IN PARTNERSHIP WITH:
**CNRS**

**Ecole normale supérieure de Paris**

Activity Report 2015

# 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

*Creation of the Project-Team: 2008 July 01*

**Keywords:**

**Computer Science and Digital Science:**

4. - Security and privacy
4.3. - Cryptography
4.3.1. - Public key cryptography
4.3.3. - Cryptographic protocols
7. - Fundamental Algorithmics
7.7. - Number theory

**Other Research Topics and Application Domains:**

6.3.3. - Network services
6.4. - Internet of things
9.4.1. - Computer science
9.8. - Privacy

# 1. Members

**Research Scientists**

David Pointcheval [Team leader, CNRS, Senior Researcher, HdR]
Michel Ferreira Abdalla [CNRS, Senior Researcher, HdR]
Vadim Lyubashevsky [Inria, Researcher, until July 2015]
Hoeteck Wee [CNRS, Researcher]

**Faculty Members**

David Naccache [Univ. Paris II, Professor, until September 2015, HdR]
Jacques Stern [ENS Paris, Emeritus Professor, HdR]
Damien Vergnaud [ENS Paris, Associate Professor, HdR]

**PhD Students**

Sonia Belaid [Thales, until October 2015]
Fabrice Ben Hamouda–Guichoux [ENS Paris, Fondation CFM]
Raphael Bost [DGA]
Florian Bourse [CNRS, ERC CryptoCloud]
Jeremie Clement [Crocus, CIFRE, until September 2015]
Simon Cogliani [CS Systems, CIFRE, until September 2015]
Mario Cornejo Ramirez [Inria, CORDI-S]
Geoffroy Couteau [CNRS, ERC CryptoCloud]
Rafael Del Pino [Inria, FUI CryptoComp]
Pierre-Alain Dupont [DGA, from March 2015]
Houda Ferradi [ENS Paris, ANR Simpatic, until September 2015]
Romain Gay [ENS Paris, from September 2015]
Remi Geraud [Ingenico, CIFRE, until September 2015]
Dahmun Gourdazi [CryptoExperts, CIFRE, from October 2015]
Louiza Khati [Oppida, from October 2015]
Diana Maimut [Advanced Technology Institute, Bucharest, Romania, until September 2015]
Pierrick Meaux [Inria, ANR JCJC CLE]

Thierry Mefenza Nountu [ENS Paris, ANR JCJC ROMAnTIC]
Michele Minelli [ENS Paris, H2020 ITN ECRYPT-NET, from October 2015]
Anca Nitulescu [CNRS, ERC CryptoCloud, from October 2015]
Alain Passelegue [ENS Paris, DGA & ANR Prince]
Thomas Prest [Thales, CIFRE, until December 2015]
Razvan Rosie [ENS Paris, H2020 ITN ECRYPT-NET, from October 2015]
Sylvain Ruhault [Oppida, until June 2015]
Olivier Sanders [Orange Labs, CIFRE, until September 2015]
Quentin Santos [Orange Labs, CIFRE, from November 2015]
Adrian Thillard [ANSSI]

**Post-Doctoral Fellows**
Angelo de Caro [ENS Paris, ANR Simpatic, until April 2015]
Itai Dinur [ENS Paris, FSMP, until August 2015]
Thomas Peters [CNRS, ERC CryptoCloud, until December 2015]

**Administrative Assistants**
Nathalie Gaudechoux [Inria]
Joëlle Isnard [CNRS, Administrative Head DI/ENS]

**Others**
Guiseppe Guagliardo [ENS Paris, Internship Univ. Bordeaux, from March to July 2015]
Maxime Faron [ENS Lyon, Internship, from June to July 2015]
Benjamin Battino [Telecom ParisTech, Internship, July 2015]

# 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 important part 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. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Conferences*

Our group presented 8 papers (among 57) at Eurocrypt, 7 (among 74) at Crypto, and 3 (among 64) at Asiacrypt, the main general IACR conferences, and 6 papers (among 36) at PKC and 2 (among 34) at CHES, the two thematic IACR conferences on our domains (public-key cryptography and hardware-oriented cryptography).

### *5.1.2. Awards*

In February 2015, Tancrède Lepoint has received the Gilles Kahn PhD Thesis Award 2014.

# 6. New Results

## 6.1. 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):

- New zero-knowledge proofs
- Advanced families of hash proofs

- More efficient constructions with lattices
- New e-cash constructions
- Advanced primitives for the privacy in the cloud
- Efficient functional encryption
- Various predicate encryption schemes
- Cryptanalysis of symmetric primitives
- New leakage-resilient primitives
- Stronger security with related-key security

# 7. Partnerships and Cooperations

## 7.1. National Initiatives with Industrials

### *7.1.1. PRINCE*

Title: Proven Resilience against Information leakage in Cryptographic Engineering

Program: ANR ARPEGE

Duration: December 2010 – May 2015

Coordinator: Tranef

Partners:

ENS

UVSQ

Oberthur Technologies

Ingenico

Gemalto

Tranef

Local coordinator: Michel Abdalla

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.

