

2025 Activity Report

RESEARCH CENTRE: Inria Centre at Rennes University

IN PARTNERSHIP WITH: Université de Rennes

Project-Team

CAPSULE

Applied Cryptography and Implementation Security

In collaboration with Institut de recherche en informatique et systèmes aléatoires (IRISA)



Project-Team CAPSULE

Creation of the Project-Team: 2023 January 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

- A1.2.8. – Network security
- A4.3. – Cryptography
 - A4.3.1. – Public key cryptography
 - A4.3.2. – Secret key cryptography
 - A4.3.3. – Cryptographic protocols
- A4.6. – Authentication
- A4.8. – Privacy-enhancing technologies
- A7.1.4. – Quantum algorithms
- A8.5. – Number theory

Other research topics and application domains

- B6.4. – Internet of things
- B9.5.1. – Computer science
- B9.5.2. – Mathematics
- B9.10. – Privacy

Contents

Project-Team CAPSULE	1
1 Team members, visitors, external collaborators	5
2 Overall objectives	6
3 Research program	7
3.1 Security against post-quantum attackers	7
3.2 Symmetric Cryptography	8
3.3 Elliptic curves for public-key cryptography	10
3.4 Security of cryptographic implementation and Real-World Cryptography	10
4 Application domains	12
4.1 Designing, Analyzing and Choosing Cryptographic Standards	12
5 Social and environmental responsibility	13
5.1 Impact of research results	13
6 Highlights of the year	13
6.1 Awards	13
7 Latest software developments, platforms, open data	13
7.1 Latest software developments	13
7.1.1 TNFS-alpha	13
7.1.2 Qarton	14
8 New results	14
8.1 Secret-Key Cryptography	14
8.1.1 Proofs of Security of Symmetric Constructions	14
8.1.2 Symmetric Cryptanalysis of Primitives and Tools	14
8.1.3 Quantum Cryptanalysis	17
8.2 Public-key cryptography	17
8.2.1 Lattices	17
8.2.2 Elliptic curves and isogenies	20
8.2.3 Quantum Cryptanalysis	21
8.2.4 Protocols	22
8.3 Side-Channel Attacks	23
9 Bilateral contracts and grants with industry	24
9.1 Bilateral Grants with Industry	24
10 Partnerships and cooperations	25
10.1 International initiatives	25
10.1.1 Visits to international teams	25
10.2 National initiatives	26
11 Dissemination	28
11.1 Promoting scientific activities	28
11.1.1 Scientific events: organisation	28
11.1.2 Scientific events: selection	28
11.1.3 Journal	29
11.1.4 Invited talks	29
11.1.5 Scientific expertise	30
11.1.6 Research administration	30
11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach	30

11.2.1 Teaching	30
11.2.2 Supervision	32
11.2.3 Juries	33
11.2.4 Educational and pedagogical outreach	34
11.3 Popularization	34
11.3.1 Productions (articles, videos, podcasts, serious games, ...)	34
11.3.2 Participation in Live events	34
12 Scientific production	35
12.1 Major publications	35
12.2 Publications of the year	35
12.3 Cited publications	38

1 Team members, visitors, external collaborators

Research Scientists

- Patrick Derbez [INRIA, HDR]
- Aurore Guillevic [INRIA, Researcher]
- Andre Schrottenloher [INRIA, Researcher]
- Yixin Shen [INRIA, Researcher]

Faculty Members

- Pierre-Alain Fouque [Team leader, Univ Rennes, Professor, HDR]
- Daniel De Almeida Braga [Univ Rennes, Associate Professor]
- Damien Marion [Univ Rennes, Associate Professor]

Post-Doctoral Fellows

- Pierrick Dartois [INRIA, from Sep 2025]
- Charles Meyer-Hilfiger [Univ Rennes, Post-Doctoral Fellow, from Oct 2025]

