IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Paris

Activity Report 2019

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:

A4. - Security and privacy
A4.3. - Cryptography
A4.3.1. - Public key cryptography
A4.3.3. - Cryptographic protocols
A4.8. - Privacy-enhancing technologies
A7. - Theory of computation
A8.5. - Number theory

Other Research Topics and Application Domains:

B6.4. - Internet of things
B9.5.1. - Computer science
B9.10. - Privacy

1. Team, Visitors, External Collaborators

Research Scientists

David Pointcheval [Team leader, CNRS, Senior Researcher, HDR]
Michel Ferreira Abdalla [CNRS, Researcher, HDR]
Georg Fuchsbauer [Inria, Researcher]
Brice Minaud [Inria, Researcher]
Phong-Quang Nguyen [Inria, Senior Researcher, HDR]
Hoeteck Wee [CNRS, Researcher, HDR]

Post-Doctoral Fellows

Ehsan Ebrahimi [Ecole Normale Supérieure Paris, from Feb 2019]
Pooya Farshim [CNRS, until Sep 2019]
Junqing Gong [CNRS]
Azam Soleimanian [Ecole Normale Supérieure Paris, from Feb 2019]

PhD Students

Balthazar Bauer [Inria]
Jérémy Chotard [CNRS]
Baptiste Cottier [Worldline, from Feb 2019]
Romain Gay [Ecole Normale Supérieure Paris, until Mar 2019]
Lenaïck Gouriou [Leanear, from Nov 2019]
Chloé Hébant [CNRS]
Louiza Khati [ANSSI, until Jun 2019]
Michele Orrù [CNRS]
Antoine Plouviez [Inria]
Mélissa Rossi [Thales & ANSSI]
Théo Ryffel [Inria, from Feb 2019]

2. Overall Objectives

2.1. Presentation

Cryptographic algorithms are the equivalent of locks, seals, security stamps and identification documents over the Internet. They are essential to protect our online bank transactions, credit cards, medical and personal information, and to support e-commerce and e-government. They come in different flavors. Encryption algorithms are necessary 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) and MAC algorithms replace hand-written signatures in electronic transactions. Identification protocols allow to securely verify the identity of a remote party. As a whole, cryptology is a research area with a high strategic impact in industry, for individuals, and for society as a whole. The research activity of project-team CASCADE addresses the following topics, which cover most of the areas that are currently active in the international cryptographic community, with a focus on public-key algorithms:

1. Implementation of cryptographic algorithms, and applied cryptography;
2. Algorithm and protocol design, and provable security;
3. Theoretical and practical 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 computational 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 to 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 group 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 provable security without such idealized assumptions, under new and possibly stronger computational assumptions. As a consequence, a cryptographer has to deal with the following four important steps, which are **all** main goals of ours:

computational assumptions, which are the foundation 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 ones, with additional features, etc.

security proof, which consists in exhibiting a reduction.

3. Research Program

3.1. Quantum-Safe 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 computing discrete logarithms. This is 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, which also offer features that other alternative public-key cryptosystems (such as MQ-based, code-based or hash-based schemes) cannot provide.

3.2. Advanced Encryption

Fully Homomorphic Encryption (FHE) has become a very active research area since 2009, when IBM announced the discovery of a FHE scheme by Craig Gentry. FHE allows to perform any computation on encrypted data, yielding the result encrypted under the same key. This enables outsourcing computation in the Cloud, on encrypted data, so the Cloud provider does not learn any information. However, FHE does not allow to share the result.

Functional encryption is another recent tool that allows an authority to deliver functional decryption keys, for any function f of his choice, so that when applied to the encryption of a message m, the functional decryption key yields $f(m)$. Since m can be a large vector, f can be an aggregation or statistical function: on encrypted data, one can get the result $f(m)$ in clear.

While this functionality has initially been defined in theory, our team has been very active in designing concrete instantiations for practical purposes.

