RESEARCH CENTRE

Inria Paris Centre

IN PARTNERSHIP WITH:

CNRS, Ecole normale supérieure de Paris

2024

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team CASCADE

Creation of the Project-Team: 2020 October 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

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

- Phong Nguyen [Team leader, INRIA, Senior Researcher, from Jun 2024]
- David Pointcheval [Team leader, CNRS, Senior Researcher, until May 2024]
- Francesco Arzani [INRIA, Advanced Research Position, QAT AEx Team]
- Ulysse Chabaud [INRIA, Researcher, QAT AEx Team]
- Claude Crepeau [INRIA, Senior Researcher, from May 2024 until Jul 2024]
- Jianwei Li [INRIA, Starting Research Position]
- Brice Minaud [INRIA, Researcher]
- Phong Nguyen [INRIA, Senior Researcher, until May 2024]
- Harold Ollivier [INRIA, Senior Researcher, until Apr 2024, QAT AEx Team]
- David Pointcheval [CNRS, Senior Researcher, from Jun 2024]
- Mathys Rennela [INRIA, Starting Research Position, until Aug 2024, QAT AEx Team]

Faculty Member

- Céline Chevalier [UNIV PARIS II, Associate Professor, Conventionnée ENS Paris, HDR]

Post-Doctoral Fellows

- Jack Davis [INRIA, Post-Doctoral Fellow, QAT AEx Team]
- Wissam Ghantous [INRIA, Post-Doctoral Fellow, until Aug 2024]
- Jules Maire [INRIA, Post-Doctoral Fellow, from Nov 2024]
- Florette Martinez [ENS Paris, Post-Doctoral Fellow, until Aug 2024]
- Amit Saha [INRIA, Post-Doctoral Fellow, from Mar 2024, QAT AEx Team]
- Zacharie Van Herstraeten [INRIA, Post-Doctoral Fellow, from Feb 2024, QAT AEx Team]

PhD Students

- Sami Abdul Sater [INRIA, QAT AEx Team]
- Henry Bambury [DGA]
- Hugo Beguinet [THALES, until Oct 2024]
- Nicolas Bon [CRYPTOEXPERTS]
- Sacha Cerf [DI-ENS, from Oct 2024, QAT AEx Team]
- Sharon David [INRIA, from Oct 2024]
- Paola De Perthuis [COSMIAN, until Aug 2024]
- Cedric Geissert [INRIA, from Nov 2024]
- Paul Hermouet [SORBONNE UNIVERSITE, until Oct 2024]

- Guirec Lebrun [ANSSI]
- Ngoc Nguyen [ENS PARIS, until Sep 2024]
- Rajarsi Pal [INRIA, QAT AEx Team]
- Robert Schadlich [ENS PARIS]
- Hugo Thomas [Quandela, from Mar 2024, QAT AEx Team]
- Varun Upreti [INRIA, from Oct 2024, QAT AEx Team]

Technical Staff

- Sacha Bernheim [INRIA, Engineer, from Oct 2024, QAT AEx Team]
- Maxime Garnier [INRIA, Engineer, from Oct 2024, QAT AEx Team]
- Benjamin Guichard [INRIA, Engineer, from Nov 2024, QAT AEx Team]

Interns and Apprentices

- Sacha Bernheim [INRIA, Intern, from Mar 2024 until Aug 2024, QAT AEx Team]
- Sacha Cerf [INRIA, Intern, from Apr 2024 until Sep 2024, QAT AEx Team]
- Sharon David [INRIA, from Apr 2024 until Sep 2024, QAT AEx Team]
- Cedric Geissert [INRIA, Intern, from Apr 2024 until Sep 2024]
- Benjamin Guichard [INRIA, Intern, from Mar 2024 until Aug 2024, QAT AEx Team]
- Cong Ha Nguyen [INRIA, Intern, from Mar 2024 until Aug 2024]
- Varun Upreti [INRIA, Intern, from May 2024 until Jul 2024, QAT AEx Team]