PhD Students

- Roderick Asselineau [AIRBUS, CIFRE, from Jun 2025]
- Mathias Boucher [Univ Rennes, from Sep 2025]
- Clemence Chevignard [Univ Rennes]
- Gael Claudel [INRIA]
- Mathieu Degre [Univ Rennes]
- Paul Delhom [Univ Rennes, CIFRE, from Nov 2025]
- Marie Euler [DGA-MI, from Oct 2025]
- Baptiste Germon [Univ Rennes]
- Théo Goureau [INRIA, from Oct 2025]
- Aymeric Hiltenbrand [Univ Rennes]
- Alisee Lafontaine [INRIA, from Oct 2025]
- Phuong Nguyen [Univ Rennes, until Feb 2025]
- Guilhem Niot [PQSHIELD, CIFRE]
- Pierrick Philippe [INRIA, from Oct 2025]
- Aurel Pichollet–Mugnier [Univ Rennes]

Technical Staff

- Zoe Vignes [INRIA, Engineer, from Sep 2025]

Interns and Apprentices

- Alexandre Autran [INRIA, Intern, from Jun 2025 until Aug 2025]
- Mathias BOUCHER [Univ Rennes, from Mar 2025 until Jun 2025]
- Todd Cauet-Male [INRIA, Intern, until Jul 2025]
- Hubert DE GROOTE [Univ Rennes, from Mar 2025 until Aug 2025]
- Alisée LAFONTAINE [INRIA, from Mar 2025 until Aug 2025]
- Adrien LAGASSE [INRIA, from May 2025 until Aug 2025]
- Babacar Ndiaye [INRIA, Intern, from Apr 2025 until Aug 2025]

Administrative Assistants

- Loïc LESAGE [INRIA, from Mar 2025 until Sep 2025]
- Eleonora SABA [INRIA, from Oct 2025]

External Collaborators

- Clément Dell'Aiera [DGA-MI]
- Marie Euler [DGA-MI]
- Mathieu Goessens [Univ Rennes, until Aug 2025]
- Tuong-Huy Nguyen [DGA-MI]

2 Overall objectives

Nowadays, and contrary to the past decades, the design of cryptographic algorithms follows an integrated approach which considers security, efficiency and implementation requirements at the same time. The research activities of the team CAPSULE tackle these challenges in order to provide more secure cryptographic implementations and applications deployed in the real world.

- Highly efficient symmetric cryptosystems are a prerequisite for all cryptographic infrastructure. Recently, many new designs have been proposed, which aim to perform well under various constraints (e.g., lightweight cryptographic schemes, or schemes tailored for advanced FHE and MPC protocols). The confidence in these schemes is based on cryptanalysis, analyzing their security against classical and quantum adversaries. Our research lies not only in finding new attacks, but also in designing automated audit tools that simplify and systematize this task.
- Post-quantum security is a major challenge that cryptographers are facing right now. As new post-quantum designs for encryption and digital signatures are being standardized by NIST, the CAPSULE team is actively involved in further improving the efficiency of these schemes and their security analysis, both against classical and quantum adversaries.
- Both symmetric and asymmetric cryptosystems need ultimately to be implemented, and these implementations can be vulnerable to various types of side-channel attacks. Finding new attacks and implementing new countermeasures are two sides of the same coin.
- We are also interested in studying the security of well-known deployed systems, such as the security of TLS, secure messaging, and databases.

3 Research program

3.1 Security against post-quantum attackers

The seminal paper of Peter Shor at FOCS 1994 [97] shows that if we were able to build quantum computers, then the factorization and discrete logarithm problems could be solved in polynomial time. Since then, there has been a tremendous effort in the cryptographic community to propose cryptosystems that are secured in the presence of quantum computers. Many alternatives to the two number theoretic problems above have been proposed. Among them, our team already has activities and interests in two types of assumptions:

- lattice-based schemes, where security is based on the difficulty of computing short vectors in random euclidean lattices;
- code-based schemes, where security is based on the difficulty on computing low hamming weight words in random codes.

Euclidean lattices are discrete subgroups of \mathbb{R}^n , while codes are linear subspaces of a vector space over a finite field. The semantic similarities between the hardness assumptions are not unexpected: lattices and codes appearing in cryptography are often related objects, that one could say considered from different metric perspectives.