3.3. Security amidst Concurrency on the Internet

Cryptographic protocols that are secure when executed in isolation can become 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, 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, and
2. 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 and the Blockchain

Electronic cash (e-cash) was first proposed in the 1980s but has never been deployed on a large scale. Other means of digital payments are instead largely replacing physical cash, but they do not respect the citizens' right to privacy, which includes their right of anonymous payments of moderate sums. Recently, so-called decentralized currencies, such as Bitcoin, have become a third type of payments in addition to physical cash, and card and other (non-anonymous) electronic payments. The continuous growth of popularity and usage of this new kind of currencies, also called "cryptocurrencies", have triggered a renewed interest in cryptographic e-cash.

On the one hand, our group investigates "centralized" e-cash, in keeping with the current economic model that has money be issued by (central) banks (while cryptocurrencies use money distribution as an incentive for participation in the system, on which its stability hinges). Of particular interest among centralized e-cash schemes is transferable e-cash, which allows users to transfer coins between each other without interacting with a third party (or the blockchain). Existing efficient e-cash schemes are not transferable, as they require coins to be deposited at the bank after having been used in a payment. Our goal is to propose efficient transferable e-cash schemes.

Another direction concerns (decentralized) cryptocurrencies, whose adoption has grown tremendously over the last few years. While in Bitcoin all transactions are publicly posted on the so-called "blockchain", other cryptocurrencies such as *Zcash* respect user privacy, whose security guarantees we have analyzed. Apart from privacy, two pressing challenges for cryptocurrencies, and blockchains in general, are sustainability and scalability. Regarding the former, we are addressing the electricity waste caused by the concept of "proof of work" used by all major cryptocurrencies by proposing alternatives; for the latter, we are working on proposals that avoid the need for all data having to be stored on the blockchain forever.

Blockchains have meanwhile found many other applications apart from electronic money. Together with Microsoft Research, our group investigates decentralized means of authentication that uses cryptography to guarantee privacy.

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.

5. Highlights of the Year

5.1. Awards

- The paper "The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes", by Tatsuaki Okamoto and David Pointcheval from PKC 2001, has received the Test-of-Time award at PKC 2019
- Raphaël Bost received the "2019 PhD Thesis Award" from the GDR Sécurité Informatique
- Mélissa Rossi received the L'Oréal-UNESCO For Women in Science Rising Talent Award Scholarship 2019.

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):

- Advanced primitives for privacy in the cloud
- Efficient functional encryption
- Attribute and predicate encryption schemes
- New primitives for efficient anonymous authentication
- Applications to machine learning
- Blockchain protocols
- Searchable Encryption

7. Partnerships and Cooperations

7.1. National Initiatives with Industry

7.1.1. ANBLIC: Analysis in Blind Clouds

Program: FUI

Duration: January 2018 – December 2020

Coordinator: Wallix

Partners: UPEC, CEA, Atos, SOGETI, CoeSSI

Local coordinator: David Pointcheval

The main goal is to industrialize for the first time several privacy enhancing technologies that are on the edge of theory and practice.

Fully Homomorphic Encryption let cloud providers compute arbitrary functions on their client's encrypted data, ensuring at the same time full privacy and functionality. Functional Encryption is a refinement of classical encryption, which allows data owners to delegate fine-grained access to their data. Thus it is possible to enable the computation of aggregated statistics over your personal data, while cryptographically ensuring its confidentiality.

However both these technologies still suffer from prohibitive inefficiencies for business applications. ANBLIC's academic partners will create new cryptographic schemes and performance models, tailored for industrial use cases, and create the first real-life scenario of encrypted queries on encrypted data and on open data.

7.1.2. RISQ: Regroupement de l'Industrie française pour la Sécurité Post-Quantique

Program: GDN

Duration: February 2017 – September 2020

Coordinator: Secure-IC

Partners: ANSSI, AIRBUS, C-S, CEA LIST, CryptoExperts, Inria/ENS/CASCADE, GEMALTO, Inria POLSYS, Inria AriC, IRISA, Orange Labs, THALES, UVSQ, PCQC

Local coordinator: Michel Abdalla and Phong Nguyen since September 2019

The main goal of RISQ is to help the French Industry and Academia become a significant international player in the transition to post-quantum cryptography.