### *7.1.2. SIMPATIC*

Title: SIM and PAiring Theory for Information and Communications security

Program: ANR INS

Duration: February 2013 – July 2016

Coordinator: Orange Labs

Partners:

Orange Labs

ENS

INVIA

Oberthur Technologies

STMicroelectronics

Université Bordeaux 1

Université de Caen Basse-Normandie

Université de Paris VIII

Local coordinator: David Pointcheval

We aim at providing the most possible efficient and secure hardware/software implementation of a bilinear pairing in a SIM card.

### 7.1.3. CryptoComp

Program: FUI

Duration: October 2014 – September 2017

Coordinator: CryptoExperts

Partners:

CEA

CNRS

Kalray

Inria

Dictao

Université de Limoges

VIACESS

Bertin technologies

GEMALTO

Local coordinator: Vadim Lyubashevsky (until July 2015) and David Pointcheval (from August 2015)

We aim at studying delegation of computations to the cloud, in a secure way.

## 7.2. National Collaborations within Academics

### 7.2.1. ROMAnTIC

Title: Randomness in Mathematical Cryptography

Program: ANR JCJC

Duration: October 2012 – September 2016

PI: Damien Vergnaud

Partners:

ANSSI

Univ. Paris 7

Univ. Limoges

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).

### 7.2.2. CLE

Title: Cryptography from Learning with Errors

Program: ANR JCJC

Duration: October 2013 – December 2015

PI: Vadim Lyubashevsky

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.

### *7.2.3. EnBiD*

Title: Encryption for Big Data

Program: ANR JCJC

Duration: October 2014 – September 2018

PI: Hoeteck Wee

Partners:

Univ. Paris 2

Univ. Limoges

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.

## 7.3. European Initiatives

### *7.3.1. CryptoAction*

Title: Cryptography for Secure Digital Interaction

Program: H2020 ICT COST

Duration: April 2014 – April 2018

Local coordinator: Vadim Lyubashevsky (until July 2015) and Michel Abdalla (from August 2015)

The aim of this COST CryptoAction 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.

### *7.3.2. CryptoCloud*

Title: Cryptography for the Cloud

Program: FP7 ERC Advanced Grant

Duration: June 2014 – May 2019

PI: David Pointcheval

The goal of the CryptoCloud project is to develop new interactive tools to provide privacy to the Cloud.

### *7.3.3. SAFEcrypto*

Title: Secure Architectures of Future Emerging Cryptography

Program: H2020

Duration: January 2015 - January 2019

Coordinator: The Queen's University of Belfast

Partners:

Inria/ENS (France)

Emc Information Systems International (Ireland)

Hw Communications (United Kingdom)

The Queen's University of Belfast (United Kingdom)

Ruhr-Universitaet Bochum (Germany)

Thales Uk (United Kingdom)

Universita della Svizzera italiana (Switzerland)

Local coordinator: Vadim Lyubashevsky (until July 2015) and Michel Abdalla (from August 2015)

SAFEcrypto will provide a new generation of practical, robust and physically secure post quantum cryptographic solutions that ensure long-term security for future ICT systems, services and applications. Novel public-key cryptographic schemes (digital signatures, authentication, public-key encryption, identity-based encryption) will be developed using lattice problems as the source of computational hardness. The project will involve algorithmic and design optimisations, and implementations of the lattice-based cryptographic schemes addressing the cost, energy consumption, performance and physical robustness needs of resource-constrained applications, such as mobile, battery-operated devices, and of real-time applications such as network security, satellite communications and cloud. Currently a significant threat to cryptographic applications is that the devices on which they are implemented on leak information, which can be used to mount attacks to recover secret information. In SAFEcrypto the first analysis and development of physical-attack resistant methodologies for lattice-based cryptographic implementations will be undertaken. Effective models for the management, storage and distribution of the keys utilised in the proposed schemes (key sizes may be in the order of kilobytes or megabytes) will also be provided. This project will deliver proof-of-concept demonstrators of the novel lattice-based public-key cryptographic schemes for three practical real-word case studies with real-time performance and low power consumption requirements. In comparison to current state-of-the-art implementations of conventional public-key cryptosystems (RSA and Elliptic Curve Cryptography (ECC)), SAFEcrypto's objective is to achieve a range of lattice-based architectures that provide comparable area costs, a 10-fold speed-up in throughput for real-time application scenarios, and a 5-fold reduction in energy consumption for low-power and embedded and mobile applications.