In post-quantum cryptography, lattice-based assumptions take an important place and received an increasing amount of attention in the last decade, thanks to the strong security guarantees provided by these assumptions as well as their flexibility for cryptographic designs. Indeed, Ajtai and Regev presented reductions between, respectively, finding Short Integer Solutions of random linear systems (SIS) or solving random noisy linear systems (“Learning With Errors”, LWE) and computing short vectors in euclidean lattices in the worst case. They both serve as the foundation of security to design public-key encryptions, digital signatures, zero-knowledge proof systems, key-encapsulation mechanisms, homomorphic encryption ... In order to improve practical efficiency, “structured” versions of these problems relying on lattices with symmetries have been proposed. Such lattices are related to algebraic objects appearing in the geometry of numbers and some of the resulting schemes have been the clear winners of NIST’s call for standardization.

Better Reductions. Our trust in the hardness of lattice-based constructions relies fundamentally on our understanding of the security reductions between the (many, structured) variants of SIS and LWE. Depending on the additional structure allowed to the designer, they are associated to number rings, ideals, and, more generally, modules over the integer ring of a number field, and related to the corresponding class of lattices with symmetries. Additionally, for LWE the noise distribution is also a parameter of the problem. Overall, this leads to a plethora of variants and versions that need some hierarchizing and a better understanding of the interplay between their related parameters. Thankfully, important classifying works have already been presented, regularly involving members of our team (e.g. [56, 94, 51]).

Yet, there are still many unclear results or relations that are not yet satisfyingly understood. For example, the fundamental reductions of Ajtai and Regev are far from tight, incurring a blowup in important parameters (sometimes estimated to be in $O(n^{11})$). While this is not a problem asymptotically, it clearly raises concerns on how to select parameters and the level of security they actually achieve. However, these proofs techniques have not been updated since their presentations: it is not unlikely that more recent tools could lead to improvements. In another example, there seems to be a non smooth gap of difficulty between the hardness of very structured variants of LWE (linked to “ideal lattices problems”) and less-but-still-quite structured ones. Roughly speaking, the former seems to belong to subexponential complexity while the latter variants are still considered exponential. Our current knowledge is also not enough to guarantee the actual existence of this gap, which prevents an accurate understanding of the underlying problems’ concrete hardness. In a last example, one can also notice that all the proof strategies for these general reductions rely on the same high-level arguments. Yet, multiple works dealing with subcases had to be presented to reach the current state of the art. On the one hand, it could be that there is a unifying, all-encompassing presentation that would greatly simplify the state of the affairs and bring a kind of maturity to this field. On the other hand, there may be fundamental obstructions to a general framework, and highlighting them would definitely help the community’s understanding. These three examples raise important questions first about security, but also

about our way of using the mathematical tools behind these results. Our team’s objectives are to investigate all these paths and to find either positive or negative answers to improve the general understanding of the area.

Algorithms for hard problems and attacks on cryptosystems. We have proposed some algorithms to study the security of hard computational problems in cyclotomic fields as the Principal Ideal Problem (PIP) in [47], reducing module lattices as a generalization of the LLL algorithm in the ring of integers of a number field in [83] or in a tower of cyclotomic fields in [78]. We generalized the BKW algorithm to binary LWE setting in [79] and studied the Learning Parities with Noise (LPN) Problem in [84].

We have also attacked concrete cryptographic schemes. We broke some multivariate schemes such as the SFLASH signature schemes in [64] and variants [71], and the ASASA schemes in [87]. We have also broken FHE schemes based on overstretched NTRU parameters in [80] or concrete FHE in [58].

We want to study the resistance of post-quantum cryptosystems and hard problems against classical and quantum adversaries. It is particularly interesting for lattice problems since the cryptanalysis of these problems is very young. One key objective in this line of research would be to find an analog of the BKZ algorithm for structured lattices defined over a number field. It is also interesting to improve the recent work of [45], which suggests that this problem may be weaker than previously thought.

Constructions and practical cryptosystems. Applications of cryptography usually culminate with the description of an efficient cryptosystem. An important part of our activity in post-quantum cryptography therefore targets the design of new schemes resistant to quantum attackers, providing advanced functionalities to its users, without sacrificing efficiency.