Administrative Assistants

- Meriem Guemair [INRIA]
- Diana Marino Duarte [INRIA]

External Collaborator

- Claude Crepeau [UNIV MCGILL, from Aug 2024]

2 Overall objectives

2.1 Presentation

Cryptographic algorithms are the equivalent of locks, seals, and identification documents over the Internet. They are essential to protect our online bank transactions, medical and personal information, and to support e-commerce and e-government. These algorithms come in various forms. Encryption algorithms protect sensitive data from unauthorized access. Digital signature algorithms—often used in combination with hash functions—and message authentication codes (MACs) serve as digital replacements for handwritten signatures in electronic transactions. Identification protocols enable the secure verification of a remote party's identity. As a whole, cryptology is a research area with a high strategic impact in industry, for individuals, and for society. The research activities of the CASCADE project-team address the following topics, which cover most of the areas currently active in the international cryptographic community, with a focus on public-key algorithms:

1. Algorithm and protocol design, with provable security;
2. Theoretical and practical attacks.

2.2 Design of Provably Secure Primitives and Protocols

Since the advent of public-key cryptography, marked by the seminal Diffie–Hellman paper, many algorithmic problems suitable for cryptographic use have been proposed, and numerous cryptographic schemes have been designed—often accompanied by more or less heuristic proofs of their security, based on the assumed intractability of the underlying problems. However, many of these schemes have subsequently been broken. The mere fact that a cryptographic algorithm has withstood cryptanalytic attacks for several years is often taken as a kind of validation, but it may take a long time before a scheme is broken. As a result, the absence of known attacks at a given time should never be considered a full validation of a scheme's security.

A fundamentally different approach is offered by the concept of provable security. A significant line of research has aimed to provide formal proofs within the framework of computational complexity theory (also known as reductionist security proofs). These proofs reduce the task of breaking a cryptographic protocol to solving a well-studied hard problem (e.g., factoring, RSA, or the discrete logarithm problem).

Initially, researchers focused on defining the security notions required by practical cryptographic schemes, and then designing protocols that satisfied these notions. The techniques were derived directly from complexity theory, relying on polynomial-time reductions. However, this line of work was primarily theoretical in nature. The goal was to minimize the assumptions needed on cryptographic primitives (e.g., one-way functions, permutations, possibly with trapdoors), without regard to practical efficiency. Thus, it was sufficient to design a scheme with polynomial-time algorithms and to present polynomial reductions from the hardness of the underlying problem to an attack on the security notion, in an asymptotic sense. However, such results have limited practical impact on real-world security.

Over time, the community has sought more efficient, quantitatively meaningful reductions—an approach known as exact or concrete security—which aims to produce security guarantees that are not only theoretically sound but also practically relevant, with concrete efficiency parameters.

To this aim, 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, for concrete parameters;

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.

2.3 Attacks and security analysis

But, some schemes are still published without complete security proofs, hence their security requires further analysis, and attacks may be found. And even for provably secure schemes, attacks are not excluded, and may appear at several levels:

- A **computational assumption** may prove wrong. So we study them, and in particular the ones that are believed to resist quantum computers.
- the **security model** may be inappropriate, and allow for devastating attacks in concrete usage scenarios.

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 Computations on encrypted data

In the area of computations on encrypted data, there are three main families of approaches:

Advanced Encryption, with fully homomorphic encryption and functional encryption:

- *Fully Homomorphic Encryption* (FHE), which has been announced in 2009, allows to perform any computation on encrypted data, getting the result encrypted under the same key. This is perfect in order to outsource computation in the Cloud, on encrypted data: the Cloud provider does not learn any information;
- *Functional Encryption* (FE), proposed in 2011, allows an authority to deliver functional decryption keys, for any function f of his choice, so that on the encryption of any message m, the functional decryption key leads to $f(m)$. This is a generalization of Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE) and Predicate Encryption (PE), which where limited to the identity function, under some access-control.