### 7.3.4. ECRYPT-NET

Title: Advanced Cryptographic Technologies for the Internet of Things and the Cloud

Program: H2020 ITN

Duration: March 2015 – February 2019

Coordinator: KU Leuven (Belgium)

Partners:

KU Leuven (Belgium)

École Normale Supérieure (France)

Ruhr-Universität Bochum (Germany)

Royal Holloway, University of London (UK)

University of Bristol (UK)

CryptoExperts (France)

NXP Semiconductors (Belgium)

Technische Universiteit Eindhoven (the Netherlands)

Local coordinator: Michel Abdalla

ECRYPT-NET is a research network of six universities and two companies, as well as 7 associated companies, that intends to develop advanced cryptographic techniques for the Internet of Things and the Cloud and to create efficient and secure implementations of those techniques on a broad range of platforms.

### *7.3.5. aSCEND*

Title: Secure Computation on Encrypted Data

Program: H2020 ERC Starting Grant

Duration: June 2015 – May 2020

PI: Hoeteck Wee

The goals of the aSCEND project are (i) to design pairing and lattice-based functional encryption that are more efficient and ultimately viable in practice; and (ii) to obtain a richer understanding of expressive functional encryption schemes and to push the boundaries from encrypting data to encrypting software.

## 7.4. 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.*

## 7.5. International Research Visitors

- Dennis Hofheinz (KIT, Germany)
- Melissa Chase (MSR Redmond)
- Mariana Raykova (Yale University)
- Phil Rogaway (UC Davis)
- Alexandra Boldyreva (Georgia Tech)

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### *8.1.1. Scientific Events Organisation*

*8.1.1.1. Organisation of Events*

- a weekly seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html
- monthly working group on lattices, joint with ENS Lyin
- Organization of the *Summer School on Mathematical and Practical Aspects of Fully Homomorphic Encryption and Multi-Linear Maps* at IHP, Paris, in October 2015 (supported by CryptoAction, SAFEcrypto, CryptoCloud, and aSCEND)

*8.1.1.2. 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

*8.1.1.3. Other Steering Committees*

- steering committee of the Coding and Cryptography working group (GT-C2 - https://crypto.di.ens.fr/c2:main) of the *Groupe de Recherche Informatique Mathématique* (GDR-IM): Damien Vergnaud serves on the committee and has even been elected as the Head of this steering committee

*8.1.1.4. Board of International Organisations*

- Board of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2013 – 2018), David Pointcheval (2008–2016)

### *8.1.2. Scientific Events Selection*

*8.1.2.1. Program Committee Member*

- PKC 2015 – March 30 - April 1 (Maryland, USA): Michel Abdalla
- CT-RSA – 20-25 April (San Francisco, California, USA): David Pointcheval
- Eurocrypt – 26-30 April (Sofia, Bulgaria): David Pointcheval
- ACNS – 2-5 June (New-York, USA): David Pointcheval
- CRYPTO – 16-20 Aug (Santa Barbara, California, USA): Michel Abdalla
- LATINCRYPT – 23-26 Aug (Guadalajara, Mexico): Michel Abdalla
- IWSEC – 26-28 Aug (Nara, Japan): Damien Vergnaud
- FOCS – 18-20 Oct (Berkeley, California, USA): Hoeteck Wee
- ProvSec – 24-26 Nov (Kanazawa, Japan): Michel Abdalla, Damien Vergnaud

*8.1.2.2. Funding Panel and Committee Member*

- ANR – Scientific Evaluation Panel « Global Security and Cybersecurity »: Damien Vergnaud

### *8.1.3. 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 *Computers & Security* – Elsevier: David Naccache
- of *IEEE Transactions on Information Forensics and Security*: Michel Abdalla
- of *IET Information Security*: Michel Abdalla
- of *ETRI Journal*: Michel Abdalla

## 8.2. Teaching - Supervision - Juries

### *8.2.1. Teaching*

- Master: David Pointcheval, 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: David Pointcheval, Cryptography, M2, ESIEA