In this area, members of CAPSULE have worked on the lattice-based signature scheme **Falcon** and its efficiency-security trade-off **ModFalcon** [59]. A first objective would be to extend in a useful way the so-called “trapdoor generation” which is core to the two schemes above. In a nutshell, the secret key corresponds to a basis of short vectors of a lattice, that only the user should be able to compute efficiently. **ModFalcon** already extended the class of lattices for which this can be done, and it is an interesting question to manage an even larger class of lattice. In terms of applications, this would allow for even more flexibility, which can be particularly useful when the signature scheme is used as a black box inside a larger cryptographic algorithm. It could also allow for other functionalities such as threshold signatures or maybe masked signatures. On this line of thought, we are also interested in designing masked lattice signatures or even multi-party signatures. While there have been very recent proposals (relying on a different paradigm than the Falcon family), the efficiency is still lacking in practice. A success here could lead to concrete industrial applications.

But this is not the only construction on which the team is currently working. There are many interesting cryptographic constructions that need to be studied to obtain efficient post-quantum schemes, such as signatures and zero-knowledge proofs, but also signatures with more properties like group signatures, blind signatures ... and applications like e-voting. Indeed, a lot of progress has been made to obtain efficient signatures and public key encryptions, especially with the NIST competition, but the efficiency of more advanced schemes is still far from existing (but not post-quantum) solutions. One of the big challenges would be to obtain efficient zero-knowledge proof systems, as this primitive is often an easy way to build more advanced primitives.

3.2 Symmetric Cryptography

Despite being one of the oldest forms of cryptography, symmetric cryptography is a very active research area, with recent activity focusing on new designs optimized for specific operational constraints. For example, the *lightweight cryptography* competition launched by the NIST¹ in 2017 concluded in 2023 by selecting the lightweight cipher family **Ascon** [63], optimized for hardware implementations. At the same time, many new ciphers have been proposed which are optimized to be integrated in advanced cryptographic protocols, such as the FHE-friendly block cipher **LowMC**, or protected hardware implementations.

¹National Institute for Standards and Technology, a U.S. standardization agency whose cryptographic standards become de facto world standards.

The team CAPSULE studies the security of symmetric primitives such as block ciphers, stream ciphers and hash functions, against various types of attacks. We consider both classical and quantum security, the latter being a prerequisite for post-quantum cryptography architectures.

Tools for discovering new attacks. Symmetric cryptosystems are widely used because they are the only ones that can achieve some major functionalities such as high-speed or low-cost encryption, fast message authentication, and efficient hashing. But, unlike public-key cryptographic algorithms, secret-key primitives do not have satisfying security proofs. The security of these algorithms is empirically established by cryptanalysis.

It is obvious that this security criterion, despite its success so far, is not completely satisfactory. For instance we may estimate that, for a given primitive, no more than a few dozens of researchers are actively working on breaking it. Hence, due to this weak effort, the non-discovery of an attack against a particular primitive does not mean so much. Besides, finding the best attacks on a given design is a time-consuming work, and errors can lead to under- or over-estimating its security.

Therefore, our team specializes in building tools for automatically finding large classes of attacks. This transforms the statement “we did not find any attack of this kind”, which is only a subjective guarantee, into “the audit tool X did not find any attack”, which is a formal statement, giving a quantifiable objective guarantee.

In the past, the members of the team have proposed many tools, for example for improving attacks on round-reduced versions of AES [53], Demirci-Selçuk attacks on AES [62], and impossible differential attacks [61].

Our more recent work uses tools based on MILP (Mixed Integer Linear Programming), SAT (Satisfiability) or CP (Constraint Programming). In this setting, the search and optimization of an attack are reduced to a problem of a specific form, for which an off-the-shelf solver is used. Besides the actual work of implementing this reduction, our research aims at better understanding the differences between these optimization tools, finding which ones are more adapted for a given problem, and adapting some of these general-purpose software tools to particular cryptographic problems.

Finding and optimizing a cryptanalytic attack in its entirety is an especially interesting problem, since it requires the integration of different steps (for example a good distinguisher and a key-recovery phase). Since the search space is of exponential size, often making the problem intractable, it is possible to first find an approximation of the best attacks and then instantiate precisely the values of the parameters. Also, if MILP, SAT and CP tools quickly give an answer, it is tempting to build ad-hoc tools that can more efficiently take into account the weaknesses discovered by these tools.

Finally, there are only a few tools for analyzing the security of ARX ciphers based on additions, rotations and xor operations. These functions are hard to analyze with the current cryptanalytic techniques, and no attack has really endangered the full Chacha stream cipher proposed by Dan Bernstein or the block cipher Speck proposed by the NSA. They can be implemented very efficiently in x86 processors and currently Chacha is in the most used ciphersuites on TLS, making them prominent targets for cryptanalysis.

