RESEARCH CENTRE

Paris

IN PARTNERSHIP WITH:

CNRS, Ecole normale supérieure de Paris, CNRS, Ecole normale supérieure de Paris

2021

ACTIVITY REPORT

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, Département d'Informatique de l'Ecole Normale Supérieure

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team CASCADE

Creation of the Project-Team: 2008 July 01

Keywords

Computer sciences and digital sciences

A4. – Security and privacy

A4.3. – Cryptography

A4.3.1. – Public key cryptography

A4.3.2. – Secret key cryptography

A4.3.3. – Cryptographic protocols

A4.3.4. – Quantum Cryptography

A4.8. – Privacy-enhancing technologies

A7. – Theory of computation

A7.1.4. – Quantum algorithms

A8.5. – Number theory

A8.9. – Performance evaluation

A8.10. – Computer arithmetic

A9.2. – Machine learning

Other research topics and application domains

B6.4. – Internet of things

B9.5.1. – Computer science

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- David Pointcheval [Team leader, CNRS, Senior Researcher, HDR]
- Céline Chevalier [Univ Panthéon-Assas, Researcher, HDR]
- Michel Ferreira Abdalla [CNRS, Senior Researcher, Until Sep 2021, HDR]
- Brice Minaud [Inria, Researcher]
- Phong-Quang Nguyen [Inria, Senior Researcher, HDR]
- Thomas Vidick [Inria, Advanced Research Position, Apr 2021]

Post-Doctoral Fellow

- Thanh-Huyen Nguyen [Inria, From Dec 2021]

PhD Students

- Leonard Assouline [École Normale Supérieure de Paris]
- Hugo Beguinet [Thales, From Oct 2021]
- Baptiste Cottier [Wordline]
- Paola De Perthuis [Cosmian Tech SAS]
- Guillaume Gette [DGA]
- Lenaick Gouriou [Leanear]
- Chloe Hebant [CNRS, until Jun 2021]
- Paul Hermouet [Inria]
- Ngoc Ky Nguyen [École Normale Supérieure de Paris, from Sep 2021]
- Antoine Plouviez [Inria, until Aug 2021]
- Michael Reichle [Inria]
- Theo Ryffel [Inria]
- Hugo Senet [Thales]
- Quoc Huy Vu [Univ Panthéon-Assas]

Administrative Assistants

- Nathalie Gaudechoux [Inria]
- Meriem Guemair [Inria]

External Collaborator

- Antoine Plouviez [Ministère de l'Education Nationale, from Sep 2021 until Nov 2021]

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. 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. The techniques are derived from complexity theory, providing (polynomial) reductions. And the more efficient the reduction can be, the better the parameters of the schemes will be.

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. Better attacks against the algorithmic problems are thus studied.

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.

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, isogeny-based or hash-based schemes) cannot provide. The ERC Advanced Grant PARQ aims at evaluating the security of lattice-based cryptography, with respect to the most powerful adversaries, such as quantum computers and large-scale parallel computers.

In the meantime, although a universal quantum computer may be some decades in the future, quantum communication and quantum error correcting codes are beginning to become concretely available. It is already possible to prepare, manipulate and precisely control systems involving a few quantum information bits (qubits). Such quantum technologies could help improve the efficiency and security of concrete cryptographic protocols. The ANR JCJC project CryptiQ aims at considering three possible scenarios (first, the simple existence of a quantum attacker, then the access to quantum communication for anyone, and finally a complete quantum world) and studies the consequences on the cryptographic protocols currently available. This implies elaborating adversarial models and designing or analyzing concrete protocols with formal security proofs, in order to get ready as soon as one of these scenarios becomes the new reality.

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 (FE) 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.

