IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Paris

Activity Report 2016

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

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
- 4.8. - Privacy-enhancing technologies
- 7. - Fundamental Algorithmics
- 7.7. - Number theory

Other Research Topics and Application Domains:

- 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]
Georg Fuchsbauer [Inria, Researcher]
Hoeteck Wee [CNRS, Researcher, HDR]

Faculty Members

Jacques Stern [ENS Paris, Emeritus Professor, HDR]
Damien Vergnaud [ENS Paris, Associate Professor, HDR]

PhD Students

Fabrice Ben Hamouda–Guichoux [ENS Paris, Fondation CFM, until August 2016]
Raphael Bost [DGA, Associated member]
Florian Bourse [CNRS, ERC CryptoCloud]
Jérémy Chotard [CNRS, ERC CryptoCloud, from October 2016]
Mario Cornejo Ramirez [Inria, CORDI-S, until September 2016]
Geoffroy Couteau [CNRS, ERC CryptoCloud]
Rafael Del Pino [Inria, FUI CryptoComp, until September 2016]
Aurélien Dupin [Thales, Associated member]
Pierre-Alain Dupont [DGA]
Romain Gay [ENS Paris]
Dahmun Gourdazi [CryptoExperts, CIFRE]
Louiza Khati [Oppida]
Pierrick Meaux [Inria, H2020 ICT SAFECrypto]
Thierry Mefenza Nountu [ENS Paris, ANR JCJC ROMAnTIC]
Michele Minelli [ENS Paris, H2020 ITN ECRYPT-NET]
Anca Nitulescu [CNRS, ERC CryptoCloud]
Michele Orrù [CNRS, ERC aSCEND, from November 2016]
Alain Passelegue [ENS Paris, DGA & ANR Prince]

Razvan Rosie [ENS Paris, H2020 ITN ECRYPT-NET]
Quentin Santos [Orange Labs, CIFRE]
Adrian Thillard [ANSSI]

Post-Doctoral Fellows

Pooya Farshim [ENS Paris, ANR EnBiD, from February 2016]
Julia Hesse [CNRS, ERC CryptoCloud, from October 2016]

Administrative Assistants

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

Others

Baptiste Louf [Ecole Polytechnique, Internship, from March to July 2016]
Balthazar Bauer [ENS Lyon, Internship, from September 2016]

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. Electronic Currencies

Electronic cash (e-cash) was first proposed in the 1980s but despite extensive research it has never been deployed on a large scale. Other means of digital payments have instead largely replaced cash and other "analog" payments. Common to all digital payments offered by banks and other payment providers is that they do not respect the citizens' right to privacy, which for legitimate purchases and moderate sums also includes their right of anonymous payments.

Recently the rise of so-called decentralized currencies, such as Bitcoin and the numerous “alt-coins” inspired by it, have established a third way of payments in addition to physical cash, which offers privacy, and card and other electronic payments, which are traceable by its providers. The continuous growth of popularity and usage of this new kind of currencies, also called “cryptocurrencies” as their security and stability crucially relies on the use of cryptography, have triggered a renewed interest in cryptographic e-cash.

Our group investigates “centralized” e-cash, which respects the current economic model where money is issued by (central) banks, as opposed to cryptocurrencies, which use money distribution to incentivize widespread participation in the system, required for stability. Of particular interest among centralized e-cash schemes is transferable e-cash, which allows users to transfer coins between each other without any interaction with a third party. Currently all efficient e-cash schemes require coins to be deposited at the bank once received; they are thus not transferable. Our goal is to propose efficient transferable e-cash schemes.

Another direction concerns cryptocurrencies whose adoption is continuously growing so that now even central banks, like the Swedish *Riksbank*, are considering issuing their own currency as a cryptocurrency. While systems like Bitcoin are perceived as offering anonymous payments, a line of research has shown that this is not the case. One of the major research challenges in this area is thus to devise schemes that offer an anonymity level comparable to that of physical cash. The currently proposed schemes either lack formal security analyses or they are inefficient due to the heavy-duty cryptography used. Our group works towards practical cryptocurrencies with formally analyzed privacy guarantees.

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

- Hoeteck Wee is one of the invited speakers at Asiacrypt 2016.
- Michel Abdalla is one of the invited speakers at ICISC 2016.