New Designs. Our goal is to analyze the security of the new symmetric-key designs by developing new cryptanalytic techniques. The LowMC block cipher is one of the first symmetric primitives designed for taking into account the efficiency constraints of public-key cryptosystems. It has been built as a FHE-friendly cipher, by minimizing the number of multiplicative gates which are the main efficiency bottleneck for this application. Several attacks have been proposed on LowMC and LowMC v2. LowMC v3 was used in Picnic, a Zero-Knowledge-based post-quantum signature scheme proposed at the NIST competition, which wasn't standardized.

The Keccak hash function has been standardized in 2015 as SHA-3. Keccak brought new interest in a new design called Sponge function and permutation-based primitives. Some round-reduced versions of SHA-3 have been used in many constructions from Pseudo-Random Generator in SHAKE, to the Pseudo-Random Function Farfalle [46], the authenticated encryption scheme Keyak, or the hash function KangarooTwelve proposed as an RFC. Only a few attacks have been proposed against SHA-3 and new cryptanalysis tools need to be designed.

Quantum Cryptanalysis. Since 2016, many works have been done in the cryptanalysis of symmetric primitives using quantum algorithms. While symmetric cryptosystems are generally believed to hold well against adversaries equipped with a quantum computer, these works have substantiated these claims with dedicated security analyses, such as the best attacks against reduced-round versions of the standard AES [49].

Grover’s search algorithm, which can provide a quadratic speedup on exhaustive key search (from 2^k operations to $2^{k/2}$), is often cited as the main player in the quantum security of symmetric primitives. However, in the past few years, the landscape of quantum algorithms for cryptanalysis has considerably expanded, with notable results such as quantum speedups above quadratic for specific constructions [50]. These recent works highlight the benefit of combining state-of-the-art quantum algorithms and symmetric cryptanalysis techniques.

In team CAPSULE, our research in quantum cryptanalysis is three-fold.

First, we develop new quantum algorithms for cryptanalytic problems, which we aim to apply in symmetric cryptography, but may also have applications in public-key cryptography. An example of such a double-edged sword is our recent work on quantum walks [48].

Second, we analyze existing classical cryptanalysis techniques and study how to translate them into quantum cryptanalysis techniques. Intuitively, a primitive that is classically vulnerable should be quantumly broken as well, but this is not always the case, as classical attack strategies are not always exploitable in the quantum setting. Our research in this area focuses on the strategies which can exhibit the largest quantum speedups, quadratic (like Grover’s search) or even above by using advanced frameworks.

Finally, after identifying new classes of quantum attacks, we aim at integrating these attacks into automated tools. Indeed, the task of finding and optimizing quantum attacks can be even more challenging than classical ones, since they rely often on different strategies, sometimes counterintuitive. Furthermore, since the resulting procedures are quantum algorithms, the analysis of their time and memory complexities comes with specific technicalities. Our goal is to automatize this step as well in a way that may benefit cryptanalysts interested in this topic but unfamiliar with quantum algorithms.

3.3 Elliptic curves for public-key cryptography

With Aurore Guillevic joining the team in 2024, the research themes extended to elliptic curve cryptography. In public-key cryptography, elliptic curves over finite fields are a mathematical algebraic structure which provides the best trade-off between speed and key-sizes. The group of points on the curve efficiently replaces the multiplicative subgroup of prime finite fields as an implementation choice for discrete-logarithm based protocols. More recently with the rise of proof systems, elliptic curves with dedicated properties are designed. In particular, *pairing-friendly* elliptic curves are equipped with a bilinear pairing (like a scalar product) that allows to multiply once secret scalars “in the exponents” without revealing them. It led to Succinct Non-interactive ARguments of Knowledge (SNARK), a mechanism that blindly checks the validity of a quadratic equation “in the exponents”. The cornerstone work by Groth in 2016 obtained a SNARK of the smallest cost in terms of pairing computation and allowed the development of many variants tailored for various proof systems. The work in the team includes designing new dedicated and secure elliptic curves (finding parameters of cryptographic size), studying the security of existing curves, and developing software modules implementing fast pairings on new elliptic curves.