7.2. National Collaborations with Academics

7.2.1. EnBiD: Encryption for Big Data

Program: ANR JCJC

Duration: October 2014 – September 2019

PI: Hoeteck Wee

Partners: Université Paris 2, Université 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.

7.2.2. EfTrEC: Efficient Transferable E-Cash

Program: ANR JCJC

Duration: October 2016 – December 2019

PI: Georg Fuchsbauer

Partners: Université 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 resistant to attacks on quantum computers.

7.2.3. SaFED: Safe and Functional Encrypted Databases

Program: ANR JCJC

Duration: October 2019 – Septembre 2023

PI: Brice Minaud

Partners: ENS, DGA

This project addresses the security of encrypted databases, with the proposal of new searchable encryption techniques and deeper security analysis.

7.2.4. ALAMBIC: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – September 2020

PI: Damien Vergnaud

Partners: ENS Lyon, Université 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. CryptoCloud: Cryptography for the Cloud

Program: FP7 ERC Advanced Grant

Duration: June 2014 – May 2020

PI: David Pointcheval

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

7.3.2. SAFEcrypto: 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 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.

7.3.3. ECRYPT-NET: 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), Inria/ENS (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.

7.3.4. aSCEND: Secure Computation on Encrypted Data

Program: H2020 ERC Starting Grant

Duration: June 2015 – May 2021

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.

7.3.5. FENTEC: Functional Encryption Technologies

Program: H2020

Duration: January 2018 – December 2020

Coordinator: ATOS Spain SA

Scientific coordinator: Michel Abdalla

Partners: Inria/ENS (France), Flensburg University (Germany), KU Leuven (Belgium), University of Helsinki (Finland), Nagra (Switzerland), XLAB (Switzerland), University of Edinburgh (United Kingdom), WALLIX (France)

Local coordinator: Michel Abdalla

Functional encryption (FE) has recently been introduced as a new paradigm of encryption systems to overcome all-or-nothing limitations of classical encryption. In an FE system the decryptor deciphers a function over the message plaintext: such functional decryptability makes it feasible to process encrypted data (e.g. on the Internet) and obtain a partial view of the message plaintext. This extra flexibility over classical encryption is a powerful enabler for many emerging security technologies (i.e. controlled access, searching and computing on encrypted data, program obfuscation...). FENTEC's mission is to make the functional encryption paradigm ready for wide-range applications, integrating it in ICT technologies as naturally as classical encryption. The primary objective is the efficient and application-oriented development of functional encryption systems. FENTEC's team of cryptographers, software and hardware experts and information technology industry partners will document functional encryption needs of specific applications and subsequently design, develop, implement and demonstrate applied use of functional cryptography. Ultimately, a functional encryption library for both SW and HW-oriented application will be documented and made public so that it may be used by European ICT entities. With it, the FENTEC team will build emerging security technologies that increase the trustworthiness of the European ICT services and products. Concretely, the FENTEC team will showcase the expressiveness and versatility of the functional encryption paradigm in 3 use cases:

- Privacy-preserving digital currency, enforcing flexible auditing models
- Anonymous data analytics enabling computation of statistics over encrypted data, protecting European Fundamental Rights of Data Protection and Privacy
- Key and content distribution with improved performance & efficiency as foundational technology for establishing secure communication among a vast number of IOT devices.

7.4. International Initiatives with Industry

7.4.1. CryptBloC: Cryptography for the Blockchain

Partners: MSR Redmond (USA), MSR Cambridge (UK), Inria

Duration: October 2017 – October 2021

PI: Georg Fuchsbauer

The goal of this Microsoft-Inria joint project on privacy and decentralization is to use cryptography to improve privacy on the blockchain and decentralized systems more generally. We will investigate means of privacy-preserving authentication, such as electronic currencies, and other applications of blockchain and distributed transparency mechanisms.