5.1.2. Awards

Romain Gay and Hoeteck Wee, together with Dennis Hofheinz and Eike Kiltz, received the Best Paper Award at Eurocrypt 2016 .

BEST PAPER AWARD:

[40]
R. GAY, D. HOFHEINZ, E. KILTZ, H. WEE. *Tightly CCA-Secure Encryption without Pairings*, in "Advances in Cryptology – EUROCRYPT 2016", Vienna, Austria, Advances in Cryptology – EUROCRYPT 2016, May 2016, vol. Lectures Notes in Computer Science, n° 9665 [*DOI :* 10.1007/978-3-662-49890-3_1], https://hal.archives-ouvertes.fr/hal-01302516

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 to the research program (see before) and the research projects (see after):

- More efficient constructions with lattices
- New e-cash constructions
- Advanced primitives for the privacy in the cloud
- Efficient functional encryption
- Various predicate encryption schemes

7. Partnerships and Cooperations

7.1. National Initiatives with Industrials

7.1.1. 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.

7.1.2. CryptoComp

Program: FUI

Duration: October 2014 – November 2018

Coordinator: CryptoExperts

Partners:

CEA

CNRS

Kalray

Inria

Dictao

Université de Limoges

VIACESS

Bertin technologies

GEMALTO

Local coordinator: David Pointcheval

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: ENS Lyon, Université de Limoges

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. 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.

7.2.3. EfTrEC

Title: Efficient Transferable E-Cash

Program: ANR JCJC

Duration: October 2016 – September 2020

PI: Georg Fuchsbauer

Partners:

Univ. Paris 2

This project deals with e-cash systems which let users transfer electronic coins between them offline. The main objectives of this project are:

- establish a clean formal model for the primitive;
- construct schemes which are practically efficient;
- develop schemes that are even resistant to attacks on quantum computers.

7.2.4. ALAMBIC

Title: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – September 2020

PI: Damien Vergnaud

Partners:

ENS Lyon

Univ. Limoges

The main objectives of the proposal are the following:

- Define theoretical models for "malleable" cryptographic primitives that capture strong practical attacks (in particular, in the settings of secure computation outsourcing, server-aided cryptography, cloud computing and cryptographic proof systems);
- Analyze the security and efficiency of primitives and constructions that rely on malleability;
- Conceive novel cryptographic primitives and constructions (for secure computation outsourcing, server-aided cryptography, multi-party computation, homomorphic encryption and their applications);
- Implement these new constructions in order to validate their efficiency and effective security.

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: Michel Abdalla

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)

IBM Research Zurich (Switzerland)

Local coordinator: Michel Abdalla

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. International Research Visitors

- Sanjam Garg (UC Berkeley)
- Yuval Ishai (UCLA/Technion)
- Gregory Neven (IBM Zurich)
- Ryo Nishimaki (NTT)
- Claudio Orlandi (Aarhus)
- Rafael Pass (Cornell)
- Leonid Reyzin (Boston University)
- Alessandra Scafuro (postdoc, BU/NEU)
- Victor Shoup (NY University)
- Vinod Vaikuntanathan (MIT)
- Daniel Wichs (Northeastern University)

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Events and Activities

- a regular seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html
- quarterly Paris Crypto Days (https://pariscryptoday.github.io) supported by CryptoCloud and aSCEND
- working group on lattices (http://perso.ens-lyon.fr/damien.stehle/LATTICE_MEETINGS.html), joint with ENS Lyon
- BibTeX database of papers related to Cryptography, open and widely used by the community (https://cryptobib.di.ens.fr)

8.1.1.2. Steering Committees of International Conferences

- steering committee of CANS: David Pointcheval
- steering committee of PKC: David Pointcheval
- 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 is 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 Chair