### 8.2.2. Supervision

- PhD: Sylvain Ruhault, Security Analysis of Pseudo Random Generators, ENS, June 30th, 2015, David Pointcheval & Damien Vergnaud
- PhD: Olivier Sanders, Conception et Optimisation de Mécanismes Cryptographiques Anonymes, ENS, September 24th, 2015, David Pointcheval
- PhD: Sonia Belaïd, Security of Cryptosystems Against Power-Analysis Attacks, ENS, October 22nd, 2015, Michel Abdalla
- PhD: Thomas Prest, Gaussian Sampling in Lattice-Based Cryptography, ENS, December 8th, 2015, Vadim Lyubashevsky
- PhD: Diana Maimut*, Authentication and Encryption Protocols: Design, Attacks and Algorithmic Improvements, ENS, December 11th, 2015, David Naccache
- PhD in progress: Fabrice Ben Hamouda, Leakage of information in cryptography, from 2012, Michel Abdalla & 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: Raphael Bost, Symmetric Searchable Encryption, from 2014, David Pointcheval
- 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
- PhD in progress: Thierry Mefenza Nountu, Number-Theoretic Study of Pseudorandom Cryptographic Primitives, from 2014, Damien Vergnaud
- PhD in progress: Pierre-Alain Dupont, Secure Communications, from 2015, David Pointcheval
- PhD in progress: Romain Gay, Functional Encryption, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Dahmun Gourdazi, Secure and Fast Cryptographic Implementation for Embedded Devices, from 2015, Damien Vergnaud
- PhD in progress: Louiza Khati, Disk Encryption Modes, from 2015, Damien Vergnaud
- PhD in progress: Michele Minelli, Increased efficiency and functionality through lattice-based cryptography, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Anca Nitulescu, Verifiable Outsourced Computations, from 2015, David Pointcheval
- PhD in progress: Razvan Rosie, Practical Functional Encryption Schemes For the Cloud, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Quentin Santos, Advanced Cryptography from a Blockchain, from 2015, David Pointcheval

* Since David Naccache left the team, these students also moved in his new Security team.

### 8.2.3. Juries

- HdR Benoît Libert. *Applications of Structure-Preserving Cryptography and Pairing-Based NIZK Proofs* – ENS Lyon – France, April 29th, 2015: David Pointcheval (reviewer)
- PhD Sylvain Ruhault. *Security Analysis of Pseudo Random Generators* – ENS – France, June 30th, 2015: David Pointcheval & Damien Vergnaud (supervisors)
- PhD Olivier Sanders. *Conception et Optimisation de Mécanismes Cryptographiques Anonymes* – ENS – France, September 24th, 2015: David Pointcheval (supervisor), Michel Abdalla
- PhD Sonia Belaïd. *Security of Cryptosystems Against Power-Analysis Attacks* – ENS – France, October 22nd, 2015: Michel Abdalla (supervisor)
- PhD Thomas Prest. *Gaussian Sampling in Lattice-Based Cryptography* – ENS – France, December 8th, 2015: Vadim Lyubashevsky (supervisor), David Pointcheval
- PhD Diana Maimut. *Authentication and Encryption Protocols: Design, Attacks and Algorithmic Improvements* – ENS – France, December 11th, 2015: David Naccache (supervisor), David Pointcheval
- PhD Bastien Vialla. *Contributions to Exact Linear Algebra over Finite Fields and Homomorphic Encryption* – Montpellier – France, December 14th, 2015: Damien Vergnaud (reviewer)

# 9. Bibliography

## Major publications by the team in recent years

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, H. Shi. *Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions*, in "Journal of Cryptology", July 2008, vol. 21, n$^o$ 3, pp. 350–391

[2] M. Abdalla, D. Catalano, D. Fiore. *Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions*, in "Journal of Cryptology", 2014, vol. 27, n$^o$ 3, pp. 544-593

[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] F. Benhamouda, O. Blazy, C. Chevalier, D. Pointcheval, D. Vergnaud. *New Techniques for SPHFs and Efficient One-Round PAKE Protocols*, in "Advances in Cryptology – Proceedings of CRYPTO '13 (1)", R. Canetti, J. A. Garay (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 8042, pp. 449-475

[5] 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", P. Rogaway (editor), Lecture Notes in Computer Science, Springer, 2011, vol. 6841, pp. 487-504

[6] I. Dinur, O. Dunkelman, N. Keller, A. Shamir. *New Attacks on Feistel Structures with Improved Memory Complexities*, in "Advances in Cryptology – Proceedings of CRYPTO '15 (1)", R. Gennaro, M. Robshaw (editors), Lecture Notes in Computer Science, Springer, 2015, vol. 9215, pp. 433-454

[7] 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 "Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS '13)", Berlin, Germany, V. D. Gligor, M. Yung (editors), ACM Press, 2013, pp. 647–658

[8] 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

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

[10] S. GORBUNOV, V. VAIKUNTANATHAN, H. WEE. *Predicate Encryption for Circuits from LWE*, in "Advances in Cryptology – Proceedings of CRYPTO '15 (2)", R. GENNARO, M. ROBSHAW (editors), Lecture Notes in Computer Science, Springer, 2015, vol. 9216, pp. 503-523