Secure Multi-Party Computation (SMPC) is an interactive protocol between 2 or more parties, with their own private inputs. After several communications, this is possible to let each party to learn specific evaluations on the inputs, and nothing else.

Searchable Symmetric Encryption (SSE) proposes a trade-off between efficiency and security, using fast (structured) symmetric encryption, but allowing some leakage of information. The goal is akin to private information retrieval: one can retrieve records in a database without leaking much information about the query.

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

The publication [13] provided the first rigorous dynamical analysis of the actual BKZ lattice reduction algorithm, widely used in cryptanalysis.

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):

- Cryptanalysis (Analysis of the BKZ algorithm [13], NTRU and hypercubic lattices [17], and Signature based on quadratic forms [18])
- Functional encryption ([15])
- Post-quantum cryptography (Variant of Dilithium signature [16], , Hybrid KEM [21])
- Protocols (Signal Protocol[19], MLS [22], key agreement for MLS [23], Electronic Voting [27])
- Advanced signatures (Attribute-based signatures [24], Blind signatures [25])
- Number theory (Mertens conjecture [26])
- Advanced encryption (Attribute-Based and Predicate Encryption [28])
- Zero-knowledge proofs (Commitments [20], Zero-knowledge arguments [14])

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

PhD CIFRE Cosmian – Paola de Perthuis (2020–2024) – *Efficient Protocols for Secure Computation over Confidential Data*

PhD CIFRE Thales – Hugo Beguinet (2021–2024) – *Chiffrement avancé post-quantique sur les réseaux euclidiens*

PhD CIFRE CryptoExperts – Nicolas Bon (2022–2025) – *Design of optimized operations for homomorphic cryptography*

PhD ANSSI – Guirec Lebrun (2022–2025) – *Protocoles cryptographiques d'authentification post-quantique*

PhD Thales – Éric Sageloli (2023–2026) – *Sécurité de protocoles et primitives cryptographiques face à un attaquant quantique*

8.2 Grants with industry

RESQUE: Résilience Quantique

Participants: Céline Chevalier, Eric Sageloli.

Program: BPI

Duration: September 2023 – August 2026

Coordinator: Thales

Partners: CryptoExperts, CryptoNext, TheGreenBow, ANSSI, CNES, Inria

Inria contact: Céline Chevalier

Summary: RESQUE aims at developing cryptographic tools that will resist quantum computers.

SecNISQ: Calcul Securisé Multipartite pour Architectures NISQ

Participants: Céline Chevalier, Paul Hermouet.

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.

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.

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.

9 Partnerships and cooperations

9.1 International research visitors

9.1.1 Visits of international scientists

Inria International Chair

Participants: Claude Crépeau.

9.2 European initiatives

9.2.1 H2020 projects

PARQ 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

Inria contact: Phong Nguyen

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.

9.3 National initiatives

QAT: Quantum computing Architectures, Algorithms, Applications and their Theory

Participants: Sami Abdul Sater, Francesco Arzani, Ulysse Chabaud, Jack Davis, Harold Ollivier, Rajarsi Pal, Mathys Rennela.

Program: Exploratory Action Inria

Duration: January 2023 – December 2024

Inria contact: Harold Ollivier

Summary: Our research group believes that the development of Quantum Information Processing requires a holistic approach that integrates architectures, algorithms, and applications. We recognize that applications are crucial for end-users, but they cannot be achieved without the necessary enablers, which are algorithms and architectures. Moreover, the practical impact of this technology on current and future hardware depends on a constant interplay between these three topics, especially given the limited hardware resources available.

To this end, our research program is focused on developing advanced theoretical tools that can help us understand the capabilities of quantum computers, improve their design for specific algorithms, and unlock new functionalities using quantum information processing. By taking this integrated approach, we hope to advance the state-of-the-art in Quantum Information Processing and provide valuable insights for future developments.

HQI: Hybrid HPC Quantum Initiative

Participants: Céline Chevalier, Quoc Huy Vu.

