

2025 Activity Report

RESEARCH CENTRE: Inria Paris Centre

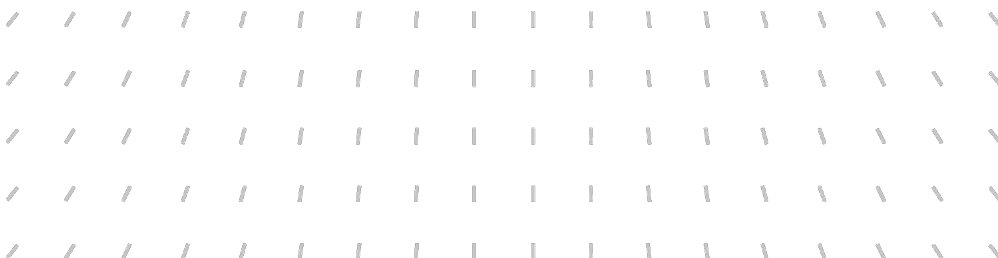
IN PARTNERSHIP WITH: CNRS, Ecole normale supérieure de Paris

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



Project-Team CASCADE

Creation of the Project-Team: 2020 October 01

Each year, Inria research teams publish an Activity Report presenting their work and results over the reporting period. These reports follow a common structure, with some optional sections depending on the specific team. They typically begin by outlining the overall objectives and research programme, including the main research themes, goals, and methodological approaches. They also describe the application domains targeted by the team, highlighting the scientific or societal contexts in which their work is situated. The reports then present the highlights of the year, covering major scientific achievements, software developments, or teaching contributions. When relevant, they include sections on software, platforms, and open data, detailing the tools developed and how they are shared. A substantial part is dedicated to new results, where scientific contributions are described in detail, often with subsections specifying participants and associated keywords. Finally, the Activity Report addresses funding, contracts, partnerships, and collaborations at various levels, from industrial agreements to international cooperations. It also covers dissemination and teaching activities, such as participation in scientific events, outreach, and supervision. The document concludes with a presentation of scientific production, including major publications and those produced during the year.

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

Contents

Project-Team CASCADE	1
1 Team members, visitors, external collaborators	5
2 Overall objectives	6
2.1 Presentation	6
2.2 Design of Provably Secure Primitives and Protocols	7
2.3 Attacks and security analysis	7
3 Research program	7
3.1 Quantum-safe cryptography	7
3.2 Computations on encrypted data	8
4 Application domains	8
4.1 Privacy for the Cloud	8
4.2 Searchable Encryption	9
4.3 Post-Quantum Standardization	10
4.4 Provable Security for the Quantum Internet	10
5 Social and environmental responsibility	10
5.1 Footprint of research activities	10
5.2 Impact of research results	10
6 Highlights of the year	10
7 Latest software developments, platforms, open data	11
7.1 Latest software developments	11
7.2 New platforms	11
7.3 Open data	11
8 New results	11
9 Bilateral contracts and grants with industry	11
9.1 Bilateral contracts with industry	11
9.2 Grants with industry	11
10 Partnerships and cooperations	12
10.1 International initiatives	12
10.1.1 Visits of international scientists	12
10.2 European initiatives	12
10.2.1 H2020 projects	12
10.3 National initiatives	13
11 Dissemination	14
11.1 Promoting scientific activities	14
11.1.1 Scientific events: organisation	14
11.1.2 Scientific events: selection	14
11.1.3 Journal	15
11.1.4 Invited talks	15
11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach	15
11.2.1 Supervision	15
11.2.2 Juries	15
11.3 Popularization	15
11.3.1 Participation in Live events	15

12 Scientific production	16
12.1 Major publications	16
12.2 Publications of the year	16

1 Team members, visitors, external collaborators

Research Scientists

- Phong-Quang Nguyen [Team leader, INRIA, Senior Researcher, HDR]
- Francesco Arzani [INRIA, Advanced Research Position]
- Ulysse Chabaud [INRIA, Researcher]
- Céline Chevalier [UNIV PARIS II, Researcher, HDR]
- Claude Crepeau [UNIV MCGILL, Senior Researcher, from Sep 2025 until Nov 2025]
- Claude Crepeau [UNIV MCGILL, Senior Researcher, from Jun 2025 until Aug 2025]
- Jonas Landman [INRIA, ISFP, from Oct 2025]
- Brice Minaud [INRIA, Researcher]

