RESEARCH CENTRE

Inria Paris Center

IN PARTNERSHIP WITH:

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

2022
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 PARIS II, Researcher, HDR]
- Jianwei Li [INRIA, Starting Research Position, from Feb 2022]
- Brice Minaud [INRIA, Researcher]
- Phong-Quang Nguyen [INRIA, Senior Researcher, HDR]

Post-Doctoral Fellow

- Thanh-Huyen Nguyen [Inria, until Nov 2022]

PhD Students

- Leonard Assouline [ENS PARIS]
- Henry Bambury [DGA, from Oct 2022]
- Hugo Beguinet [THALES, CIFRE]
- Nicolas Bon [CryptoExperts, CIFRE, from Oct 2022]
- Baptiste Cottier [WORLDLINE, CIFRE]
- Paola De Perthuis [COSMIAN, CIFRE]
- Guillaume Gette [DGA]
- Lénaïck Gouriou [Leanear, CIFRE]
- Paul Hermouet [SORBONNE UNIVERSITE]
- Guirec Lebrun [ANSSI, from Oct 2022]
- Ngoc Ky Nguyen [ENS PARIS]
- Michael Reichle [INRIA]
- Robert Schaedlich [ENS PARIS, from Oct 2022]
- Hugo Senet [THALES, CIFRE]
- Quoc Huy Vu [ENS PARIS]

Administrative Assistants

- Nathalie Gaudechoux [INRIA]
- Meriem Guemair [INRIA]

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. The first selection of standards was announced in July 2022. Out of four standards, three are based on lattice problems: CRYSTALS-KYBER for encryption, CRYSTALS-DILITHIUM and FALCON for signature. We intend to study the best lattice algorithms in order to assess the security of the three NIST standards (and two other NIST finalists SABER and NTRU) 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

- March 2022 – Michel Abdalla, Pierre-Alain Fouque, David Pointcheval: Password-Based Authenticated Key Exchange in the Three-Party Setting. Public Key Cryptography 2005: Test-of-Time Award at PKC 2022
- August 2022 – Brice Minaud, Michael Reichle: Dynamic Local Searchable Symmetric Encryption. CRYPTO (4) 2022: Paper invited for Journal of Cryptology
- December 2022 – Baptiste Cottier, David Pointcheval: Security Analysis of Improved EDHOC. FPS 2022: Best Paper Award

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 encryption schemes
- New primitives for efficient anonymous authentication
- Application of multi-party computation to machine learning
- Searchable Encryption
- Cryptanalysis

8 Bilateral contracts and grants with industry

8.1 Bilateral grants with industry

SecNISQ: Calcul Securisé Multipartite pour Architectures NISQ

Participants: Céline Chevalier, Quoc Huy Vu.

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

Participants: David Pointcheval, Ngoc Ky Nguyen.

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.

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

Participants: David Pointcheval, Paola De Perthuis.

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 European initiatives

9.1.1 H2020 projects

CryptAnalytics

Participants: David Pointcheval.

CryptAnalytics project on cordis.europa.eu

Title: Secure Analytics as Business Services

Duration: From April 1, 2021 to September 30, 2022

Partners:

- CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS (CNRS), France

Coordinator: 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.

PARQ

Participants: Phong Nguyen, Brice Minaud.

PARQ project on cordis.europa.eu

Title: Lattices in a Parallel and Quantum World

Duration: From July 1, 2020 to June 30, 2025

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS (CNRS), France

Coordinator: Phong Nguyen

Summary: Today's digital world creates many security and privacy issues. But cryptography, a pillar of cybersecurity, is facing two major challenges. The first challenge is the threat of quantum computers, fueled by massive investment worldwide. Shor showed that a quantum computer can break the most prevalent forms of public-key cryptography used every day by e-commerce and bitcoins. This threat is now taken seriously by governmental organizations: the NIST initiated in 2016 a process to standardize by 2024 public-key cryptographic algorithms resistant to quantum computers. The second challenge is new environments, such as big data, IoT, or crypto-currencies. Because classical cryptography no longer suffices for these applications, novel cryptographic schemes and functionalities have been developed, e.g. to allow anyone to compute with encrypted data. But these benefits come at the cost of security uncertainty: it requires more risky assumptions and makes it more difficult to select parameters with confidence. Worryingly, the past few years have seen several established cryptographic assumptions collapse. Lattices are mathematical objects which have emerged in the past twenty years as the key technique to respond to these challenges: the ongoing standardization of homomorphic encryption and the majority of the candidates to NIST's post-quantum standardization rely on the conjectured hardness of lattice problems. This proposal aims at readying lattice-based cryptography for real-world deployment, by protecting it against the most powerful adversaries, from ASIC farms to quantum computers. We will study the best parallel and quantum algorithms for lattice problems, and derive automated tools to select safe parameters. The proposal will use the renowned expertise of the PI in lattice algorithms and cryptanalysis to explore the quantum frontiers of cryptanalysis.