- Africacrypt '16 – 13-15 April (Fes, Morocco): David Pointcheval

8.1.2.2. Program Committee Member

- Financial Crypto '16 – 22–26 February (Barbados): Damien Vergnaud
- PKC '16 – 6-9 March (Taiwan): David Pointcheval
- Africacrypt '16 – 13-15 April (Fes, Morocco): Georg Fuchsbauer
- Eurocrypt '16 – 8-12 May (Vienna, Austria): Michel Abdalla and Georg Fuchsbauer
- AsiaPKC 2016 – 30 May 30 - 03 June (Xi'an, China): Damien Vergnaud
- Crypto '16 – 14-18 August (Santa Barbara, California, USA): David Pointcheval
- ACM CCS '16 – 24-28 October (Vienna, Austria): Hoeteck Wee
- ProvSec '16 – 10-12 November (Nanjing, China): Georg Fuchsbauer
- CANS '16 – 14-16 November (Milan, Italy): Georg Fuchsbauer
- Asiacrypt '16 – 4-8 December (Hanoi, Vietnam): Georg Fuchsbauer

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 *IET Information Security*: Michel Abdalla
- of *ETRI Journal*: Michel Abdalla
- of *Applicable Algebra in Engineering, Communication and Computing*: David Pointcheval

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, Cryptography, M2, MPRI
- Master: Damien Vergnaud, Advanced Algebra and Applications to Cryptography, Ecole Centrale Paris
- Master: David Pointcheval, Cryptography, M2, ESIEA
- IACR-SEAMS School on "Cryptography: Foundations and New Directions": David Pointcheval

8.2.2. Defenses

- PhD: Adrian Thillard, Counter-measures against side-channel attacks and secure multi-party computation, ENS, December 12th, 2016 (Supervisor: Damien Vergnaud)
- PhD: Alain Passelègue, Algebraic Frameworks for Pseudorandom Functions, ENS, December 9th, 2016 (Supervisor: Michel Abdalla)
- PhD: Mario Cornejo, Security for the cloud, ENS, November 17th, 2016 (Supervisor: Michel Abdalla)
- HdR: Hoeteck Wee, Advances in Functional Encryption, ENS, July 1st, 2016
- PhD: Fabrice Ben Hamouda, Diverse Modules and Zero-Knowledge, ENS, July 1st, 2016 (Supervisors: Michel Abdalla & David Pointcheval)

8.2.3. Supervision

- PhD in progress: Raphael Bost, Symmetric Searchable Encryption, from 2014, David Pointcheval (with Pierre-Alain Fouque, at Rennes)
- 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: 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: Aurélien Dupin, Multi-Party Computations, from 2015, David Pointcheval (with Christophe Bidan, at Rennes)
- 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
- PhD in progress: Jérémy Chotard, Attribute-Based Encryption, from 2016, David Pointcheval (with Duong Hieu Phan, at Limoges)
- PhD in progress: Michele Orrù, Functional Encryption, from 2016, Hoeteck Wee & Georg Fuchsbauer

8.2.4. Juries

- PhD Adrian Thillard. *Countermeasures to side-channel attacks and secure multi-party computation* – ENS – France, December 12th, 2016: Damien Vergnaud (supervisor)
- PhD Alain Passelègue. *Algebraic Frameworks for Pseudorandom Functions* – ENS – France, December 9th, 2016: Michel Abdalla (supervisor)
- PhD Mario Cornejo. *Security for the cloud* – ENS – France, November 17th, 2016: Michel Abdalla (supervisor), David Pointcheval
- PhD Christian Janson. *On the Verification of Computation and Data Retrievability* – Royal Holloway University of London – UK, October 11th, 2016: Michel Abdalla
- PhD Brice Minaud. *Analyse de primitives cryptographiques récentes* – Université Rennes I – France, October 7th, 2016: David Pointcheval
- PhD Houda Ferradi. *Integrity, Authentication and Confidentiality in Public-Key Cryptography* – ENS – France, September 22nd, 2016: Michel Abdalla
- HdR Hoeteck Wee. *Advances in Functional Encryption* – ENS – France, July 1st, 2016: Michel Abdalla, David Pointcheval
- PhD Fabrice Ben Hamouda. *Diverse Modules and Zero-Knowledge* – ENS – France, July 1st, 2016: Michel Abdalla & David Pointcheval (supervisors)
- PhD Alberto Battistello. *On the security of embedded systems against physical attacks* – UVSQ – France, June 29th, 2016: David Pointcheval
- PhD Antoine Delignat-Lavaud. *On the Security of Authentication Protocol for the Web* – ENS – France, March 14th, 2016: David Pointcheval
- PhD Rémy Chrétien. *Automated analysis of equivalence properties for cryptographic protocols* – ENS Cachan – January 11th, 2016: David Pointcheval