Another approach is to focus on a type of computation over encrypted data of particular interest, namely the ability to search over encrypted data. Here, a client encrypts its data, and sends it to a distant server. The client should then be able to issue queries to the server, asking for elements within the encrypted data that fit some search criterion. The server should be able to correctly answer the query, without learning the client's data (which remains encrypted), or even the contents of the query (which is also encrypted). In this context, the server is regarded as a honest-but-curious adversary attempting to infer private information as it processes the client's queries. By restricting the range of functionalities

compared to FHE and FE, and allowing a controlled amount of leakage, Searchable Symmetric Encryption (SSE) enables very efficient solutions, which can be deployed at scale.

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.

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** (FE), 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, namely for machine learning techniques. Machine learning makes an intensive use of comparisons, for the activation of neurons, and new approaches have been proposed for efficient comparisons with interactive protocols.

4.2 Searchable Encryption

Searchable Encryption (SE) is another technique that aims to protect users' privacy with regard to data uploaded to the cloud. Searchable Encryption is equally concerned with scalability, with the aim to accomodate large real-world databases. As a concrete application, an email provider may wish to store its users' emails in an encrypted form to provide privacy; but it is obviously highly desirable that users should still be able to search for emails that contain a given word, or whose date falls within a given range. Businesses may also want to outsource databases containing sensitive information, such as client data, for example to dispense with a costly dedicated IT department. To be usable at all, the outsourced encrypted database should still offer some form of search functionality. Failing that, the entire database must be downloaded to process each query to the database, defeating the purpose of cloud storage.

In many contexts, the amount of data outsourced by a client is large, and the overhead incurred by generic solutions such as FHE or FE becomes prohibitive. The goal of Searchable Encryption is to find practical trade-offs between privacy, functionality, and efficiency. Regarding functionality, the focus is mainly on privately searching over encrypted cloud data, altough many SE schemes also support simple forms of update operation. Regarding privacy, SE typically allows the server to learn *some* information on the encrypted data. This information is formally captured by a *leakage function*. Security proofs show that the cloud server does not learn any more information about the client's data than what is expressed by the leakage function.

The additional flexibility afforded by allowing a controlled amount of leakage enables SE to offer highly efficient solutions, which can be deployed in practice on large datasets. The main goal of our research in this area is to analyze the precise privacy impact of different leakage functions; propose new techniques to reduce this leakage; as well as extend the range of functionality achieved by Searchable Encryption.

4.3 Post-Quantum Standardization

In recent years, there has been very significant investment on research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography or quantum-safe cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communication protocols and networks.

In 2016, NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Round 3 candidates were announced on July 22, 2020. Out of the seven finalists, five are based on lattice problems: CRYSTALS-KYBER, NTRU and SABER for encryption, CRYSTALS-DILITHIUM and FALCON for signature. We intend to study the best lattice algorithms in order to assess the security of the five NIST finalists based on the hardness of lattice problems.

4.4 Provable Security for the Quantum Internet

With several initiatives such as the development of a 2,000 km quantum network in China, the access of IBM's quantum platform freely available and the efforts made in the EU for instance with the quantum

internet alliance team, we can assume that in a further future, not only the adversary has potential access to a quantum computer, but everybody may have access to quantum channels, allowing honest parties to exchange quantum data up to a limited amount. Going one step further than post-quantum cryptography, it is therefore needed to carefully study the security models and properties of classical protocols or the soundness of classical theoretical results in such a setting. Some security notions have already been defined but others have to be extended, such as the formal treatment of superposition attacks initiated by Zhandry.

On the positive side, some quantum primitives which are already well-studied, unconditionally quantum secure and already deployed in practice (such as Quantum Key Distribution) allow for new security properties such as everlasting confidentiality for sensitive long-lived data (which holds even if an attacker stores encrypted data now and decrypts them later when a quantum computer becomes available). We intend to study to what extent allowing honest parties to have access to currently available (or near-term) quantum technologies allows to achieve quantum-enhanced protocols (for classical functionalities) with improved security or efficiency beyond what is possible classically.