9.2 National initiatives

PEPR Cybersécurité SecureCompute: Sécurité des Calculs

Participants: David Pointcheval, Brice Minaud, Robert Schaedlich, Ngoc Ky Nguyen.

Program: ANR PEPR Cybersécurité

Duration: July 2022 – June 2028

Coordinator: PSL

Partners: ENS, Inria, CNRS, CEA

Coordinator: David Pointcheval

Summary: For cost reasons and the sake of simplification, companies massively outsource their data storage and data processing to untrusted providers. Many individuals do the same with their photos or other personal documents. Although these documents contain sensitive information, they are exposed on the web, and information leaks regularly break the news. Financial, economic, or medical data are at stake, with all the risks that this can bring, both to companies and to individuals. The purpose of this project is to study the cryptographic mechanisms allowing to ensure the security of data, during their transfer, at rest, but also during processing, despite uncontrolled environments such as the Internet for exchanges and the Cloud for hosting and processing. Security, in this context, not only means confidentiality but also integrity, a.k.a. the correct execution of operations. It is indeed essential, when outsourcing data and processing, that no sensitive information can leak but also that the results are correct. There are many areas of application, especially when large amounts of data are involved, such as medical analysis, logs, training data, etc.

SaFED: Safe and Functional Encrypted Databases

Participants: Brice Minaud, Michael Reichle.

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

Participants: Céline Chevalier, Quoc Huy Vu.

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

Participants: David Pointcheval, Brice Minaud.

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

10.2 Scientific events: selection

Program Committee Member

- AFRICACRYPT '22 (Fes, Maroc): Céline Chevalier
- CT-RSA '22 (San Francisco, California, USA): David Pointcheval, Brice Minaud
- ToSC/FSE '22 (Athens, Greece): Brice Minaud
- PKC '23 (Atlanta, Georgia, USA): David Pointcheval
- IEEE Information Theory Workshop '23 (Saint Malo, France): Phong Nguyen

10.2.1 Journal

Member of the editorial boards

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

10.2.2 Invited talks

- VIASM Annual Meeting 2022 (Hanoi – Vietnam). *Computations on Encrypted Data*: David Pointcheval
- AMUSEC 2022 – Forum Aix-Marseille de la Cybersécurité (CIRM – France). *Calculer sur des données distribuées privées et sensibles*: David Pointcheval
- ALMASTY team seminar (LIP6 - Paris). *Multi-Party PSM, Revisited - Improved Communication and Unbalanced Communication*: Léonard Assouline.
- ESL Seminar (Brown University - United States - online). *SSE and SSD: Page-Efficient Searchable Symmetric Encryption*: Michael Reichle.
- Seminar (NTT - Japan). *The NIST Post-Quantum Cryptography Standards*: Phong Nguyen.
- Real-World Crypto Day (Hanoi – Vietnam). *The NIST Post-Quantum Cryptography Standards*: Phong Nguyen.

10.3 Teaching - Supervision - Juries

10.3.1 Education

- Master: 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, Phong Nguyen, David Pointcheval, Introduction to Cryptology, L3/M1, ENS
- Summer School on Cryptography (Hanoi – Vietnam): David Pointcheval, Hash Proof Systems and Functional Encryption
- Summer School COGENT on Cohomology, Geometry and Explicit number theory (Grenoble – France): Phong Nguyen, Computational Aspects of Euclidean Lattices

10.3.2 PhD's in the Team

Defenses

- PhD: Théo Ryffel, Cryptography for Privacy-Preserving Machine Learning, ENS, June 23rd, 2022 (Supervisors: Francis Bach & David Pointcheval)