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] 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

[6] 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

[7] R. GAY, D. HOFHEINZ, E. KILTZ, H. WEE. *Tightly CCA-Secure Encryption Without Pairings*, in "Advances in Cryptology – Proceedings of Eurocrypt '16 (2)", M. FISCHLIN, J.-S. CORON (editors), Lecture Notes in Computer Science, Springer, 2016, vol. 9665, pp. 1–27

[8] 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

[9] 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

[10] 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

[11] F. BENHAMOUDA. *Diverse modules and zero-knowledge*, PSL Research University ; ENS Paris, July 2016, https://hal.inria.fr/tel-01399476

[12] M. CORNEJO-RAMIREZ. *Security for the Cloud*, ENS Paris - Ecole Normale Supérieure de Paris, November 2016, https://hal.inria.fr/tel-01399914

[13] A. PASSELÈGUE. *Algebraic Frameworks for Pseudorandom Functions*, PSL Research University, December 2016, https://hal.inria.fr/tel-01422093

[14] A. THILLARD. *Countermeasures to side-channel attacks and secure multi-party computation*, Ecole normale supérieure - ENS PARIS ; PSL Research University, December 2016, https://hal.inria.fr/tel-01415754

[15] H. WEE. *Advances in Functional Encryption*, ENS Paris - Ecole Normale Supérieure de Paris, July 2016, Habilitation à diriger des recherches, https://hal.inria.fr/tel-01399451

Articles in International Peer-Reviewed Journals

[16] M. ABDALLA, F. BENHAMOUDA, D. POINTCHEVAL. *Public-key encryption indistinguishable under plaintext-checkable attacks*, in "IET Information Security", November 2016, vol. 10, n° 6, pp. 288–303 [*DOI :* 10.1049/IET-IFS.2015.0500], https://hal.inria.fr/hal-01385178

[17] F. BENHAMOUDA, J. HERRANZ, M. JOYE, B. LIBERT. *Efficient Cryptosystems From 2^k -th Power Residue Symbols*, in "Journal of Cryptology", April 2016 [*DOI :* 10.1007/S00145-016-9229-5], https://hal.inria.fr/hal-01394400

[18] F. BENHAMOUDA, M. JOYE, B. LIBERT. *A New Framework for Privacy-Preserving Aggregation of Time-Series Data*, in "ACM Transactions on Information and System Security", April 2016, vol. 18, n° 3, 21 p. [*DOI :* 10.1145/2873069], https://hal.inria.fr/hal-01181321

[19] S. CANARD, D. POINTCHEVAL, O. SANDERS, J. TRAORÉ. *Divisible e-cash made practical*, in "IET Information Security", July 2016 [*DOI :* 10.1049/IET-IFS.2015.0485], https://hal.inria.fr/hal-01377998

[20] C. HAZAY, A. LÓPEZ-ALT, H. WEE, D. WICHS. *Leakage-Resilient Cryptography from Minimal Assumptions*, in "Journal of Cryptology", 2016, vol. 29, n° 3, pp. 514–551 [*DOI :* 10.1007/S00145-015-9200-X], https://hal.inria.fr/hal-01378199

[21] D. VERGNAUD. *Comment on "A strong provably secure IBE scheme without bilinear map" by M. Zheng, Y. Xiang and H. Zhou [J. Comput. Syst. Sci. 81 (2015) 125–131]*, in "Journal of Computer and System Sciences (JCSS)", August 2016, vol. 82, n° 5, 2 p. [*DOI :* 10.1016/J.JCSS.2015.12.003], https://hal.inria.fr/hal-01305462

International Conferences with Proceedings

[22] M. ABDALLA, M. CORNEJO, A. NITULESCU, D. POINTCHEVAL. *Robust Password-Protected Secret Sharing*, in "ESORICS 2016 - 21st European Symposium on Research in Computer Security", Heraklion, Greece, I. ASKOXYLAKIS, S. IOANNIDIS, S. KATSIKAS, C. MEADOWS (editors), Lecture Notes in Computer Science, Springer, September 2016, vol. 9879, pp. 61-79 [*DOI :* 10.1007/978-3-319-45741-3_4], https://hal.archives-ouvertes.fr/hal-01380699