Post-Doctoral Fellows

- Jack Davis [INRIA, Post-Doctoral Fellow]
- Jules Maire [INRIA, Post-Doctoral Fellow]
- Florette Martinez [ENS Paris, Post-Doctoral Fellow, until Oct 2025]
- Amit Saha [INRIA, Post-Doctoral Fellow]
- Zacharie Van Herstraeten [INRIA, Post-Doctoral Fellow]

PhD Students

- Sami Abdul Sater [INRIA]
- Henry Bambury [DGA, until Sep 2025]
- Nicolas Bon [CRYPTOEXPERTS, until Oct 2025]
- Alexandre Camelin [INRIA, from Sep 2025]
- Sacha Cerf [DI-ENS, ATER]
- Luca Francesco D'Alessandro [INRIA, from Oct 2025]
- Luca Francesco D'Alessandro [INRIA, from Jun 2025 until Sep 2025]
- Sharon David [INRIA]
- Cedric Geissert [INRIA]
- Laurent Holin [ENS PARIS]
- Guirec Lebrun [ANSSI, until Sep 2025]
- Rajarsi Pal [INRIA]
- Robert Schadlich [ENS PARIS, until Sep 2025]
- Hugo Thomas [Quandela]
- Florian Tousnakhoff [ENS PARIS, from Oct 2025]
- Varun Upreti [INRIA]
- Bo Yang [INRIA, from Aug 2025]

Technical Staff

- Maxime Garnier [INRIA, Engineer]
- Emlyn Graham [INRIA, Engineer, from Oct 2025]
- Benjamin Guichard [INRIA, Engineer, until Apr 2025]
- Pranav Gopinadhan Nair [INRIA, Engineer, from Nov 2025]
- Mateo Uldemolins Nivelá [INRIA, Engineer, from Jun 2025]

Interns and Apprentices

- Alexandre Camelin [INRIA, Intern, from Apr 2025 until Aug 2025]
- Florian Cottier [INRIA, Intern, from Oct 2025]
- Florian Cottier [INRIA, Intern, from Mar 2025 until Jul 2025]
- Martina Leonetti [INRIA, Intern, from Feb 2025 until Jul 2025]
- Giacomo Spriano [INRIA, Intern, from Mar 2025 until Jul 2025]

Administrative Assistants

- Diana Marino Duarte [INRIA]
- Abigail Palma [INRIA]

Visiting Scientist

- Claude Crepeau [UNIV MCGILL, from Nov 2025]

External Collaborator

- Claude Crepeau [UNIV MCGILL, until Jun 2025]

2 Overall objectives

2.1 Presentation

Cryptographic algorithms play the role of locks, seals, and identity documents on the Internet. They are fundamental to securing online banking, protecting medical and personal data, and enabling trusted e-commerce and e-government services.

These algorithms serve different but complementary purposes. Encryption safeguards sensitive information against unauthorized access. Digital signature schemes — often combined with hash functions — and message authentication codes (MACs) provide the electronic equivalent of handwritten signatures, ensuring integrity and authenticity in digital transactions. Identification protocols allow parties to verify each other's identity securely, even at a distance.

Taken together, cryptology is a field of research with major strategic importance for industry, individuals, and society as a whole.

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 were 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 accommodate 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, although 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 the first four standards, three are based on lattice problems: CRYSTALS-KYBER for encryption, CRYSTALS-DILITHIUM and FALCON for signature. We 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

There is no highlight.

7 Latest software developments, platforms, open data

7.1 Latest software developments

7.2 New platforms

Participants: Not Applicable.

Not applicable.

7.3 Open data

Participants: Henry Bambury, Nicolas Bon, Alexandre Camelin, Céline Chevalier, Guirec Lebrun, Jules Maire, Brice Minaud, Phong Nguyen, David Pointcheval, Robert Schadlich

8 New results

- Functional encryption [22]
- Cryptanalysis: [17]
- Protocols [21, 20]
- Advanced encryption [23]
- Zero-knowledge proofs [15, 19]
- Security proofs [13]
- Homomorphic encryption [14, 18]

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

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*

PhD Airbus – Roderick Asselineau (2025–2028) – *Cryptanalyse de constructions symétriques et extraction de modèles IA*

9.2 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 Sécurisé 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.