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: 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, 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

- PhD in progress: Hugo Senet, Anonymous Post-Quantum Cryptographic Protocols, from 2020, Céline Chevalier
- PhD in progress: Paul Hermouet, Etude de protocoles de cryptographie quantique, from 2020, Céline Chevalier
- PhD in progress: Hugo Beguinet, Chiffrement avancé post-quantique sur les réseaux euclidiens, from 2021, Céline Chevalier
- PhD in progress: Ngoc Ky Nguyen, Computations on encrypted data, from 2021, David Pointcheval
- PhD in progress: Henry Bambury, Cryptanalysis of algebraic lattices, from 2022, Phong Nguyen
- PhD in progress: Nicolas Bon, Design of optimized operations for homomorphic cryptography, from 2022, David Pointcheval
- PhD in progress: Robert Schaedlich, Computing on encrypted data, from 2022, David Pointcheval
- PhD in progress: Guirec Lebrun, Protocoles cryptographiques d'authentification post-quantique, from 2022, Céline Chevalier

10.3.3 Committees

- PhD Léo Robert. *Design and Analysis of Provably Secure Protocols: Applications to Messaging and Attestation* – Université Clermont Auvergne – France – September 22nd, 2022: David Pointcheval (Chair)
- PhD Benjamin Lipp. *Preuves mécanisées de protocoles cryptographiques et leur lien avec des implémentations vérifiées* – Ecole Normale Supérieure – France – June 28th, 2022: David Pointcheval (Chair)
- PhD Théo Ryffel. *Cryptography for Privacy-Preserving Machine Learning* – Ecole Normale Supérieure – France – June 23rd, 2022: David Pointcheval (Co-supervisor)
- PhD Agnese Gini. *ON THE HARDNESS OF THE HIDDEN SUBSET SUM PROBLEM: ALGEBRAIC AND STATISTICAL ATTACKS* – Université du Luxembourg – Luxembourg – July 7th, 2022: Phong Nguyen (Member)
- PhD Étienne Marcatel. *Contribution à la Cryptographie Post-Quantique* – Université Grenoble Alpes – France – October 11th, 2022: Phong Nguyen (Reviewer)
- HDR Matthieu Rivain. *On the Provable Security of Cryptographic Implementations* – Ecole Normale Supérieure – France – June 21st, 2022: David Pointcheval.
- HDR Cristina Onete. *On the Security of Modern-Day Secure- Channel Establishment* – Université de Limoges – France – March 23rd, 2022: David Pointcheval
- PhD Neals Fournaise. *Protocoles cryptographiques pour le respect de la vie privée* – Université de Limoges – France – January 4th, 2022: Céline Chevalier

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. Music, C. Chevalier and E. Kashefi. 'Dispelling myths on superposition attacks: formal security model and attack analyses'. In: *Designs, Codes and Cryptography* 90.4 (Apr. 2022), pp. 881–920. DOI: 10.1007/s10623-022-01017-3. URL: https://hal.inria.fr/hal-03943311.

International peer-reviewed conferences

[11] S. Bettaieb, L. Bidoux, O. Blazy, B. Cottier and D. Pointcheval. 'Post-Quantum and UC-secure Oblivious Transfer from SPHF with Grey Zone'. In: *15th International Symposium on Foundations & Practice of Security (FPS–2022)*. 15th International Symposium on Foundations & Practice of Security (FPS – 2022). Ottawa, Canada, 12th Dec. 2022. URL: https://hal.science/hal-03772089.

[12] C. Chevalier, E. Ebrahimi and Q.-H. Vu. 'On Security Notions for Encryption in a Quantum World'. In: *Progress in Cryptology – INDOCRYPT 2022*. INDOCRYPT 2022 - 23rd International Conference on Cryptology in India. Vol. 13774. Lecture Notes in Computer Science. Kolkata, India: Springer International Publishing, 1st Jan. 2022, pp. 592–613. DOI: 10.1007/978-3-031-22912-1_26. URL: https://hal.inria.fr/hal-03943268.

[13] B. Cottier and D. Pointcheval. 'Security Analysis of Improved EDHOC Protocol'. In: 15th International Symposium on Foundations & Practice of Security (FPS – 2022). Ottawa, Canada, 12th Dec. 2022. URL: https://hal.science/hal-03772082.