[23] H. ABUSALAH, G. FUCHSBAUER. *Constrained PRFs for Unbounded Inputs with Short Keys*, in "Applied Cryptography and Network Security - 14th International Conference, ACNS 2016", Guildford, United Kingdom, June 2016 [*DOI :* 10.1007/978-3-319-39555-5_24], https://hal.inria.fr/hal-01384375

[24] H. ABUSALAH, G. FUCHSBAUER, K. PIETRZAK. *Offline Witness Encryption*, in "Applied Cryptography and Network Security - 14th International Conference, ACNS 2016", Guildford, United Kingdom, June 2016 [*DOI :* 10.1007/978-3-319-39555-5_16], https://hal.inria.fr/hal-01384371

[25] S. BELAID, F. BENHAMOUDA, A. PASSELÈGUE, E. PROUFF, A. THILLARD, D. VERGNAUD. *Randomness Complexity of Private Circuits for Multiplication*, in "EUROCRYPT 2016", Vienna, Austria, May 2016, pp. 616-648 [*DOI :* 10.1007/978-3-662-49896-5_22], https://hal.archives-ouvertes.fr/hal-01324823

[26] M. BELLARE, G. FUCHSBAUER, A. SCAFURO. *NIZKs with an Untrusted CRS: Security in the Face of Parameter Subversion*, in "Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference

on the Theory and Application of Cryptology and Information Security", Hanoi, Vietnam, December 2016, https://hal.inria.fr/hal-01384384

[27] F. BENHAMOUDA, C. CHEVALIER, A. THILLARD, D. VERGNAUD. *Easing Coppersmith Methods Using Analytic Combinatorics: Applications to Public-Key Cryptography with Weak Pseudorandomness*, in "Public-Key Cryptography – PKC 2016", Taipei, Taiwan, IACR, March 2016, vol. 9615, 31 p. [*DOI :* 10.1007/978-3-662-49387-8_3], https://hal.inria.fr/hal-01278460

[28] N. BITANSKY, R. NISHIMAKI, A. PASSELÈGUE, D. WICHS. *From Cryptomania to Obfustopia through Secret-Key Functional Encryption*, in "TCC 2016-B - Fourteenth IACR Theory of Cryptography Conference", Beijing, China, October 2016, https://hal.inria.fr/hal-01379256

[29] O. BLAZY, C. CHEVALIER, D. VERGNAUD. *Mitigating Server Breaches in Password-Based Authentication: Secure and Efficient Solutions*, in "CT-RSA 2016", San Francisco, France, K. SAKO (editor), The Cryptographers' Track at the RSA Conference, February 2016, vol. LNCS, n^{o} 9610 [*DOI :* 10.1007/978-3-319-29485-8_1], https://hal.archives-ouvertes.fr/hal-01292699

[30] F. BOURSE, R. DEL PINO, M. MINELLI, H. WEE. *FHE Circuit Privacy Almost for Free*, in "Crypto 2016 - 36th Annual International Cryptology Conference", Santa Barbara, United States, Crypto 2016, Springer Verlag, August 2016, vol. Lecture Notes in Computer Science, n^{o} 9815 [*DOI :* 10.1007/978-3-662-53008-5_3], https://hal.inria.fr/hal-01360110

[31] Z. BRAKERSKI, D. CASH, R. TSABARY, H. WEE. *Targeted Homomorphic Attribute-Based Encryption*, in "14th International Conference, TCC 2016-B", Beijing, China, M. HIRT, A. SMITH (editors), Lecture Notes in Computer Science, Springer, October 2016, vol. 9986, pp. 330-360, https://hal.inria.fr/hal-01378341

[32] Z. BRAKERSKI, V. VAIKUNTANATHAN, H. WEE, D. WICHS. *Obfuscating Conjunctions under Entropic Ring LWE*, in "ITCS", Cambridge, United States, 2016 [*DOI :* 10.1145/2840728.2840764], https://hal.inria.fr/hal-01378193

[33] P. CHAIDOS, V. CORTIER, G. FUCHSBAUER, D. GALINDO. *BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme*, in "23rd ACM Conference on Computer and Communications Security (CCS'16)", Vienna, Austria, October 2016 [*DOI :* 10.1145/2976749.2978337], https://hal.inria.fr/hal-01377917