Program: ANR PEPR Quantique

Duration: April 2022 – April 2028

Coordinator: CEA

Partners: CEA, CNRS, CPU, GENCI, Inria

Inria contact: Céline Chevalier

Summary: Following the announcement made in January 2021 of the National Quantum Strategy by the President of the French Republic, the SGPI entrusted the CEA, GENCI and Inria with the responsibility of setting up a national hybrid HPC quantum-computing platform named HQI. The project to set up this platform consists of purchases of quantum computers (entrusted to GENCI and subject to a separate agreement), research and development entrusted to industrialists and academics as well as support for communities using the platform (objects of this agreement).

SecureCompute: Security of Computations

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

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.

10 Dissemination

10.1 Promoting scientific activities

10.1.1 Scientific events: selection

Member of the conference program committees

- Africacrypt ’24 (Céline Chevalier)

- Crypto ’24 (Phong Nguyen)
- PKC ’24 (David Pointcheval)
- SCN ’24 (Phong Nguyen, David Pointcheval)’

Reviewer

- Eurocrypt ’24 (Phong Nguyen)
- ANTS ’24 (Phong Nguyen)

10.1.2 Journal

Member of the editorial boards

- Journal of Applicable Algebra in Engineering, Communication and Computing (AAECC): David Pointcheval (Associate Editor)
- Journal of Mathematical Cryptology: Phong Nguyen (Associate Editor)
- Journal of Cryptology / Topical Collection on Computing on Encrypted Data: David Pointcheval

10.1.3 Invited talks

- 25th Workshop on Elliptic Curve Cryptography (ECC): Phong Nguyen.
- Talk on Multivariate Cryptography at the 2024 summer school on post-quantum cryptography (PEPR PQ-TLS): Brice Minaud.
- Talk on Encrypted Databases at the 2024 winter school organized by PEPR Cybersecurity : Brice Minaud.

10.2 Teaching - Supervision - Juries

- Introduction to Cryptology (ENS 1st year students): a total of 20 hours of lecture, 20 hours of TA/year
- Techniques in cryptography and cryptanalysis (Master M2 MPRI): 24 hours of lecture/year
- Cryptographic protocols: computational and symbolic proofs (Master M2 MPRI): 12 hours of lecture/year
- Introduction to Cryptography (Master M1, ESI Léonard de Vinci)
- Cryptography (Master MSSIS, ESIEA)
- Joint directorship of MPRI (M2, PSL/IPP/UPC/UPS).
- Examinator for entrance exams to ENS (oral exam in Fundamental Computer Science).

10.3 Popularization

10.3.1 Productions (articles, videos, podcasts, serious games, ...)

- Podcast [31]

10.3.2 Participation in Live events

- Podcast [31]

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] D. Aggarwal, J. Li, P. Q. Nguyen and N. Stephens-Davidowitz. 'Slide Reduction, Revisited—Filling the Gaps in SVP Approximation'. In: CRYPTO 2020 - 40th Annual International Cryptology Conference. Santa Barbara / Virtual, United States, 10th Aug. 2020, pp. 274–295. DOI: 10.1007/978-3-030-56880-1_10. URL: https://inria.hal.science/hal-03068203.

[4] 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.

[5] 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.

[6] J. Chotard, E. Dufour Sans, R. Gay, D. Pointcheval and D. H. Phan. 'Decentralized Multi-Client Functional Encryption for Inner Product'. In: ASIACRYPT '18 - 24th Annual International Conference on the Theory and Application of Cryptology and Information Security. Vol. Lecture Notes in Computer Science. Advances in Cryptology - ASIACRYPT '18 11273. Brisbane, Australia: Springer, Dec. 2018. DOI: 10.1007/978-3-030-03329-3_24. URL: https://hal.science/hal-01668020.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.science/hal-03863896.

[12] 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

[13] J. Li and P. Q. Nguyen. 'A Complete Analysis of the BKZ Lattice Reduction Algorithm'. In: *Journal of Cryptology* (2024). URL: https://hal.science/hal-04728596. In press (cit. on p. 8).