5 Social and environmental responsibility

5.1 Footprint of research activities

Unfortunately, private computation is usually at a huge cost: it definitely costs more to compute on encrypted data than on clear inputs. However, our goal is definitely to reduce this cost, as it will improve the user experience at the same time, with shorter computation time.

5.2 Impact of research results

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.

Both design of new primitives and study of the best attacks are essential for this goal.

6 Highlights of the year

6.1 Awards

- May 2021. David Pointcheval is the recipient of the RSA Conference 2021 Award for Excellence in the Field of Mathematics
- March 2021. David Pointcheval has been awarded the CNRS silver medal

7 New results

All the results of the team have been published (see the list of publications). They are all related to the research program (see Section 3) and the research projects (see Sections 8 and 9):

- Advanced primitives for privacy in the cloud
- Efficient functional encryption
- Attribute and predicate encryption schemes
- New primitives for efficient anonymous authentication
- Application of multi-party computation to machine learning
- Searchable Encryption

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

CryptBloC: Cryptography for the Blockchain

Duration: October 2017 – October 2021

Partners: MSR Redmond (USA), MSR Cambridge (UK), Inria/ENS/Cascade

Inria contact: David Pointcheval

Summary: 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.

8.2 Bilateral grants with industry

SecNISQ: Calcul Securisé Multipartite pour Architectures NISQ

Program: ANR PRCE

Duration: October 2021 – October 2025

Coordinator: Elham Kashefi

Partners: LIP6/Univ. Paris 6, CRED/Univ. Paris 2, VeriQloud, Inria

Inria contact: Céline Chevalier

Summary: SecNISQ aims at developing a platform for multi clients-server distributed quantum computing. While currently some quantum devices are remotely accessible, providing integrity as well as privacy of data processing remains a challenging task that we aim to address in this project. We have recently proposed the first framework for secure multi party quantum computing as a novel path to address this challenge. However optimizing these protocols for currently available NISQ devices on one hand as well as specific usecases identified by the industry partner on the other hand, is the main target of this project. This will be based on detailed use-case analyses, classical and quantum sub-protocol designs, guided by numerical simulations of the performances that could be obtained in realistic situation taking into account also the underlying constraints of the NISQ architecture.

PRESTO: PRocessing Encrypted Streams for Traffic Oversight

Program: ANR PRCE

Duration: January 2020 – June 2024

Coordinator: David Pointcheval

Partners: Inria/ENS/Cascade, IMT/Telecom SudParis, LORIA, Orange Labs, 6cure

Inria contact: David Pointcheval

Summary: While GDPR (General Data Protection Regulation) imposes some privacy constraints, growing threats against servers require traffic analysis to detect malicious behaviors. This analysis includes identification of illegitimate connections to mitigate denial of service attacks, content filtering to limit content exposition or content leakage, and log management for later forensic analysis. Security Information and Event Management (SIEM) that deals with internal and external threats should still remain effective under GDPR constraints. Data protection usually means encryption, which in turn heavily limits the traffic analysis capabilities.

The main goal of this project is to bridge the gap between these two security and privacy requirements, with advanced cryptographic tools (such as searchable encryption, functional encryption, fully homomorphic encryption, and multi-party computation) in order to provide privacy to the end-users while allowing traffic monitoring by the network security manager. While current tools already work on encrypted streams by analyzing the meta-data only, advanced encryption tools may enrich the analysis by specific researches in the encrypted payload.

ANBLIC: Analysis in Blind Clouds

Program: FUI

Duration: January 2018 – November 2021

Coordinator: Wallix

Partners: UPEC, CEA, Atos, SOGETI, CoeSSI, Inria/ENS/Cascade

Inria contact: David Pointcheval

Summary: 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.