[11] V. LYUBASHEVSKY, C. PEIKERT, O. REGEV. *On Ideal Lattices and Learning with Errors over Rings*, in "Journal of the ACM", 2013, vol. 60, n$^{o}$ 6, pp. 43:1–43:35

[12] V. LYUBASHEVSKY, T. PREST. *Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices*, in "Advances in Cryptology – Proceedings of Eurocrypt '15 (1)", E. OSWALD, M. FISCHLIN (editors), Lecture Notes in Computer Science, Springer, 2015, vol. 9056, pp. 789-815

## Publications of the year

### Doctoral Dissertations and Habilitation Theses

[13] S. BELAÏD. *Security of Cryptosystems Against Power-Analysis Attacks*, ENS, October 2015, https://hal.inria.fr/tel-01235207

[14] T. PREST. *Gaussian Sampling in Lattice-Based Cryptography*, École Normale Supérieure, December 2015, https://tel.archives-ouvertes.fr/tel-01245066

[15] S. RUHAULT. *Security Analysis for Pseudo-Random Numbers Generators*, Ecole Normale Supérieure, June 2015, https://hal.inria.fr/tel-01236602

[16] O. SANDERS. *Design and Improvements of Anonymous Cryptographic Primitives*, Ecole Normale Supérieure, September 2015, https://hal.inria.fr/tel-01235213

### Articles in International Peer-Reviewed Journals

[17] M. ABDALLA, P.-A. FOUQUE, V. LYUBASHEVSKY, M. TIBOUCHI. *Tightly Secure Signatures From Lossy Identification Schemes*, in "Journal of Cryptology", 2015, 35 p. [*DOI :* 10.1007/s00145-015-9203-7], https://hal.inria.fr/hal-01136799

[18] I. DINUR, O. DUNKELMAN, N. KELLER, A. SHAMIR. *Reflections on slide with a twist attacks*, in "Designs, Codes and Cryptography", 2015, https://hal.archives-ouvertes.fr/hal-01235172

[19] D. NACCACHE, R. GÉRAUD, H. FERRADI, A. TRIA. *When organized crime applies academic results: a forensic analysis of an in-card listening device*, in "Journal of Cryptographic Engineering", October 2015, pp. 1-11 [*DOI :* 10.1007/s13389-015-0112-3], http://hal-emse.ccsd.cnrs.fr/emse-01222610

### Invited Conferences

[20] G. Couteau, T. Peters, D. Pointcheval. *Secure Distributed Computation on Private Inputs*, in "8th International Symposium on Foundations & Practice of Security", Clermont-Ferrand, France, LNCS, Springer, October 2015, https://hal.inria.fr/hal-01243278

### International Conferences with Proceedings

[21] M. Abdalla, S. Belaïd, D. Pointcheval, S. Ruhault, D. Vergnaud. *Robust Pseudo-Random Number Generators with Input Secure Against Side-Channel Attacks*, in "ACNS 2015", New York, United States, T. Malkin, V. Kolesnikov, A. B. Lewko, M. Polychronakis (editors), Lecture Notes in Computer Science, Springer, June 2015, vol. 9092 [*DOI :* 10.1007/978-3-319-28166-7_31], https://hal.inria.fr/hal-01242003

[22] M. Abdalla, F. Benhamouda, P. MacKenzie. *Security of the J-PAKE Password-Authenticated Key Exchange Protocol*, in "2015 IEEE Symposium on Security and Privacy", San Jose, United States, IEEE Computer Society, May 2015, pp. 571-587 [*DOI :* 10.1109/SP.2015.41], https://hal.inria.fr/hal-01175785

[23] M. Abdalla, F. Benhamouda, A. Passelègue. *An Algebraic Framework for Pseudorandom Functions and Applications to Related-Key Security*, in "CRYPTO 2015", Santa Barbara, United States, R. Gennaro, M. Robshaw (editors), Lecture Notes in Computer Science, Springer, August 2015, vol. 9215, pp. 388-409 [*DOI :* 10.1007/978-3-662-47989-6_19], https://hal.inria.fr/hal-01175786

[24] M. Abdalla, F. Benhamouda, A. Passelègue. *Multilinear and Aggregate Pseudorandom Functions: New Constructions and Improved Security*, in "ASIACRYPT 2015", Auckland, New Zealand, T. Iwata, J. H. Cheon (editors), Lecture Notes in Computer Science, Springer, November 2015, vol. 9452, pp. 103-120 [*DOI :* 10.1007/978-3-662-48797-6_5], https://hal.inria.fr/hal-01233740

