Scottsdale, Arizona, United States, ACM, November 2014, pp. 1004-1015 [*DOI :* 10.1145/2660267.2660377], https://hal.inria.fr/hal-01084490

[31] N. Desmoulins, R. Lescuyer, O. Sanders, J. Traoré. *Direct Anonymous Attestations with Dependent Basename Opening*, in "Cryptology and Network Security (CANS) 2014", Heraklion, Greece, October 2014 [*DOI :* 10.1007/978-3-319-12280-9_14], https://hal.inria.fr/hal-01091165

[32] I. Dinur. *Improved Differential Cryptanalysis of Round-Reduced Speck*, in "SAC 2014 - 21st International Conference Selected Areas in Cryptography", Montreal, Canada, August 2014, https://hal.archives-ouvertes.fr/hal-01086176

[33] I. Dinur, O. Dunkelman, N. Keller, A. Shamir. *Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys*, in "ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung", Kaoshiung, Taiwan, P. Sarkar, T. Iwata (editors), LNCS - Lecture Notes in Computer Science, Springer, December 2014, vol. 8873, pp. 439-457 [*DOI :* 10.1007/978-3-662-45611-8_23], https://hal.archives-ouvertes.fr/hal-01086179

[34] I. Dinur, O. Dunkelman, N. Keller, A. Shamir. *Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64*, in "FSE 2014 - 21st International Workshop on Fast Software Encryption", London, United Kingdom, March 2014, https://hal.archives-ouvertes.fr/hal-01086175

[35] I. Dinur, J. Jean. *Cryptanalysis of FIDES*, in "FSE 2014 - 21st International Workshop on Fast Software Encryption", London , United Kingdom, March 2014, https://hal.archives-ouvertes.fr/hal-01086173

[36] I. Dinur, G. Leurent. *Improved Generic Attacks Against Hash-based MACs and HAIFA*, in "Advances in Cryptology - CRYPTO 2014", Santa Barbara, CA, United States, LNCS, Springer, August 2014, vol. 8616 [*DOI :* 10.1007/978-3-662-44371-2_9], https://hal.archives-ouvertes.fr/hal-01086177

[37] L. Ducas, V. Lyubashevsky, T. Prest. *Efficient identity-based encryption over NTRU lattices*, in "Asiacrypt 2014", Kaohsiung, Taiwan, December 2014, https://hal.inria.fr/hal-01094814

[38] J. A. Garay, Y. Ishai, R. Kumaresan, H. Wee. *On the Complexity of UC Commitments*, in "Advances in Cryptology – EUROCRYPT 2014", Copenhagen, Denmark, May 2014 [*DOI :* 10.1007/978-3-642-55220-5_37], https://hal.archives-ouvertes.fr/hal-01094702

[39] A. Guillevic, D. Vergnaud. *Algorithms for Outsourcing Pairing Computation*, in "CARDIS - 13th Smart Card Research and Advanced Application Conference", Paris, France, M. Joye, A. Moradi (editors), Springer, November 2014, https://hal.inria.fr/hal-01084550

[40] Y. ISHAI, H. WEE. *Partial Garbling Schemes and Their Applications*, in "Automata, Languages, and Programming: ICALP", Copenhagen, Denmark, July 2014 [*DOI :* 10.1007/978-3-662-43948-7_54], https://hal.archives-ouvertes.fr/hal-01094699

[41] T. LEPOINT, J.-S. CORON, M. TIBOUCHI. *Scale-Invariant Fully-Homomorphic Encryption over the Integers*, in "PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography", Buenos Aires, Argentina, H. KRAWCZYK (editor), Springer, March 2014, vol. 8383, pp. 311-328 [*DOI :* 10.1007/978-3-642-54631-0_18], https://hal.inria.fr/hal-00950481

[42] T. LEPOINT, M. NAEHRIG. *A Comparison of the Homomorphic Encryption Schemes FV and YASHE*, in "AFRICACRYPT 2014", Marrakesh, Morocco, D. POINTCHEVAL, D. VERGNAUD (editors), Lecture Notes in Computer Science, Springer, May 2014, vol. 8469, pp. 318-335 [*DOI :* 10.1007/978-3-319-06734-6_20], https://hal.archives-ouvertes.fr/hal-01006484

[43] V. LOMNÉ, E. PROUFF, M. RIVAIN, T. ROCHE, A. THILLARD. *How to Estimate the Success Rate of Higher Order Side-Channels Attacks*, in "Workshop on Cryptographic Hardware and Embedded Systems (CHES)", Busan, South Korea, September 2014, https://hal.inria.fr/hal-01089215

[44] M. MEHARI, M. KONSTANTINOS, D. NACCACHE, M. KEITH. *Verifying Software Integrity in Embedded Systems: A Side Channel Approach*, in "Constructive Side-Channel Analysis and Secure Design", Paris, France, Constructive Side-Channel Analysis and Secure Design, Springer, April 2014, vol. Lecture Notes in Computer Science 2014, 19 p. [*DOI :* 10.1007/978-3-319-10175-0_18], https://hal.inria.fr/hal-01098381

[45] D. NACCACHE, S. RAINER, S. ADRIANA, M. YUNG. *Narrow Bandwidth Is Not Inherent in Reverse Public-Key Encryption*, in "Security and Cryptography for Networks", Amalfi, Italy, Security and Cryptography for Networks, Springer, October 2014, vol. Lecture Notes in Computer Science Volume 8642, 9 p. [*DOI :* 10.1007/978-3-319-10879-7_34], https://hal.inria.fr/hal-01098406