Crypto4Graph-AI: advanCed pRivacY Preserving TechnOlogies for enterprise knowledge GRAPHs and Artificial Intelligence

Program: ANR PRCI

Duration: September 2021 – August 2024

Coordinator: Fraunhofer / Cosmian

Partners: Cosmian, Fraunhofer, Eccenca

Inria contact: David Pointcheval

Summary: The overall objective of CRYPTO4GRAPH-AI is to develop a data management framework to train machine learning (ML) models that utilize privacy enhancing technologies (PETs) to discover knowledge graphs (KGs) for improved decision making. KGs enjoy increasing popularity in enterprises for their ability to integrate data from heterogeneous sources, plus rich metadata and a machine-comprehensible semantic representation of background knowledge in a uniform structure. Beyond Google's or Facebook's graphs, KGs have been applied to enterprise cybersecurity, supply chain management, genomics, drug-drug-interaction, and biological networks. While data owners are often not willing to share sensitive data such as business-critical data, this data can be valuable for analyses in other contexts for different stakeholders or even for multiple data owners interested to mutualise their data.

9 Partnerships and cooperations

9.1 International research visitors

Thomas Vidick, from Caltech, visited Cascade on April 2021.

9.2 European initiatives

H2020 ICT FENTEC

Title: Functional Encryption Technologies

Duration: January 2018 – February 2021

Coordinator: ATOS Spain

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)

Inria contact: Michel Abdalla

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

H2020 ERC Advanced Grant PARQ

Title: Lattices in a Parallel and Quantum World

Duration: July 2020 – June 2025

Principal Investigator: Phong Nguyen

Summary: Quantum computers could one day become so powerful that they could break even the most sophisticated cryptography. This means that our internet communications and e-commerce will no longer be safe. Another future challenge is the threat posed by new environments such as Big Data, the Internet of Things and cryptocurrencies, where traditional cryptography is not enough. The goal of the PARQ project is to guarantee the security of lattice-based cryptography, which have been proposed for quantum-safe cryptography, homomorphic encryption and lightweight public-key cryptography. Specifically, the project will identify the best parallel and quantum algorithms for lattice problems, and propose practical methods to choose safe parameters according to the threat level.

H2020 ERC Proof of Concept CryptAnalytics

Title: Secure Analytics as Business Services

Duration: April 2021 – September 2022

Principal Investigator: David Pointcheval

Summary: Big data and data lakes are gold mines for data scientists with tons of applications to finance, medicine, economics, etc. But most of these data are quite sensitive and cannot be widely distributed or even just used without strong protection. One is thus facing the huge dilemma of having to make the choice between highly valuable analytics and privacy. The ERC CryptoCloud project

has designed several primitives perfectly well-suited to such situations. They are quite powerful but also highly technical for appropriate deployment at scale. The European start-up Cosmian has been interested in our tools, and we have already started a fruitful collaboration. The main goal of this CryptAnalytics project is to develop a unified platform that will allow dealing with many situations, for secure analytics as business services. This will accelerate the development of Cosmian, giving a major competitive advantage on the fast emerging market of data analytics, with strong privacy guarantees by design. Companies are realizing the incredible value of privacy-preserving analytics. As a result, the number of business use-cases is exploding, but each application is a new challenge in itself, with new kinds of evaluations, new privacy concerns, and different amounts of data.

9.3 National initiatives

SaFED: Safe and Functional Encrypted Databases

Program: ANR JCJC

Duration: October 2019 – March 2024

Coordinator: Brice Minaud

Partners: DGA, Inria/ENS/Cascade

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

CryptiQ: Cryptography in a Quantum World

Program: ANR JCJC

Duration: January 2019 – June 2023

Coordinator: Céline Chevalier

Partners: Univ Panthéon-Assas

Summary: In a context where the threat of a quantum attacker which could completely break many widely-used public-key cryptosystems becomes plausible and quantum communication technologies become available in practice, the goal of the project is to anticipate these major changes in three plausible scenarios (post-quantum cryptography, quantum-enhanced classical cryptography and cryptography in a quantum world), and find in each case the most relevant security models to construct and prove concrete protocols.