[14] J. Maire and D. Vergnaud. 'Compact zero-knowledge arguments for Blum integers'. In: *Theoretical Computer Science* 1038 (22nd May 2025), p. 115155. DOI: 10.1016/j.tcs.2025.115155. URL: https://hal.science/hal-04987985 (cit. on p. 8).

[15] K. Nguyen, D. Pointcheval and R. Schädlich. 'Decentralized Multi-Client Functional Encryption with Strong Security'. In: *IACR Communications in Cryptology* 1.2 (8th July 2024). DOI: 10.62056/andkp2fgx. URL: https://hal.science/hal-05029125 (cit. on p. 8).

International peer-reviewed conferences

[16] H. Bambury, H. Beguinet, T. Ricosset and E. Sageloli. 'Polytopes in the Fiat-Shamir with Aborts Paradigm'. In: Advances in Cryptology – CRYPTO 2024. Vol. 14920. Lecture Notes in Computer Science. Santa Barbara, United States, 16th Aug. 2024, pp. 339–372. DOI: 10.1007/978-3-031-68376-3_11. URL: https://hal.science/hal-04688010 (cit. on p. 8).

[17] H. Bambury and P. Q. Nguyen. 'Improved Provable Reduction of NTRU and Hypercubic Lattices'. In: PQCrypto 2024 - 15th International Workshop Post-Quantum Cryptography. Vol. LNCS-14771. Lecture Notes in Computer Science. Oxford (UK), United Kingdom: Springer Nature Switzerland, 11th June 2024, pp. 343–370. DOI: 10.1007/978-3-031-62743-9_12. URL: https://hal.science/hal-05016862 (cit. on p. 8).

[18] H. Bambury and P. Q. Nguyen. 'Cryptanalysis of an Efficient Signature Based on Isotropic Quadratic Forms'. In: *Lecture Notes in Computer ScienceI*. 16th International Workshop on Post-Quantum Cryptography (PQCrypto 2025). Vol. 15578. Post-Quantum Cryptography 16th International Workshop, PQCrypto 2025, Taipei, Taiwan, April 8–10, 2025, Proceedings, Part II Conference proceedings. Taipei, Taiwan: Springer Nature Switzerland, 2025, pp. 153–175. DOI: 10.1007/978-3-031-86602-9_6. URL: https://hal.science/hal-05016873 (cit. on p. 8).

[19] H. Beguinet, C. Chevalier, T. Ricosset and H. Senet. 'Formal Verification of a Post-Quantum Signal Protocol with Tamarin'. In: *LNCS*. VECOS 2023 - 16th International Conference on Verification and Evaluation of Computer and Communication Systems. Vol. 14368. Lecture Notes in Computer Science. Marrakech, Morocco: Springer Nature Switzerland, 19th Dec. 2024, pp. 105–121. DOI: 10.1007/978-3-031-49737-7_8. URL: https://hal.science/hal-04361766 (cit. on p. 8).

[20] X. Bultel, C. Chevalier, C. Jojon, D. Liu and B. Nguyen. 'Cryptographic Commitments on Anonymizable Data'. In: EuroS&P 2025 - 10th IEEE European Symposium on Security and Privacy. Venice, Italy, 30th June 2025. URL: https://hal.science/hal-05027266 (cit. on p. 8).

[21] C. Chevalier, G. Lebrun and A. Martinelli. 'Spilling-Cascade: an Optimal PKE Combiner for KEM Hybridization'. In: 23rd International Conference on Applied Cryptography and Network Security (ACNS'25). Munich, Germany, 23rd June 2025. URL: https://hal.science/hal-05027882 (cit. on p. 8).

[22] C. Chevalier, G. Lebrun, A. Martinelli and J. Plût. 'The Art of Bonsai: How Well-Shaped Trees Improve the Communication Cost of MLS'. In: 10th IEEE European Symposium on Security and Privacy (EuroS&P 2025). Venise, Italy, 30th June 2025. URL: https://hal.science/hal-05031107 (cit. on p. 8).