[46] D. POINTCHEVAL, O. SANDERS. *Forward Secure Non-Interactive Key Exchange*, in "The 9th Conference on Security in Communication Networks (SCN '14)", Amalfi, Italy, M. ABDALLA, R. D. PRISCO (editors), Proceedings of the 9th Conference on Security in Communication Networks (SCN '14), Springer, September 2014, vol. LNCS, n^{o} 8642, pp. 21-39 [*DOI :* 10.1007/978-3-319-10879-7_2], https://hal.inria.fr/hal-01089001

[47] H. WEE. *Dual System Encryption via Predicate Encodings*, in "Theory of Cryptography (TCC 2014)", San Diego, United States, February 2014 [*DOI :* 10.1007/978-3-642-54242-8_26], https://hal.archives-ouvertes.fr/hal-01094703

Books or Proceedings Editing

[48] M. ABDALLA, R. D. PRISCO (editors). *Security and Cryptography for Networks - SCN 2014*, Lecture Notes in Computer Science, SpringerAmalfi, Italy, September 2014, vol. 8642, 609 p. [*DOI :* 10.1007/978-3-319-10879-7], https://hal.inria.fr/hal-01068374

[49] D. NACCACHE, D. SAUVERON (editors). *Information Security Theory and Practice. Securing the Internet of Things* , Lecture Notes in Computer Science, SpringerHeraklion, Crete, Greece, June 2014, vol. 8501 [*DOI :* 10.1007/978-3-662-43826-8], https://hal.inria.fr/hal-01098408

[50] D. Pointcheval, D. Vergnaud (editors). *Progress in Cryptology – AFRICACRYPT 2014*, Lecture Notes in Computer Science, Springer, May 2014, vol. 8469, 476 p. [*DOI :* 10.1007/978-3-319-06734-6], https://hal.inria.fr/hal-01089517

Research Reports

[51] M. Abdalla, F. Benhamouda, A. Passelègue, K. G. Paterson. *Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier*, June 2014, n^o Cryptology ePrint Archive: Report 2014/488, https://hal.inria.fr/hal-01068465

[52] M. Abdalla, F. Benhamouda, D. Pointcheval. *Disjunctions for Hash Proof Systems: New Constructions and Applications*, June 2014, n^{o} Cryptology ePrint Archive: Report 2014/483, https://hal.inria.fr/hal-01068420

[53] M. Abdalla, F. Benhamouda, D. Pointcheval. *Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks*, IACR, August 2014, n^{o} Cryptology ePrint Archive: Report 2014/609, https://hal.inria.fr/hal-01068416

[54] M. Abdalla, F. Benhamouda, D. Pointcheval. *Removing Erasures with Explainable Hash Proof Systems*, February 2014, n^{o} Cryptology ePrint Archive: Report 2014/125, https://hal.inria.fr/hal-01068442

[55] M. Abdalla, B. Florian, A. De Caro, D. Pointcheval. *Simple Functional Encryption Schemes for Inner Products*, IACR, January 2015, n^{o} Cryptology ePrint Archive: Report 2015/017, https://hal.inria.fr/hal-01108287

[56] A. Bar-On, I. Dinur, O. Dunkelman, V. Lallemand, B. Tsaban. *Improved Analysis of Zorro-Like Ciphers*, IACR Cryptology ePrint Archive, March 2014, n^{o} 2014/228, https://hal.inria.fr/hal-01092323

[57] F. Benhamouda, D. Pointcheval. *Verifier-Based Password-Authenticated Key Exchange: New Models and Constructions*, IACR Cryptology ePrint Archive, October 2014, n^{o} Cryptology ePrint Archive: Report 2013/833, https://hal.inria.fr/hal-01093876

[58] T. Bourgeat, J. Bringer, H. Chabanne, R. Champenois, J. Clément, H. Ferradi, M. Heinrich, P. Melotti, D. Naccache, A. Voizard. *New Algorithmic Approaches to Point Constellation Recogniti*, Ecole normale supérieure, March 2014, n^{o} CoRR abs/1405.1402 (2014), 14 p. , https://hal.inria.fr/hal-01098399

[59] S. Canard, D. Pointcheval, O. Sanders, J. Traoré. *Divisible E-Cash Made Practical*, IACR, October 2014, n^{o} Cryptology ePrint Archive: Report 2014/785, https://hal.inria.fr/hal-01088999

[60] R. Gay, P. Méaux, H. Wee. *Predicate Encryption for Multi-Dimensional Range Queries from Lattices*, Inria Paris-Rocquencourt - CASCADE ; ENS Paris - Ecole Normale Supérieure de Paris ; LIENS - Laboratoire d'informatique de l'école normale supérieure , November 2014, n^{o} Cryptology ePrint Archive: Report 2014/965, https://hal.inria.fr/hal-01094685

Scientific Popularization

[61] A. Teston, L. Ducas, M. Jouhet, T. Viéville. *Cryptris 1/2. Comprendre une des techniques les plus sophistiquées de cryptographie en... jouant à Tetris.*, in "Image des Maths", June 2014, https://hal.inria.fr/hal-01009430