7.5. International Research Visitors

7.5.1. Professors

- Sep 1 - Oct 31, 2019: Manuel Barbosa (University of Porto)
- Jun 20 - 21, 2019: Jean Paul Degabriele (TU Darmstadt)
- Jun 20 - 30, 2019: Joël Alwen (Wickr)
- Jul 4-5, 2019: David Wu (University of Virginia)

7.5.2. PhD students

- Jun 18 - 25, 2019: Ward Beullens (KU Leuven)
- Jun 15 - Jul 1, 2019: Rotem Tsabary (Weizmann)
- June 1 - 30, 2019: Hendrik Waldner (Edinburgh)
- Jun 23 - Jul 3, 2019: Naty Peter (Ben-Gurion University)

7.6. Internships

- Apr-Sep 2019: Hugo Marival (Ecole Polytechnique) - Michel Abdalla and David Pointcheval
- Apr-Sep 2019: Thibaut Bagory (ENS Paris-Saclay - UVSQ) - Brice Minaud
- Oct-Dec 2019: Marie Euler (X - DGA) - Brice Minaud

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Events and Activities

- Quarterly Paris Crypto Days (https://pariscryptoday.github.io) supported by CryptoCloud and aSCEND
- Seminars are organized: https://crypto.di.ens.fr/web2py/index/seminars

- OPACity – Obfuscation: Proofs, Attacks & Candidates, (http://crypto-events.di.ens.fr/opacity/) Eurocrypt affiliated event. May 19, 2019, Darmstadt, supported by aSCEND
- 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 Information-Theoretic Cryptography Conference: Hoeteck Wee

8.1.1.3. Board of International Organisations

- Board of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2013 – 2021)
- President-Elect of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2019 –)

8.1.2. Scientific Events Selection

8.1.2.1. Program Committee Member

- ACNS '19 (Bogotá, Colombia): Michel Abdalla
- ASIACRYPT '19 (Kobe, Japan): Brice Minaud, Hoeteck Wee
- CT-RSA '19 (San Francisco, California, USA): David Pointcheval
- EUROCRYPT '19 (Darmstadt, Germany): Michel Abdalla
- LATINCRYPT '19 (Santiago, Chile): Michel Abdalla
- PKC '20 (Edinburgh, Scotland): Georg Fuchsbauer

8.1.2.2. Editorial Boards of Journals

Editor-in-Chief

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

Associate Editor

- of *ETRI Journal*: Michel Abdalla
- of *Journal of Mathematical Cryptology*: Phong Nguyen
- of *Applicable Algebra in Engineering, Communication and Computing*: David Pointcheval

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Master: Michel Abdalla, Brice Minaud, Cryptography, M2, MPRI
- Master: Phong Nguyen, Cryptography, M2, ESIEA
- Bachelor: Brice Minaud, Georg Fuchsbauer, David Pointcheval, Introduction to Cryptology, L3/M1, ENS
- Bachelor: Michel Abdalla, Formal Languages, Computability, and Complexity, L3/M1,
- Bachelor: Georg Fuchsbauer, Cryptography, École supérieure d'ingénieurs Léonard-de-Vinci

8.2.2. Defenses

- PhD: Romain Gay, Public-key Encryption, Revisited: Tight Security and Richer Functionalities, ENS, March 18th, 2019 (Supervisors: Michel Abdalla & Hoeteck Wee)

- PhD: Anca Nitulescu, A Tale of SNARKs: Quantum Resilience, Knowledge Extractability and Data Privacy, ENS, April 1st, 2019 (Supervisors: Michel Abdalla, Dario Fiore & David Pointcheval)
- PhD: Razvan Rosie, On the Achievability of White-Box Cryptography, ENS, May 28th, 2019 (Supervisor: Michel Abdalla)
- PhD: Louiza Khati, Full Disk Encryption and Beyond, ENS, July 15th, 2019 (Supervisor: Damien Vergnaud)
- PhD: Jérémy Chotard, Delegation in Functional Encryption, ENS, December 2nd, 2019 (Supervisor: David Pointcheval, with Duong Hieu Phan, at Limoges)