[34] C. CHEVALIER, F. LAGUILLAUMIE, D. VERGNAUD. *Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis and Optimal Constructions*, in "Computer Security - ESORICS 2016", Heraklion, Greece, I. G. ASKOXYLAKIS, S. IOANNIDIS, S. K. KATSIKAS, C. A. MEADOWS (editors), Computer Security – ESORICS 2016, Springer, September 2016, vol. 9878, pp. 261-278 [*DOI :* 10.1007/978-3-319-45744-4_13], https://hal.inria.fr/hal-01375817

[35] G. COUTEAU, T. PETERS, T. PETERS, D. POINTCHEVAL. *Encryption Switching Protocols*, in "Crypto 2016 - 36th Annual International Cryptology Conference", Santa Barbara, United States, M. ROBSHAW, J. KATZ (editors), Springer, August 2016 [*DOI :* 10.1007/978-3-662-53018-4_12], https://hal.inria.fr/hal-01407341

[36] R. DEL PINO, V. LYUBASHEVSKY, D. POINTCHEVAL. *The Whole is Less Than the Sum of Its Parts: Constructing More Efficient Lattice-Based AKEs*, in "SCN 2016 - 10th International Conference Security and Cryptography for Networks", Amalfi, Italy, V. ZIKAS, R. D. PRISCO (editors), Security and Cryptography for Networks, Springer , August 2016, vol. Lecture Notes in Computer Science, n^{o} 9841, pp. 273 - 291 [*DOI :* 10.1007/978-3-319-44618-9_15], https://hal.inria.fr/hal-01378005

[37] H. FERRADI, R. GÉRAUD, D. MAIMUT, D. NACCACHE, D. POINTCHEVAL. *Legally Fair Contract Signing Without Keystones*, in "ACNS 2016 - 14th International Conference Applied Cryptography and Network Security", Guildford, United Kingdom, M. MANULIS, A.-R. SADEGHI, S. SCHNEIDER (editors), Applied Cryptography and Network Security, Springer, June 2016, vol. LNCS, n° 9696, pp. 175 - 190 [*DOI :* 10.1007/978-3-319-39555-5_10], https://hal.inria.fr/hal-01377993

[38] D. FIORE, A. NITULESCU. *On the (In)security of SNARKs in the Presence of Oracles*, in "TCC 2016-B - Fourteenth IACR Theory of Cryptography Conference", Beijing, China, Theory of Cryptography 14th International Conference, TCC 2016-B, Beijing, China, November 1-3, 2016, Proceedings, October 2016, https://hal.inria.fr/hal-01378013

[39] G. FUCHSBAUER, C. HANSER, C. KAMATH, D. SLAMANIG. *Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions*, in "Security and Cryptography for Networks - 10th International Conference, SCN 2016", Amalfi, Italy, August 2016 [*DOI :* 10.1007/978-3-319-44618-9_21], https://hal.inria.fr/hal-01384381

[40] *Best Paper*
R. GAY, D. HOFHEINZ, E. KILTZ, H. WEE. *Tightly CCA-Secure Encryption without Pairings*, in "Advances in Cryptology – EUROCRYPT 2016", Vienna, Austria, Advances in Cryptology – EUROCRYPT 2016, May 2016, vol. Lectures Notes in Computer Science, n° 9665 [*DOI :* 10.1007/978-3-662-49890-3_1], https://hal.archives-ouvertes.fr/hal-01302516.

[41] D. GOUDARZI, M. RIVAIN. *On the Multiplicative Complexity of Boolean Functions and Bitsliced Higher-Order Masking* , in "CHES", Santa-Barbara, United States, 2016, https://hal.inria.fr/hal-01379296

[42] D. GOUDARZI, M. RIVAIN, D. VERGNAUD. *Lattice Attacks against Elliptic-Curve Signatures with Blinded Scalar Multiplication*, in "Selected Areas in Cryptography - SAC 2016", St. John's, Canada, R. AVANZI, H. HEYS (editors), Selected Areas in Cryptography - SAC 2016, Springer, August 2016, https://hal.inria.fr/hal-01379249