[14] G. Couteau, D. Goudarzi, M. Klooß and M. Reichle. 'Sharp: Short Relaxed Range Proofs'. In: CCS '22: 2022 ACM SIGSAC Conference on Computer and Communications Security. Los Angeles CA USA, United States: ACM, 7th Nov. 2022, pp. 609–622. DOI: 10.1145/3548606.3560628. URL: https://hal.archives-ouvertes.fr/hal-03860720.

[15] C. Delerablée, L. Gouriou and D. Pointcheval. 'Key-Policy ABE With Switchable Attributes'. In: SCN 2022 - Security and Cryptography for Networks: 13th International Conference. Vol. 13409. LNCS - Lecture Notes in Computer Science. Amalfi, Italy: Springer, 12th Sept. 2022. DOI: 10.1007/978-3-031-14791-3_7. URL: https://hal.archives-ouvertes.fr/hal-03794260.

[16] C. Hébant and D. Pointcheval. 'Traceable Constant-Size Multi-authority Credentials'. In: SCN 2022 - 13th conference on security and cryptography for networks. Vol. 13409. Lecture Notes in Computer Science. Amalfi, Italy: Springer International Publishing, 5th Sept. 2022, pp. 411–434. DOI: 10.1007/978-3-031-14791-3_18. URL: https://hal.science/hal-03816213.

[17] M. Izabachène, A. Nitulescu, P. de Perthuis and D. Pointcheval. 'MyOPE: Malicious SecuritY for Oblivious Polynomial Evaluation'. In: *Lecture Notes in Computer Science*. SCN 2022 - 13th Conference on Cryptography and Security for Networks. Vol. 13409. Security and Cryptography for Networks 13th International Conference, SCN 2022, Amalfi (SA), Italy, September 12–14, 2022, Proceedings. Amalfi, Italy: Springer, 2022, pp. 663–686. DOI: 10.1007/978-3-031-14791-3_29. URL: https://hal.archives-ouvertes.fr/hal-03820565.

[18] B. Libert, K. Nguyen and A. Passelègue. 'Cumulatively All-Lossy-But-One Trapdoor Functions from Standard Assumptions'. In: SCN 2022 - Proceedings of the 13th Conference on Security in Communication Networks. Amalfi, Italy, 12th Sept. 2022. URL: https://hal.inria.fr/hal-03820072.

[19] B. Minaud and M. Reichle. 'Dynamic Local Searchable Symmetric Encryption'. In: Crypto 2022 - 42nd Annual International Cryptology Conference. Vol. LNCS - 13510. Advances in Cryptology – CRYPTO 2022. Santa Barbara, United States: Springer, 15th Aug. 2022. DOI: 10.1007/978-3-031-15985-5_4. URL: https://hal.archives-ouvertes.fr/hal-03863896.

[20] K. Nguyen, D. H. Phan and D. Pointcheval. 'Multi-Client Functional Encryption with Fine-Grained Access Control'. In: Asiacrypt 2022 - 28th Annual International Conference on the Theory and Application of Cryptology and Information Security. Advances in Cryptology - Proceedings of ASIACRYPT '22. Taipei, Taiwan, 5th Dec. 2022. URL: https://hal.inria.fr/hal-03910053.

[21] P. de Perthuis and D. Pointcheval. 'Two-Client Inner-Product Functional Encryption with an Application to Money-Laundering Detection'. In: ACM CCS- Computer and Communications Security 2022. Los Angeles, United States, 7th Nov. 2022. URL: https://hal.archives-ouvertes.fr/hal-03830846.

[22] D. Rausch, R. Küsters and C. Chevalier. 'Embedding the UC Model into the IITM Model'. In: *Advances in Cryptology – EUROCRYPT 2022*. EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 13276. Lecture Notes in Computer Science. Trondheim, Norway: Springer International Publishing, 25th May 2022, pp. 242–272. DOI: 10.1007/978-3-031-07085-3_9. URL: https://hal.inria.fr/hal-03943297.

Reports & preprints

[23] T. Ryffel, F. Bach and D. Pointcheval. *Differential Privacy Guarantees for Stochastic Gradient Langevin Dynamics*. 5th Feb. 2022. URL: https://hal.inria.fr/hal-03547726.