ALAMBIC: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – April 2022

Coordinator: Damien Vergnaud

Partners: ENS Lyon, Université Limoges, Inria/ENS/Cascade

Inria contact: David Pointcheval

Summary: 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.

10 Dissemination

10.1 Scientific events: organisation

- Seminars are organized: see Web Page
- BibTeX database of papers related to Cryptography, open and widely used by the community (see Web Page)

Steering Committees of International Conferences

- Steering committee of CANS: David Pointcheval
- Steering committee of PKC: David Pointcheval
- Steering committee of LATINCRYPT: Michel Abdalla

Board of International Organisations

- President of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2020 – 2022)

10.2 Scientific events: selection

Program Committee Member

- CT-RSA '22 (San Francisco, California, USA): David Pointcheval, Brice Minaud
- ToSC/FSE '22 (Athens, Greece): Brice Minaud
- Latincrypt'21 (Bogotá, Colombia): Céline Chevalier
- Indocrypt'21 (Jaipur, India): Céline Chevalier
- Crypto '21 (Virtual): Brice Minaud
- CT-RSA '21 (San Francisco, California, USA): Céline Chevalier

Editorial Boards of Journals

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

10.3 Teaching - supervision - juries

10.3.1 Education

- Master: Michel Abdalla, Brice Minaud, Phong Nguyen, David Pointcheval, Cryptography, M2, MPRI
- Master: Phong Nguyen, Cryptography, M2, ESIEA
- Master: Céline Chevalier, Data Science, M2, Univ Panthéon-Assas
- Bachelor: Brice Minaud, David Pointcheval, Introduction to Cryptology, L3/M1, ENS
- Bachelor: Michel Abdalla, Formal Languages, Computability, and Complexity, L3/M1, ENS

10.3.2 PhD's in the Team

Defenses

- PhD: Antoine Plouviez, The security of the One-More Discrete-Logarithm assumption and Blind Schnorr Signatures, ENS, October 29th, 2021 (Supervisors: Georg Fuchsbauer & David Pointcheval)
- PhD: Chloé Hébant, Homomorphic Cryptography and Privacy, ENS, May 20th, 2021 (Supervisors: David Pointchevak & Duong Hieu Phan, at Telecom Paris)

Supervision

- PhD in progress: Quoc-Huy Vu, Cryptography in a Quantum World, from 2018, Céline Chevalier
- PhD in progress: Baptiste Cottier, Privacy-preserving anomaly detection, from 2019, David Pointcheval (with Olivier Blazy, at Ecole Polytechnique)
- 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
- PhD in progress: Léonard Assouline, Encryption for Fine-Grained Access Control, from 2020, Michel Abdalla and Brice Minaud
- PhD in progress: Paola de Perthuis, Efficient Protocols for Secure Computation over Confidential Data, from 2020, David Pointcheval
- PhD in progress: Michael Reichle, Searchable encryption, from 2020, Brice Minaud and Michel Abdalla
- PhD in progress: Hugo Senet, Anonymous Post-Quantum Cryptographic Protocols, from 2020, Céline Chevalier
- PhD in progress: Paul Hermouet, from 2020, Céline Chevalier
- PhD in progress: Guillaume Gette, from 2020, Phong Nguyen
- PhD in progress: Hugo Beguinet, from 2021, Céline Chevalier
- PhD in progress: Ngoc Ky Nguyen, Computations on encrypted data, from 2021, David Pointcheval