10 Partnerships and cooperations

10.1 International initiatives

10.1.1 Visits of international scientists

Inria International Chair

Participants: Claude Crépeau.

10.2 European initiatives

10.2.1 H2020 projects

PARQ [PARQ project on cordis.europa.eu](https://cordis.europa.eu/parq)

Title: Lattices in a Parallel and Quantum World

Duration: From July 1, 2020 to June 30, 2026

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:

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.

10.3 National initiatives

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.

PQ-TLS: Post-Quantum TLS

Participants: Brice Minaud.

Program: ANR PEPR quantique

Duration: 2022 – 2028

Coordinator: Pierre-Alain Fouque

Partners: ENS, Inria, CNRS, DGA, CryptoExperts, PQShield, ANSSI, CryptoNext, Thales

Summary: This integrated project aims to develop in 5 years post-quantum primitives, suitable for use in a post-quantum version of TLS.

11 Dissemination

Participants: Brice Minaud, Phong Nguyen, David Pointcheval

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

Member of the organizing committees

- Comité de pilotage du GT C2, Codage et Cryptographie (Brice Minaud)

11.1.2 Scientific events: selection

Member of the conference program committees

Crypto 2025 (Brice Minaud)

Eurocrypt 2025 (Brice Minaud)

CT-RSA 2025 (Brice Minaud)

PQCrypto 2025 (Phong Nguyen)

Reviewer

- Eurocrypt '25 (Phong Nguyen)
- Crypto '25' (Phong Nguyen)

11.1.3 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)

11.1.4 Invited talks

- PQ-TLS Summer School, invited talk on multivariate cryptography (Brice Minaud)
- PEPR Cybersécurité Winter School 2025, invited talk on encrypted databases (Brice Minaud)

11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

- 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
- Cryptography (Master MSSIS, ESIEA)
- Joint directorship of MPRI (M2, PSL/IPP/UPC/UPS).
- Examiner for entrance exams to ENS (oral exam in Fundamental Computer Science).
- Corrector for entrance exams to ENS (written exam in Fundamental Computer Science).

11.2.1 Supervision

- M2 Internship of Alexandre Camelin (Phong Nguyen)
- M2 Internship of Giacomo Spriano (Phong Nguyen)

11.2.2 Juries

- Reviewer of Maya Chartouni's PhD, UVSQ (Phong Nguyen)
- Jury member of Paul Kirchner's PhD, Univ. Rennes (Phong Nguyen)
- Jury member of Pierre Pébereau's PhD, Sorbonne Univ. (Brice Minaud)
- Jury member of Adam Oumar Abdel-Rahman's PhD, Télécom Sud Paris (Brice Minaud)

11.3 Popularization

11.3.1 Participation in Live events

- Program "Semaine NSI/Chiche" at Inria Paris: Phong Nguyen gave an introduction to cryptography for 120 high-school students.

12 Scientific production

12.1 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](https://doi.org/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](https://doi.org/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](https://doi.org/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.

12.2 Publications of the year

International journals

- [13] B. Abdolmaleki, C. Chevalier, E. Ebrahimi, G. Malavolta and Q.-H. Vu. ‘On Quantum Simulation-Soundness’. In: *IACR Communications in Cryptology* 1.4 (13th Jan. 2025). doi: [10.62056/a66ce01uc](https://doi.org/10.62056/a66ce01uc). URL: <https://hal.science/hal-05058158> (cit. on p. 11).

- [14] C. Brzuska, S. Canard, C. Fontaine, D. H. Phan, D. Pointcheval, M. Renard and R. Sirdey. ‘Relations Among New CCA Security Notions for Approximate FHE’. In: *IACR Communications in Cryptology* 2.1 (8th Apr. 2025), pp. 1–35. DOI: [10.62056/ae0iv7sf](https://doi.org/10.62056/ae0iv7sf). URL: <https://hal.science/hal-05104791> (cit. on p. 11).
- [15] 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](https://doi.org/10.1016/j.tcs.2025.115155). URL: <https://hal.science/hal-04987985> (cit. on p. 11).
- [16] L. Monbroussou, E. Mamon, H. Thomas, V. Yacoub, U. Chabaud and E. Kashefi. ‘Toward quantum advantage with photonic state injection’. In: *Physical Review Research* 7.3 (11th July 2025), p. 033051. DOI: [10.1103/PhysRevResearch.7.033051](https://doi.org/10.1103/PhysRevResearch.7.033051). URL: <https://hal.science/hal-05409630>.