8.2.3. Supervision

- PhD in progress: Michele Orrù, Functional Encryption, from 2016, Georg Fuchsbauer & Hoeteck Wee
- PhD in progress: Balthazar Bauer, Transferable e-Cash, from 2017, Georg Fuchsbauer
- PhD in progress: Chloé Hébant, Big Data and Privacy, from 2017, David Pointcheval (with Duong Hieu Phan, at Limoges)
- PhD in progress: Mélissa Rossi, Post-Quantum Cryptography, from 2017, Michel Abdalla (with Henri Gilbert at ANSSI)
- PhD in progress: Antoine Plouviez, Privacy and Decentralization, from 2018, Georg Fuchsbauer
- PhD in progress: Baptiste Cottier, Privacy-preserving anomaly detection, from 2019, David Pointcheval (with Olivier Blazy, at Limoges)
- PhD in progress: Théo Ryffel, Privacy-preserving federated learning, from 2019, Francis Bach and David Pointcheval
- PhD in progress: Lénaïck Gouriou, Advanced encryption with post-quantum security, from 2019, David Pointcheval (with Cécile Delerablée at Leanear)

8.2.4. Committees

- PhD Marc Beunardeau. *Cryptographie Appliquée à la Sécurité des Systèmes d'Information* – Ecole Normale Supérieure – France – January 15th, 2019: David Pointcheval (Chair)
- HdR Catalin Hritcu. *The Quest for Formally Secure Compartmentalizing Compilation* – Ecole Normale Supérieure – France – January 29th, 2019: David Pointcheval
- PhD Romain Gay. *Public-key Encryption, Revisited: Tight Security and Richer Functionalities* – Ecole Normale Supérieure – France – March 18th, 2019: Michel Abdalla and Hoeteck Wee (Co-supervisors)
- PhD Mary Maller. *Practical zero-knowledge arguments from structured reference strings* – University College London – United Kingdom – March 26th, 2019: Georg Fuchsbauer (Reviewer)
- PhD Anca Nitulescu. *A Tale of SNARKs: Quantum Resilience, Knowledge Extractability and Data Privacy* – Ecole Normale Supérieure – France – April 1st, 2019: Michel Abdalla and David Pointcheval (Co-supervisors)
- PhD José Miguel López Becerra. *Provable Security Analysis for the PAKE Problem* – University of Luxembourg – Luxembourg – May 14th, 2019: Michel Abdalla
- PhD Razvan Rosie. *On the Achievability of White-Box Cryptography* – Ecole Normale Supérieure – France – May 28th, 2019: Michel Abdalla (Supervisor)
- HdR Olivier Blazy. *Hash Proofs Systems and Applications to Implicit Cryptography* – Université de Limoges – France – June 12th, 2019: David Pointcheval
- PhD Aurélien Dupin. *Secure Multi-Party Computation and Privacy* – Université Bretagne Loire – France – June 13rd, 2019: David Pointcheval (Co-supervisor)

- PhD Louiza Khati. *Full Disk Encryption and Beyond* – Ecole Normale Supérieure – France – July 15th, 2019: David Pointcheval
- PhD Julian Loss. *New Techniques for the Modular Analysis of Digital Signature Schemes* – Ruhr Universität Bochum – Germany – July 20th, 2019; David Pointcheval (Reviewer)
- PhD Aisling Connolly. *New Notions of Security, Broken Assumptions, and Increased Efficiency* – Ecole Normale Supérieure – France – September 13th, 2019: Michel Abdalla
- PhD Chen Qian. *Lossy Trapdoor Primitives, Zero-Knowledge Proofs and Applications* – Université de Rennes 1 – France – October 4th, 2019: Michel Abdalla
- PhD Alice Pellet–Mary. *On ideal lattices and the GGH13 multilinear map* – Ecole Normale Supérieure de Lyon – France – October 16th, 2019: David Pointcheval (Chair and Reviewer)
- HdR Guilhem Castagnos. *Cryptography based on Quadratic Fields: Cryptanalyses, Primitives and Protocols* – Université de Bordeaux – France – November 8th, 2019: David Pointcheval (Reviewer)
- PhD Joseph Lallemand. *Vote électronique : définitions et techniques d'analyse* – Université de Lorraine – France – November 8th, 2019: David Pointcheval (Reviewer)
- PhD Loïc Ferreira. *Secure Tunnels for Constrained Environments* – Université Bretagne Loire – France – November 18th, 2019: David Pointcheval
- PhD Pauline Bert. *Lattice-based signatures: from construction to implementation* – Université Bretagne Loire – France – November 29th, 2019: David Pointcheval
- PhD Jérémy Chotard. *Delegation in functional encryption* – Université de Limoges - France – Décember 2nd, 2019: David Pointcheval (Co-supervisor) and Michel Abdalla (Chair)