[25] M. Abdalla, F. Benhamouda, D. Pointcheval. *Disjunctions for Hash Proof Systems: New Constructions and Applications*, in "EUROCRYPT 2015", Sofia, Bulgaria, E. Oswald, M. Fischlin (editors), Lecture Notes in Computer Science, Springer, April 2015, vol. 9057, pp. 69-100 [*DOI :* 10.1007/978-3-662-46803-6_3], https://hal.inria.fr/hal-01131994

[26] M. Abdalla, F. Benhamouda, D. Pointcheval. *Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks*, in "PKC 2015", Maryland, United States, J. Katz (editor), Lecture Notes in Computer Science, Springer, March 2015, vol. 9020, pp. 332-352 [*DOI :* 10.1007/978-3-662-46447-2_15], https://hal.inria.fr/hal-01131982

[27] M. Abdalla, F. Bourse, A. De Caro, D. Pointcheval. *Simple Functional Encryption Schemes for Inner Products*, in "PKC 2015", Maryland, United States, J. Katz (editor), Lecture Notes in Computer Science, Springer, March 2015, vol. 9020, pp. 733-751 [*DOI :* 10.1007/978-3-662-46447-2_33], https://hal.inria.fr/hal-01131971

[28] A. Bar-On, I. Dinur, O. Dunkelman, N. Keller, V. Lallemand, B. Tsaban. *Cryptanalysis of SP Networks with Partial Non-Linear Layers*, in "Eurocrypt 2015 : 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Sofia, Bulgaria, April 2015, pp. 315-342 [*DOI :* 10.1007/978-3-662-46800-5_13], https://hal.inria.fr/hal-01108331

[29] G. Barthe, S. Belaïd, F. Dupressoir, P.-A. Fouque, B. Grégoire, P.-Y. Strub. *Verified Proofs of Higher-Order Masking*, in "Eurocrypt 2015", Sofia, Bulgaria, Advances in Cryptology – EUROCRYPT 2015, April 2015, vol. series Lecture Notes in Computer Science, n$^{o}$ 9056 [*DOI :* 10.1007/978-3-662-46800-5_18], https://hal.inria.fr/hal-01216699

[30] A. Bauer, D. Vergnaud. *Practical Key Recovery for Discrete-Logarithm Based Authentication Schemes from Random Nonce Bits*, in "Cryptographic Hardware and Embedded Systems - CHES 2015", Saint-Malo, France, H. H. Tim Güneysu (editor), Lecture Notes in Computer Science, Springer, September 2015, vol. 9293, pp. 287-306 [*DOI :* 10.1007/978-3-662-48324-4_15], https://hal.inria.fr/hal-01214701

[31] S. Belaïd, J.-S. Coron, P.-A. Fouque, B. Gérard, J.-G. Kammerer, E. Prouff. *Improved Side-Channel Analysis of Finite-Field Multiplication*, in "CHES 2015", Saint-Malo, France, series Lecture Notes in Computer Science, September 2015, vol. 9293 [*DOI :* 10.1007/978-3-662-48324-4_20], https://hal.inria.fr/hal-01216706

[32] F. Benhamouda, G. Couteau, D. Pointcheval, H. Wee. *Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting*, in "CRYPTO 2015", Santa Barbara, United States, R. Gennaro, M. Robshaw (editors), Advances in Cryptology - CRYPTO 2015, Springer, August 2015, vol. 9216, 23 p. [*DOI :* 10.1007/978-3-662-48000-7_6], https://hal.inria.fr/hal-01187833

[33] F. Benhamouda, S. Krenn, V. Lyubashevsky, K. Pietrzak. *Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings*, in "ESORICS 2015", Vienna, Austria, Computer Security – ESORICS 2015, September 2015, vol. 9326, 21 p. [*DOI :* 10.1007/978-3-319-24174-6_16], https://hal.inria.fr/hal-01214722

[34] O. Blazy, C. Chevalier, D. Vergnaud. *Non-Interactive Zero-Knowledge Proofs of Non-Membership*, in "Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015", San Francisco, United States, K. Nyberg (editor), Springer, April 2015, vol. Lecture Notes in Computer Science 2014, n$^o$ 9048, pp. 145-164 [*DOI :* 10.1007/978-3-319-16715-2_8], https://hal.inria.fr/hal-01214711

[35] S. Canard, D. Pointcheval, O. Sanders, J. Traoré. *Divisible E-Cash Made Practical*, in "PKC 2015", Maryland, United States, J. Katz (editor), Lecture Notes in Computer Science, Springer, March 2015, vol. 9020, pp. 77-100 [*DOI :* 10.1007/978-3-662-46447-2_4], https://hal.inria.fr/hal-01134006