3.4 Security of cryptographic implementation and Real-World Cryptography

In this research axis, our aim is to study the security of implementations against various side channels such as fault attacks, power analysis and electromagnetic emanations, as well as timing attacks on various cryptographic schemes deployed in real-world systems. We are also interested in providing security proofs for real-world systems or improving their security.

Hardware and embedded implementations. Side Channel Attacks (SCA) rely on statistical tools to extract the secret information from leakage traces. Then, algorithmic techniques usually based on previous cryptanalytic results are used to efficiently recover secret data. Indeed, the known black-box attacks are extended by exploiting the leakage information, that gives more information on the internal secret variables, a.k.a. the grey-box model. The SCA information can be for instance the Hamming weight of a limited

number of variables. Recently, the white-box model has been proposed, where the adversary can stop the execution of a process and has access to *all* variables.

Side-channel attacks have been successfully applied to break many embedded implementations these last 20 years. After the information theoretic approach of Ishai, Sahai and Wagner [76] to prove the security of implementations, secure theoretical foundations have been laid by Prouff and Rivain and later Duc et al. in [93, 65]. Soon after, some tools have been developed such as [41, 42, 40] to protect software and hardware implementations with masking techniques. Nowadays, we have sound masking schemes. Some of them already have been introduced into lattice-based implementations [43], where generally securing randomness presents an interesting challenge. We aim at extending the results of [43, 44, 86, 70] to other post-quantum alternatives like code-based, multivariate, or hash-based schemes and to **provide secure implementations**.

More recently, other tools coming from statistical learning (such as deep learning) have been proposed to break embedded implementations. They open the door to powerful techniques and more efficient attacks. Template attacks model the leakage distribution with a Gaussian distribution, approximating the actual distribution by considering its mean and its standard deviation. More standard attacks, a.k.a. Differential Power Analysis (DPA), only consider the mean. However, higher moments can be useful to consider. Deep learning techniques are useful to efficiently extract complex relations between variables even in the presence of noise. Taking into account these more powerful **deep learning** or **white-box** attacks as well as developing countermeasures is a hot, trendy topic in SCA. In the former, deep learning allow to find correlations between many points of interest of one curve, a.k.a. horizontal attacks. In the latter, white-box cryptography provides the adversary with the same kind of information, since they can stop the execution of the program and get noiseless information on all of its variables. Taking into account such powerful attackers is one main challenge for side-channel attacks.

Finally, we are interested in working on the new micro-architectural attacks **HertzBleed** and **others**. These attacks show that side-channel attacks are also a threat to software implementations. Porting to software some of the many techniques used to secure embedded systems is thus a major topic.

Software implementations. Constant-time implementation is a programming principle that aims at providing code where the running time and memory accesses are independent of the secret values. Timing leakage can be used to mount attacks on computers and smartphones. There exist many tools in the literature that help developers to avoid these leakage, but insecure implementations are still aplenty. For instance, we recently broke the WPA-3 implementation used in FreeRadius and iwd (iNet Wireless Daemon) [54], and also found other weaknesses.

We want to **discover new attacks in open-source libraries** and to help developers in order to **verify the constant-time property** of their codes. For example, some tools are tailored to small pieces of cryptographic codes and do not scale well with more complex codes that rely on many libraries. Our goal is to provide verification tools for analyzing the constant-time property of large source codes. We are also interested in studying the security of DRM systems used in widely deployed systems. We do not have permanent researchers on reverse-engineering, but we work with postdoc students such as Alexandre Gonzalez, as well as Mohamed Sabt from the Spicy team on this topic. Besides, we co-supervise 3 theses on the security of software implementations.

Security Proofs of Protocols and Real-World Systems. We are interested in studying the security of cryptographic protocols deployed in the real-world such as WhatsApp, middlebox, Content-Delivery Network (CDN), TLS, and 5G networks. Recently, we have also considered the security of searchable symmetric encryption, where the goal is to outsource the storage of a database to an untrusted server, while maintaining search capabilities. This last area is a nice application of secure computations and the PhD thesis of R. Bost (P.A. Fouque's PhD student) in this domain received the GDR Security price of the best PhD in 2018. We also work with Cristina Onete, an assistant professor at Limoges on this topic. Currently, we are interested to propose hybridization techniques between pre- and post-quantum cryptography for various protocols such as Signal, IPSEC, ... in the PEPR post-quantum cryptography.