10.3.3 Committees

- PhD Céline Duguey. *On the Security of Instant Messaging (Towards solutions for multi-device and group applications)* – Université de Rennes – France – December 14th, 2021: Céline Chevalier
- PhD Katharina Boudgoust. *Theoretical Hardness of Algebraically Structured Learning With Errors* – Université de Rennes – France – November 16th, 2021: Michel Abdalla, Céline Chevalier (Reviewer)
- PhD Antoine Plouviez. *The security of the One-More Discrete-Logarithm assumption and Blind Schnorr Signatures* – Ecole Normale Supérieure – France – October 29th, 2021: David Pointcheval (Co-supervisor)
- PhD Luka Music. *Multi-Party Quantum Cryptography: From Folklore to Real-World* – Sorbonne Université – France – July 9th, 2021: Céline Chevalier (Co-supervisor) and David Pointcheval (Chair)
- PhD Adel Hamdi. *Chiffrement fonctionnel pour le traitement des données externes en aveugle* – Université Claude Bernard Lyon 1 – France – July 9th, 2021: Michel Abdalla, Céline Chevalier (Reviewer)

- PhD Luca Notarnicola. *On Euclidean Lattices, Edwards Curves and Cryptographic Multilinear Maps* – Université du Luxembourg – Luxembourg – July 6th, 2021: Phong Nguyen
- HDR Adeline Roux-Langlois. *On the hardness of the Learning With Errors problem and its variants* – Université de Rennes – France – June 22nd, 2021: Céline Chevalier (Reviewer), David Pointcheval
- PhD Chloé Hébant. *Homomorphic Cryptography and Privacy* – Ecole Normale Supérieure – France – May 20th, 2021: David Pointcheval (Co-supervisor)
- PhD Xuan Thanh Do. *Constructions des schémas cryptographiques multi-utilisateurs* – Université de Limoges / Vietnam National University – March 26th, 2021: Céline Chevalier (reviewer), David Pointcheval (Chair)
- PhD Rajendra Kumar. *Exponential Time/Space Algorithms and Reductions for Lattice Problems* – Indian Institute of Technology, Kanpur and National University of Singapore – 2021: Phong Nguyen (Reviewer)

11 Scientific production

11.1 Major publications

[1] M. Abdalla, D. Catalano and D. Fiore. 'Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions'. In: *Journal of Cryptology* 27.3 (2014), pp. 544–593.

[2] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev and M. Ohkubo. 'Structure-Preserving Signatures and Commitments to Group Elements'. In: *Journal of Cryptology* 29.2 (2016), pp. 363–421.

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

[4] P. Chaidos, V. Cortier, G. Fuchsbauer and 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)*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers and S. Halevi. ACM Press, 2016, pp. 1614–1625.

[5] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergnaud and 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)*. Ed. by V. D. Gligor and M. Yung. Berlin, Germany: ACM Press, 2013, pp. 647–658.

[6] R. Gay, D. Hofheinz, E. Kiltz and H. Wee. 'Tightly CCA-Secure Encryption Without Pairings'. In: *Advances in Cryptology – Proceedings of Eurocrypt '16 (2)*. Ed. by M. Fischlin and J.-S. Coron. Vol. 9665. Lecture Notes in Computer Science. Springer, 2016, pp. 1–27.

[7] S. Gorbunov, V. Vaikuntanathan and H. Wee. 'Predicate Encryption for Circuits from LWE'. In: *Advances in Cryptology – Proceedings of CRYPTO '15 (2)*. Ed. by R. Gennaro and M. Robshaw. Vol. 9216. Lecture Notes in Computer Science. Springer, 2015, pp. 503–523.

[8] V. Lyubashevsky, C. Peikert and O. Regev. 'On Ideal Lattices and Learning with Errors over Rings'. In: *Journal of the ACM* 60.6 (2013), 43:1–43:35.

[9] W. Quach, H. Wee and D. Wichs. 'Laconic Function Evaluation and Applications'. In: *59th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2018)*. Ed. by M. Thorup. IEEE, 2018.

11.2 Publications of the year

International journals

[10] L. Assouline and T. Liu. 'Multi-party PSM, Revisited: Improved Communication and Unbalanced Communication'. In: *Lecture Notes in Computer Science* (2021). URL: https://hal.archives-ouvertes.fr/hal-03413130.