International peer-reviewed conferences

- [17] H. Bambury and P. Q. Nguyen. ‘Cryptanalysis of an Efficient Signature Based on Isotropic Quadratic Forms’. In: *Lecture Notes in Computer Science*. 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](https://doi.org/10.1007/978-3-031-86602-9_6). URL: <https://hal.science/hal-05016873> (cit. on p. 11).
- [18] J. Baudrin, S. Belaïd, N. Bon, C. Boura, A. Canteaut, G. Leurent, P. Paillier, L. Perrin, M. Rivain, Y. Rotella and S. Tap. ‘Transistor: a TFHE-Friendly Stream Cipher’. In: *Lecture Notes in Computer Science*. CRYPTO 2025 - 45th Annual International Cryptology Conference. Vol. LNCS-16004. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 17th Aug. 2025, pp. 530–565. DOI: [10.1007/978-3-032-01901-1_17](https://doi.org/10.1007/978-3-032-01901-1_17). URL: <https://hal.science/hal-05258560> (cit. on p. 11).
- [19] X. Bultel, C. Chevalier, C. Jojon, D. Liu and B. Nguyen. ‘Cryptographic Commitments on Anonymizable Data’. In: 10th IEEE European Symposium on Security and Privacy (EuroS&P 2025). 10th IEEE European Symposium on Security and Privacy (EuroS&P 2025). Venice, Italy: IEEE, 30th June 2025. URL: <https://hal.science/hal-05027266> (cit. on p. 11).
- [20] 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. 11).
- [21] 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). Venice, Italy, 30th June 2025. URL: <https://hal.science/hal-05031107> (cit. on p. 11).
- [22] K. Nguyen, D. H. Phan and D. Pointcheval. ‘Multi-client Functional Encryption with Public Inputs and Strong Security’. In: *Public-Key Cryptography – PKC 2025* 28th IACR International Conference on Practice and Theory of Public-Key Cryptography, Røros, Norway, May 12–15, 2025, Proceedings, Part III. Public-Key Cryptography – IACR PKC 2025 - 28th IACR International Conference on Practice and Theory of Public-Key Cryptography. Vol. 15676. Lecture Notes in Computer Science. Røros, Norway: Springer, 5th May 2025, pp. 68–101. DOI: [10.1007/978-3-031-91826-1_3](https://doi.org/10.1007/978-3-031-91826-1_3). URL: <https://hal.science/hal-05104777> (cit. on p. 11).
- [23] D. Pointcheval and R. Schädlich. ‘Multi-client Attribute-Based and Predicate Encryption from Standard Assumptions’. In: *Theory of Cryptography, 22nd International Conference, TCC 2024, Milan, Italy, December 2–6, 2024, Proceedings, Part III*. 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](https://doi.org/10.1007/978-3-031-78020-2_2). URL: <https://hal.science/hal-05029340> (cit. on p. 11).

Doctoral dissertations and habilitation theses

- [24] N. Bon. ‘Development of Optimized Operations for Homomorphic Cryptography’. Ecole Normale Supérieure, 14th Nov. 2025, pp. 302–341. URL: <https://theses.hal.science/tel-05542687>.
- [25] G. Lebrun. ‘Security and Efficiency of Secure Group Messaging Protocols’. École Normale Supérieure de Paris - ENS Paris; Paris Sciences et Lettres, 1st Dec. 2025. URL: <https://theses.hal.science/tel-05541205>.
- [26] R. Schädlich. ‘Secure Computation on Encrypted Data in Multi-User Systems’. ENS-PSL, 2nd Dec. 2025. URL: <https://theses.hal.science/tel-05561744>.

Reports & preprints

- [27] F. Arzani, R. I. Booth and U. Chabaud. *Can effective descriptions of bosonic systems be considered complete?* 2025. DOI: [10.48550/arXiv.2501.13857](https://doi.org/10.48550/arXiv.2501.13857). URL: <https://hal.science/hal-04990688>.
- [28] C. E. Lopetegui-González, G. Massé, E. Oudot, U. I. Meyer, F. Centrone, F. Grosshans, P.-E. Emeriau, U. Chabaud and M. Walschaers. *A unified framework for Bell inequalities from continuous-variable contextuality*. 12th Jan. 2026. URL: <https://hal.science/hal-05491952>.