9. Bibliography

Major publications by the team in recent years

[1] 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

[2] M. ABE, G. FUCHSBAUER, J. GROTH, K. HARALAMBIEV, M. OHKUBO. *Structure-Preserving Signatures and Commitments to Group Elements*, in "Journal of Cryptology", 2016, vol. 29, n^{o} 2, pp. 363–421

[3] 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

[4] P. CHAIDOS, V. CORTIER, G. FUCHSBAUER, D. GALINDO. *BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme*, in "Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS '16)", E. R. WEIPPL, S. KATZENBEISSER, C. KRUEGEL, A. C. MYERS, S. HALEVI (editors), ACM Press, 2016, pp. 1614–1625

[5] 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

[6] 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

[7] 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

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

[9] W. QUACH, H. WEE, D. WICHS. *Laconic Function Evaluation and Applications*, in "59th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2018)", M. THORUP (editor), IEEE, 2018

Publications of the year

Doctoral Dissertations and Habilitation Theses

[10] J. CHOTARD. *Delegation in functional encryption*, Université de Limoges, France, December 2019, https://hal.archives-ouvertes.fr/tel-02394349

[11] R. GAY. *Public-Key Encryption, Revisited: Tight Security and Richer Functionalities*, PSL Research University, March 2019, https://tel.archives-ouvertes.fr/tel-02137987

[12] L. KHATI. *Full Disk Encryption and Beyond*, Université PSL ; ENS Paris - Ecole Normale Supérieure de Paris, July 2019, Equipe cascade, ENS, Inria, https://tel.archives-ouvertes.fr/tel-02318449

[13] A. NITULESCU. *A tale of SNARKs: quantum resilience, knowledge extractability and data privacy*, École Normale Supérieure (Paris), April 2019, https://hal.archives-ouvertes.fr/tel-02129544

[14] R. ROŞIE. *On the achievability of white-box cryptography*, PSL Research University, May 2019, https://tel.archives-ouvertes.fr/tel-02332996

Articles in International Peer-Reviewed Journals

[15] M. ABDALLA, F. BENHAMOUDA, D. POINTCHEVAL. *On the Tightness of Forward-Secure Signature Reductions*, in "Journal of Cryptology", January 2019, vol. 32, n° 1, pp. 84-150 [*DOI :* 10.1007/s00145-018-9283-2], https://hal.inria.fr/hal-01722996

[16] A. CONNOLLY, P. FARSHIM, G. FUCHSBAUER. *Security of Symmetric Primitives against Key-Correlated Attacks*, in "IACR Transactions on Symmetric Cryptology", September 2019, https://hal.inria.fr/hal-02396311

[17] M. SEO, M. ABDALLA, D. H. LEE, J. H. PARK. *New technique for chosen-ciphertext security based on non-interactive zero-knowledge*, in "Information Sciences", July 2019, vol. 490, pp. 18-35 [*DOI :* 10.1016/J.INS.2019.03.063], https://hal.inria.fr/hal-02135837

International Conferences with Proceedings

[18] M. ABDALLA, F. BENHAMOUDA, R. GAY. *From Single-Input to Multi-client Inner-Product Functional Encryption*, in "Advances in Cryptology – ASIACRYPT 2019", Kobe, Japan, S. D. GALBRAITH, S. MORIAI