[11] O. Blazy, L. Brouilhet, C. Chevalier, P. Towa, I. Tucker and D. Vergnaud. 'Hardware security without secure hardware: How to decrypt with a password and a server'. In: *Theoretical Computer Science* 895 (Dec. 2021), pp. 178–211. DOI: 10.1016/j.tcs.2021.09.042. URL: https://hal.archives-ouvertes.fr/hal-03378464.

[12] C. Chevalier, F. Laguillaumie and D. Vergnaud. 'Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis and Optimal Constructions'. In: *Algorithmica* 83.1 (30th Jan. 2021), pp. 72–115. DOI: 10.1007/s00453-020-00750-2. URL: https://hal.archives-ouvertes.fr/hal-02899803.

[13] H. Kim, Y. Lee, M. Abdalla and J. H. Park. 'Practical dynamic group signature with efficient concurrent joins and batch verifications'. In: *Journal of information security and applications* 63 (Dec. 2021), p. 103003. DOI: 10.1016/j.jisa.2021.103003. URL: https://hal.inria.fr/hal-03442068.

International peer-reviewed conferences

[14] S. Bettaieb, L. Bidoux, O. Blazy, B. Cottier and D. Pointcheval. 'Secure Decision Forest Evaluation'. In: ARES 2021 - 16th International Conference on Availability, Reliability and Security. Vienna, Austria: ACM, 16th Aug. 2021, pp. 1–12. DOI: 10.1145/3465481.3465763. URL: https://hal.inria.fr/hal-03321368.

[15] A. Bossuat, R. Bost, P.-A. Fouque, B. Minaud and M. Reichle. 'SSE and SSD: Page-Efficient Searchable Symmetric Encryption'. In: Crypto 2021 - Annual International Cryptology Conference. Virtual, France, 16th Aug. 2021. URL: https://hal.inria.fr/hal-03377462.

Scientific book chapters

[16] M. Abdalla, M. Barbosa, J. Katz, J. Loss and J. Xu. 'Algebraic Adversaries in the Universal Composability Framework'. In: *Advances in Cryptology – ASIACRYPT 2021*. Vol. 13092. Lecture Notes in Computer Science. Springer International Publishing, 1st Dec. 2021, pp. 311–341. DOI: 10.1007/978-3-030-92078-4_11. URL: https://hal.inria.fr/hal-03517558.

[17] M. Abdalla, B. Haase and J. Hesse. 'Security Analysis of CPace'. In: *Advances in Cryptology – ASIACRYPT 2021*. Vol. 13093. Lecture Notes in Computer Science. Springer International Publishing, 1st Dec. 2021, pp. 711–741. DOI: 10.1007/978-3-030-92068-5_24. URL: https://hal.inria.fr/hal-03517563.

Doctoral dissertations and habilitation theses

[18] C. Hébant. 'Homomorphic Cryptography and Privacy'. Université PSL, 20th May 2021. URL: https://hal.archives-ouvertes.fr/tel-03439366.

[19] A. Plouviez. 'The security of the One-More Discrete-Logarithm assumption and Blind Schnorr Signatures'. ENS Paris, 29th Oct. 2021. URL: https://hal.archives-ouvertes.fr/tel-03450109.

Reports & preprints

[20] M. Abdalla, M. Barbosa, J. Katz, J. Loss and J. Xu. *Algebraic Adversaries in the Universal Composability Framework*. IACR Cryptology ePrint Archive, Sept. 2021. URL: https://hal.inria.fr/hal-03442093.

[21] M. Abdalla, B. Haase and J. Hesse. *Security Analysis of CPace*. Report 2021/114. IACR Cryptology ePrint Archive, Jan. 2021. URL: https://hal.inria.fr/hal-03442101.

[22] H. Kim, O. Sanders, M. Abdalla and J. H. Park. *Practical Dynamic Group Signatures Without Knowledge Extractors*. Report 2021/351. IACR Cryptology ePrint Archive, Mar. 2021. URL: https://hal.inria.fr/hal-03442108.