[23] C. Chevalier, G. Lebrun, A. Martinelli and A. R. Taleb. 'Quarantined-TreeKEM: A Continuous Group Key Agreement for MLS, Secure in Presence of Inactive Users'. In: The 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24). Salt Lake City (UT), United States, 18th Oct. 2024, pp. 2400–2414. DOI: 10.1145/3658644.3690265. URL: https://hal.science/hal-05026639 (cit. on p. 8).

[24] C. Delerablée, L. Gouriou and D. Pointcheval. 'Attribute-Based Signatures with Advanced Delegation, and Tracing'. In: CT-RSA 2024 - Cryptographers' Track at RSA Conference. Vol. Lecture Notes in Computer Science. Lecture Notes in Computer Science 14643. San Francisco California, United States: Springer Nature Switzerland, 6th May 2024, pp. 224–248. DOI: 10.1007/978-3-031-58868-6_9. URL: https://hal.science/hal-05029256 (cit. on p. 8).

[25] J. Kastner, K. Nguyen and M. Reichle. 'Pairing-Free Blind Signatures from Standard Assumptions in the ROM'. In: *CRYPTO 2024*. IACR CRYPTO 2024 - 44th Annual International Cryptology Conference. Vol. 14920. Lecture Notes in Computer Science. Santa barbara, United States: Springer Nature Switzerland, 16th Aug. 2024, pp. 210–245. DOI: 10.1007/978-3-031-68376-3_7. URL: https://hal.science/hal-05029146 (cit. on p. 8).

[26] S. Kim and P. Q. Nguyen. ‘On counterexamples to the Mertens conjecture’. In: *Research in Number Theory*. Sixteenth Algorithmic Number Theory Symposium (ANTS XVI). Vol. 11. 1. Cambridge (MA), United States, 4th Dec. 2024, p. 3. DOI: 10.1007/s40993-024-00603-9. URL: https://hal.science/hal-05016898 (cit. on p. 8).

[27] D. Pointcheval. ‘Efficient Universally-Verifiable Electronic Voting with Everlasting Privacy’. In: SCN 2024 - The 14th Conference on Security in Communication Networks. Vol. Lecture Notes in Computer Science. Lecture Notes in Computer Science 14973. Amalfi, Italy: Springer Nature Switzerland, 10th Sept. 2024, pp. 323–344. DOI: 10.1007/978-3-031-71070-4_15. URL: https://hal.science/hal-05029286 (cit. on p. 8).

Conferences without proceedings

[28] D. Pointcheval and R. Schädlich. ‘Multi-client Attribute-Based and Predicate Encryption from Standard Assumptions’. In: TCC 2024 - 22nd Theory of Cryptography Conference. Vol. Lecture Notes in Computer Science. Lecture Notes in Computer Science 15366. Milan, Italy: Springer Nature Switzerland, 30th Nov. 2025, pp. 31–64. DOI: 10.1007/978-3-031-78020-2_2. URL: https://hal.science/hal-05029340 (cit. on p. 8).

Reports & preprints

[29] F. Arzani, R. I. Booth and U. Chabaud. *Can effective descriptions of bosonic systems be considered complete?* 2025. DOI: 10.48550/arXiv.2501.13857. URL: https://hal.science/hal-04990688.

[30] J. Davis, N. Fabre and U. Chabaud. *Identifying quantum resources in encoded computations*. 29th July 2024. DOI: 10.48550/arXiv.2407.18394. URL: https://hal.science/hal-04990702.

Scientific popularization

[31] B. Minaud. ‘Quel est le prix à payer pour la sécurité de nos données ? [podcast]’. In: *Interstices* (13th Sept. 2024). DOI: 10.60527/r6pb-q242. URL: https://inria.hal.science/hal-04698367 (cit. on p. 13).