(editors), Lecture Notes in Computer Science, November 2019, vol. 11923, pp. 552-582 [*DOI :* 10.1007/978-3-030-34618-8_19], https://hal.inria.fr/hal-02375577

[19] M. ABDALLA, F. BENHAMOUDA, M. KOHLWEISS, H. WALDNER. *Decentralizing Inner-Product Functional Encryption*, in "Public-Key Cryptography – PKC 2019", Beijing, China, D. LIN, K. SAKO (editors), Lecture Notes in Computer Science, April 2019, vol. 11443, pp. 128-157 [*DOI :* 10.1007/978-3-030-17259-6_5], https://hal.inria.fr/hal-02135871

[20] M. ABDALLA, F. BENHAMOUDA, A. PASSELÈGUE. *Algebraic XOR-RKA-Secure Pseudorandom Functions from Post-Zeroizing Multilinear Maps*, in "Advances in Cryptology – ASIACRYPT 2019", Kobe, Japan, S. D. GALBRAITH, S. MORIAI (editors), Lecture Notes in Computer Science, November 2019, vol. 11922, pp. 386-412 [*DOI :* 10.1007/978-3-030-34621-8_14], https://hal.inria.fr/hal-02375594

[21] M. BARBOSA, D. CATALANO, A. SOLEIMANIAN, B. WARINSCHI. *Efficient Function-Hiding Functional Encryption: From Inner-Products to Orthogonality*, in "Topics in Cryptology – CT-RSA 2019", San Francisco, United States, M. MATSUI (editor), Lecture Notes in Computer Science, February 2019, vol. 11405, pp. 127-148 [*DOI :* 10.1007/978-3-030-12612-4_7], https://hal.inria.fr/hal-02363215

[22] A. BAUER, H. GILBERT, G. RENAULT, M. ROSSI. *Assessment of the Key-Reuse Resilience of NewHope*, in "CT-RSA 2019 - The Cryptographers' Track at the RSA Conference", San Francisco, United States, M. MATSUI (editor), Lecture Notes in Computer Science, Springer, February 2019, vol. 11405, pp. 272-292 [*DOI :* 10.1007/978-3-030-12612-4_14], https://hal.archives-ouvertes.fr/hal-02139910

[23] W. BEULLENS, H. WEE. *Obfuscating Simple Functionalities from Knowledge Assumptions*, in "PKC 2019 - International Conference on Practice and Theory of Public Key Cryptography", Beijing, China, April 2019, pp. 254-283 [*DOI :* 10.1007/978-3-030-17259-6_9], https://hal.inria.fr/hal-02358436

[24] F. BOURSE, D. POINTCHEVAL, O. SANDERS. *Divisible E-Cash from Constrained Pseudo-Random Functions*, in "ASIACRYPT 2019 - 25th Annual International Conference on the Theory and Application of Cryptology and Information Security", Kobe, Japan, Advances in Cryptology, December 2019, vol. LNCS, n° 11922, https://hal.inria.fr/hal-02357173

[25] E. DUFOUR-SANS, D. POINTCHEVAL. *Unbounded Inner-Product Functional Encryption with Succinct Keys*, in "ACNS 2019 - 17th International Conference on Applied Cryptography and Network Security", Bogota, Colombia, Springer, May 2019, vol. LNCS, n° 11464, pp. 426-441 [*DOI :* 10.1007/978-3-030-21568-2_21], https://hal.inria.fr/hal-02357165

[26] G. FUCHSBAUER. *WI Is Not Enough: Zero-Knowledge Contingent (Service) Payments Revisited*, in "ACM CCS 2019 - 26th ACM Conference on Computer and Communications Security", London, United Kingdom, ACM Press, November 2019, pp. 49-62 [*DOI :* 10.1145/3319535.3354234], https://hal.inria.fr/hal-02396308