[43] L. KHATI, N. MOUHA, D. VERGNAUD. *Full Disk Encryption: Bridging Theory and Practice*, in "CT-RSA 2017 - RSA Conference Cryptographers' Track", San Francisco, United States, Lecture Notes in Computer Science, February 2017, 16 p. , https://hal.inria.fr/hal-01403418

[44] H. KRAWCZYK, H. WEE. *The OPTLS Protocol and TLS 1.3*, in "EuroS&P", Saarbrücken, Germany, 2016 [*DOI :* 10.1109/EUROSP.2016.18], https://hal.inria.fr/hal-01378195

[45] T. MEFENZA. *Inferring Sequences Produced by a Linear Congruential Generator on Elliptic Curves Using Coppersmith's Methods*, in "COCOON 2016", Ho Chi Minh City, Vietnam, T. N. DINH, M. T. THAI (editors), 22nd International Computing and Combinatorics Conference, COCOON 2016, Springer Verlag, August 2016, vol. Lecture Notes in Computer Science, n° 9797, 12 p. [*DOI :* 10.1007/978-3-319-42634-1_24], https://hal.inria.fr/hal-01381658

[46] P. MÉAUX, A. JOURNAULT, F.-X. STANDAERT, C. CARLET. *Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts*, in "Advances in Cryptology – EUROCRYPT 2016", WIEN, Austria, Lecture Notes in Computer Science, May 2016, vol. 9665, pp. 311-343 [*DOI :* 10.1007/978-3-662-49890-3_13], https://hal.inria.fr/hal-01405859

[47] D. POINTCHEVAL, O. SANDERS. *Short Randomizable Signatures*, in "The Cryptographers' Track at the RSA Conference 2016", San Francisco, United States, K. SAKO (editor), Springer Verlag, February 2016, vol. LNCS, n° 9610, pp. 111 - 126 [*DOI :* 10.1007/978-3-319-29485-8_7], https://hal.inria.fr/hal-01377997

[48] H. WEE. *Déjà Q: Encore! Un Petit IBE*, in "TCC 2016 A", Tel Aviv, Israel, 2016 [*DOI :* 10.1007/978-3-662-49099-0_9], https://hal.inria.fr/hal-01378189

[49] H. WEE. *KDM-Security via Homomorphic Smooth Projective Hashing*, in "Public Key Cryptography", Taipei, Taiwan, 2016 [*DOI :* 10.1007/978-3-662-49387-8_7], https://hal.inria.fr/hal-01378191

Books or Proceedings Editing

[50] D. POINTCHEVAL, A. NITAJ, T. RACHIDI (editors). *8th International Conference on Cryptology in Africa - Africacrypt 2016*, Africacrypt 2016, Springer Verlag, Fes, Morocco, 2016, vol. LNCS, n° 9646 [*DOI :* 10.1007/978-3-319-31517-1], https://hal.inria.fr/hal-01377995

Research Reports

[51] M. ABDALLA, F. BOURSE, A. DE CARO, D. POINTCHEVAL. *Better Security for Functional Encryption for Inner Product Evaluations*, IACR, January 2016, n° Cryptology ePrint Archive: Report 2016/011, https://hal.archives-ouvertes.fr/hal-01380726

[52] M. ABDALLA, M. CORNEJO, A. NITULESCU, D. POINTCHEVAL. *Robust Password-Protected Secret Sharing*, IACR, May 2016, n° Cryptology ePrint Archive: Report 2016/123, https://hal.archives-ouvertes.fr/hal-01380730

[53] M. ABDALLA, M. RAYKOVA, H. WEE. *Multi-Input Inner-Product Functional Encryption from Pairings*, IACR, April 2016, n° Cryptology ePrint Archive: Report 2016/425, https://hal.archives-ouvertes.fr/hal-01380735

[54] J. CHOTARD, D. HIEU PHAN, D. POINTCHEVAL. *Homomorphic-Policy Attribute-Based Key Encapsulation Mechanisms*, IACR Cryptology ePrint Archive, November 2016, n° Cryptology ePrint Archive: Report 2016/1089, https://hal.inria.fr/hal-01402517

Other Publications

[55] M. JOYE, A. PASSELÈGUE. *Function-Revealing Encryption*, October 2016, working paper or preprint, https://hal.inria.fr/hal-01379260