[36] S. Canard, D. Pointcheval, O. Sanders, J. Traoré. *Scalable Divisible E-Cash*, in "ACNS 2015", New York, United States, T. Malkin, V. Kolesnikov, A. B. Lewko, M. Polychronakis (editors), ACNS 2015, Springer Verlag, June 2015, vol. LNCS, n$^o$ 9092 [*DOI :* 10.1007/978-3-319-28166-7_14], https://hal.inria.fr/hal-01247652

[37] J. Chen, R. Gay, H. Wee. *Improved Dual System ABE in Prime-Order Groups via Predicate Encodings*, in "Advances in Cryptology - EUROCRYPT 2015", Sofia, Bulgaria, April 2015 [*DOI :* 10.1007/978-3-662-46803-6_20], https://hal.archives-ouvertes.fr/hal-01220358

[38] I. Dinur. *Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE*, in "EUROCRYPT 2015", Sofia, Bulgaria, Springer Verlag, 2015, vol. Lectures Notes in Computer Science, n$^o$ 9056, https://hal.archives-ouvertes.fr/hal-01235168

[39] I. Dinur, O. Dunkelman, N. Keller, A. Shamir. *New Attacks on Feistel Structures with Improved Memory Complexities*, in "CRYPTO 2015", California, United States, Springer Verlag, 2015, vol. LNCS, n$^o$ 9216, https://hal.archives-ouvertes.fr/hal-01235169

[40] I. Dinur, O. Dunkelman, G. Masha, A. Shamir. *Improved Top-Down Techniques in Differential Cryptanalysis*, in "LATINCRYPT 2015", Guadalajara, Mexico, Springer Verlag, 2015, vol. LNCS [*DOI :* 10.1007/978-3-319-22174-8_8], https://hal.archives-ouvertes.fr/hal-01235165

[41] I. DINUR, M. PAWEŁ, J. PIEPRZYK, S. MARIAN, S. MICHAŁ. *Cube Attacks and Cube-Attack-Like Cryptanalysis on the Round-Reduced Keccak Sponge Function*, in "EUROCRYPT 2015", Sofia, Bulgaria, Springer Verlag, 2015, vol. LNCS [*DOI :* 10.1007/978-3-662-46800-5_28], https://hal.archives-ouvertes.fr/hal-01235167

[42] I. DINUR, L. YUNWEN, W. MEIER, W. QINGJU. *Optimized Interpolation Attacks on LowMC*, in "ASIACRYPT 2015", Auckland, New Zealand, Springer Verlag, 2015, vol. LNCS, https://hal.archives-ouvertes.fr/hal-01235171

[43] R. GAY, I. KERENIDIS, H. WEE. *Communication Complexity of Conditional Disclosure of Secrets and Attribute-Based Encryption*, in "CRYPTO 2015 - Advances in Cryptology", Santa Barbara, United States, R. GENNARO, M. ROBSHAW (editors), Lecture Notes in Computer Science, Springer Berlin Heidelberg, August 2015, vol. 9216, pp. 485-502 [*DOI :* 10.1007/978-3-662-48000-7_24], https://hal.archives-ouvertes.fr/hal-01220355

[44] R. GAY, P. MÉAUX, H. WEE. *Predicate Encryption for Multi-dimensional Range Queries from Lattices*, in "PKC 2015 - Public-Key Cryptography", Gaithersburg, United States, J. KATZ (editor), Lecture Notes in Computer Science, Springer Berlin Heidelberg, April 2015, vol. 9020, pp. 752-776 [*DOI :* 10.1007/978-3-662-46447-2_34], https://hal.archives-ouvertes.fr/hal-01220353

[45] S. GORBUNOV, V. VAIKUNTANATHAN, H. WEE. *Predicate Encryption for Circuits from LWE*, in "CRYPTO (2) 2015", Santa Barbara, United States, August 2015 [*DOI :* 10.1007/978-3-662-48000-7_25], https://hal.inria.fr/hal-01220191

[46] E. KILTZ, P. JIAXIN, H. WEE. *Structure-Preserving Signatures from Standard Assumptions, Revisited*, in "CRYPTO (2) 2015", Santa Barbara, United States, August 2015 [*DOI :* 10.1007/978-3-662-48000-7_14], https://hal.inria.fr/hal-01220189

[47] E. KILTZ, H. WEE. *Quasi-Adaptive NIZK for Linear Subspaces Revisited*, in "EUROCRYPT 2015", Sofia, Bulgaria, April 2015, vol. LNCS [*DOI :* 10.1007/978-3-662-46803-6_4], https://hal.inria.fr/hal-01220192