[27] G. FUCHSBAUER, C. KAMATH, K. KLEIN, K. PIETRZAK. *Adaptively Secure Proxy Re-encryption*, in "Public-Key Cryptography – PKC 2019", Beijing, China, D. LIN, K. SAKO (editors), LNCS - Lecture Notes in Computer Science, Springer, April 2019, vol. 11443 [*DOI :* 10.1007/978-3-030-17259-6_11], https://hal.inria.fr/hal-02396301

[28] G. FUCHSBAUER, M. ORRÙ, Y. SEURIN. *Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble*, in "Advances in Cryptology - EUROCRYPT 2019", Darmstadt, Germany, Y. ISHAI, V. RIJMEN

(editors), LNCS - Lecture Notes in Computer Science, Springer, May 2019, vol. 11476 [*DOI :* 10.1007/978-3-030-17653-2_22], https://hal.inria.fr/hal-02396305

[29] J. GONG, B. WATERS, H. WEE. *ABE for DFA from k-Lin*, in "CRYPTO 2019 - 39th Annual International Cryptology Conference", Santa Barbara, United States, August 2019, pp. 732-764 [*DOI :* 10.1007/978-3-030-26951-7_25], https://hal.inria.fr/hal-02358440

[30] P. GRUBBS, M.-S. LACHARITÉ, B. MINAUD, K. G. PATERSON. *Learning to Reconstruct: Statistical Learning Theory and Encrypted Database Attacks*, in "IEEE Symposium on Security and Privacy (S&P) 2019", San Francisco, United States, May 2019, https://hal.inria.fr/hal-01974962

[31] C. HÉBANT, D. H. PHAN, D. POINTCHEVAL. *Decentralized Evaluation of Quadratic Polynomials on Encrypted Data*, in "ISC 2019 - International Conference on Information Security", New York, United States, Z. LIN, C. PAPAMANTHOU, M. POLYCHRONAKIS (editors), ISC 2019 - International Conference on Information Security, Springer, September 2019, vol. LNCS, n° 11723, pp. 87-106 [*DOI :* 10.1007/978-3-030-30215-3_5], https://hal.archives-ouvertes.fr/hal-02345627

[32] L. KHATI, D. VERGNAUD. *Analysis and Improvement of an Authentication Scheme in Incremental Cryptography*, in "Selected Areas in Cryptography - SAC 2018", Calgary, Canada, C. CID, M. J. JACOBSON JR. (editors), Lecture Notes in Computer Science, Springer, January 2019, vol. 11349, pp. 50-70 [*DOI :* 10.1007/978-3-030-10970-7_3], https://hal.inria.fr/hal-01893905

[33] L. KOWALCZYK, H. WEE. *Compact Adaptively Secure ABE for* NC^1 *from k-Lin*, in "EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques", Darmstadt, Germany, April 2019, pp. 3-33 [*DOI :* 10.1007/978-3-030-17653-2_1], https://hal.inria.fr/hal-02358429

[34] T. RYFFEL, E. DUFOUR-SANS, R. GAY, F. BACH, D. POINTCHEVAL. *Partially Encrypted Machine Learning using Functional Encryption*, in "NeurIPS 2019 - Thirty-third Conference on Neural Information Processing Systems", Vancouver, Canada, Advances in Neural Information Processing Systems, December 2019, https://arxiv.org/abs/1905.10214 , https://hal.inria.fr/hal-02357181

Research Reports

[35] M. ABDALLA, M. BARBOSA. *Perfect Forward Security of SPAKE2*, IACR Cryptology ePrint Archive, October 2019, n° Report 2019/1194, https://hal.inria.fr/hal-02317002

[36] M. ABDALLA, F. BENHAMOUDA, R. GAY. *From Single-Input to Multi-Client Inner-Product Functional Encryption*, IACR Cryptology ePrint Archive, May 2019, n° Report 2019/487, https://hal.inria.fr/hal-02135963

[37] M. ABDALLA, F. BENHAMOUDA, M. KOHLWEISS, H. WALDNER. *Decentralizing Inner-Product Functional Encryption*, IACR Cryptology ePrint Archive, January 2019, n° Report 2019/020, https://hal.inria.fr/hal-02317011