[48] B. LIBERT, M. JOYE, M. YUNG, T. PETERS. *Secure Efficient History-Hiding Append-Only Signatures in the Standard Model*, in "Public Key Cryptography 2015 (PKC 2015)", Washington DC, United States, Public Key Cryptography 2015 (PKC 2015), Springer, March 2015, vol. 9020 [*DOI :* 10.1007/978-3-662-46447-2_20], https://hal.inria.fr/hal-01225344

[49] B. LIBERT, T. PETERS, M. JOYE, M. YUNG. *Compactly Hiding Linear Spans: Tightly Secure Constant-Size Simulation-Sound QA-NIZK Proofs and Applications*, in "Advances in Cryptology - Asiacrypt 2015", Auckland, New Zealand, Advances in Cryptology - Asiacrypt 2015, IACR, November 2015, https://hal.inria.fr/hal-01225363

[50] B. LIBERT, T. PETERS, M. YUNG. *Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions*, in "Advances in Cryptology - Crypto 2015", Santa Barbara, United States, Advances in Cryptology - Crypto 2015, Springer, August 2015, vol. 9216 [*DOI :* 10.1007/978-3-662-48000-7_15], https://hal.inria.fr/hal-01225353

[51] V. LYUBASHEVSKY, T. PREST. *Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices*, in "Eurocrypt 2015", Sofia, Bulgaria, Springer Verlag, May 2015, vol. LNCS [*DOI :* 10.1007/978-3-662-46800-5_30], https://hal.inria.fr/hal-01235176

[52] V. LYUBASHEVSKY, D. WICHS. *Simple Lattice Trapdoor Sampling from a Broad Class of Distributions*, in "Public Key Cryptography 2015", Gaithersburgh, United States, Springer Verlag, March 2015, vol. LNCS, n$^{O}$ 9020 [*DOI :* 10.1007/978-3-662-46447-2_32], https://hal.inria.fr/hal-01235177

### Scientific Books (or Scientific Book chapters)

[53] D. VERGNAUD. *Exercices et problèmes de cryptographie - 2ème édition*, Sciences Sup, Dunod, January 2015, 304 p. , https://hal.inria.fr/hal-01214714

### Research Reports

[54] M. ABDALLA, S. BELAÏD, P.-A. FOUQUE. *Leakage-Resilient Symmetric Encryption via Re-keying*, IACR, March 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/204, https://hal.inria.fr/hal-01132195

[55] M. ABDALLA, F. BENHAMOUDA, A. PASSELÈGUE. *An Algebraic Framework for Pseudorandom Functions and Applications to Related-Key Security*, IACR, June 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/554, https://hal.inria.fr/hal-01175788

[56] M. ABDALLA, F. BENHAMOUDA, A. PASSELÈGUE. *Multilinear and Aggregate Pseudorandom Functions: New Constructions and Improved Security*, IACR, September 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/867, https://hal.inria.fr/hal-01233749

[57] M. ABDALLA, F. BENHAMOUDA, D. POINTCHEVAL. *Tighter Reductions for Forward-Secure Signature Schemes*, IACR, March 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/196, https://hal.inria.fr/hal-01132190

[58] M. ABDALLA, F. BOURSE, 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

[59] F. BENHAMOUDA, O. BLAZY, C. CHEVALIER, D. POINTCHEVAL, D. VERGNAUD. *New Techniques for SPHFs and Efficient One-Round PAKE Protocols*, IACR, March 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/188, https://hal.inria.fr/hal-01139395

[60] F. BENHAMOUDA, G. COUTEAU, D. POINTCHEVAL, H. WEE. *Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting*, IACR, March 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/246, https://hal.archives-ouvertes.fr/hal-01139320

[61] S. CANARD, D. POINTCHEVAL, O. SANDERS. *Efficient Delegation of Zero-Knowledge Proofs of Knowledge in a Pairing-Friendly Setting*, IACR, March 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/278, https://hal.inria.fr/hal-01139397

[62] S. CANARD, D. POINTCHEVAL, O. SANDERS, J. TRAORÉ. *Scalable Divisible E-cash*, IACR, March 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/300, https://hal.inria.fr/hal-01139400

[63] G. COUTEAU, T. PETERS, D. POINTCHEVAL. *Secure Distributed Computation on Private Inputs*, IACR Cryptology ePrint Archive, December 2015, n$^{O}$ Cryptology ePrint Archive: Report 2015/1196, https://hal.inria.fr/hal-01245235

## Other Publications

[64] F. BENHAMOUDA, M. JOYE, B. LIBERT. *A New Framework for Privacy-Preserving Aggregation of Time-Series Data*, November 2015, working paper or preprint, https://hal.inria.fr/hal-01181321