Microarchitectural attacks. Microarchitectural attacks are very potent side-channel attacks that exploit the microarchitecture features of modern processors, such as caches, branch predictors, and speculative execution. They represent a significant threat to the security of cryptographic implementations, as they can leak sensitive information through subtle timing variations and other side effects. Most work focuses on x86 architectures, but ARM architectures are also concerned, especially with the widespread use of ARM in mobile devices, and recent interest in deploying more ARM CPUs in laptop and desktop computer. We are interested in studying complex ARM microarchitectures, such as the Qualcomm Snapdragon chip, to understand their vulnerabilities to microarchitectural attacks. This line of work involves reverse-engineering the microarchitecture, developing new attack techniques, and proposing effective countermeasures to mitigate these threats. We investigate these topics in collaboration with the SUSHI Inria team and the ANSSI.

4 Application domains

4.1 Designing, Analyzing and Choosing Cryptographic Standards

The research community is strongly involved in the development and evolution of cryptographic standards. Many standards are developed through open competitions (e.g. AES, SHA-3) where multiple teams propose new designs, and a joint cryptanalysis effort allows to select the most suitable proposals. The analysis of established standards is also an important work, in order to deprecate weak algorithms before they can be exploited. Several members of the team have been involved in this type of effort and we plan to continue this work to ensure that secure algorithms are widely available. We believe that good cryptographic standards have a large socio-economic impact; thus, we are active in proposing schemes to future competitions, and in analyzing schemes proposed to current or future competitions, as well as widely-used algorithms and standards. At the moment, we are involved in the two standardization efforts run by NIST for post-quantum cryptography and lightweight cryptography, and other real-world protocols.

NIST post-quantum competition. The NIST post-quantum competition aims at standardizing quantum-safe public-key primitives. The goal is to propose a quantum-safe alternative for the schemes based on number theory which are threatened by the advent of quantum computers. It is expected to have a huge and long-term impact on all public-key cryptography. It received 69 proposals in November 2017. The Falcon signature scheme, co-designed by some members of the Capsule team, has been selected by NIST in July 2022. We have also submitted Solmae to the Korean Post-Quantum Competition, which is a variant of Falcon that is easier to implement hence to protect from SCA. Finally, we have also proposed BAT [69], an encryption scheme that follows the design rationale of Falcon. We plan to submit this scheme to the IETF as it enjoys interesting properties in terms of bandwidth, that are not displayed by NIST's selected key encapsulation scheme, Kyber.

In June 2023, we have submitted the PROV and VOX signature schemes to NIST's new call for digital signatures. These two schemes are based on multivariate cryptography problems, and are variants of the unbalanced Oil-and-Vinegar signature schemes, proposed in 1997 by Patarin. PROV has a security proof, while VOX is a stronger version of UOV that avoids known weaknesses (namely, UOV has a large set of isotropic vectors common to all quadratic forms of the public key).

NIST competition on lightweight symmetric encryption. The NIST lightweight cryptography standardization process is an initiative to develop and standardize new authenticated encryption algorithms suitable for constrained devices. There is a real need for new standards in lightweight cryptography, and the selected algorithms are expected to be widely deployed within the Internet of Things, as well as on more constrained devices such as contactless smart cards, or medical implants. The NIST received 56 submissions in February 2019. Team Capsule has studied the security of some of these schemes.

Monitoring Current Standards. While we are very involved in the design phase of new cryptographic standards, we also monitor the algorithms that are already standardized. We look at some implementations of WPA3 and we discovered a micro-architectural attack [55]. We also studied the privacy of the EME standard (Encrypted Media Extensions) for Digital Rights Management in browsers in [89].

5 Social and environmental responsibility

5.1 Impact of research results

The work [29] has been improved by Craig Gidney in a new evaluation for Shor's algorithm on Google Quantum architecture [72]. It shows that less than 1400 logical qubits, or about 1 million physical qubits, are needed to factor RSA 2048 bits if a quantum computer is built. This result has been presented in 2024 in QIP and in 2025 in CRYPTO. André Schrottenloher also gave a talk at the Simons Institute (Berkeley) in Summer 2025, Clémence Chevnard at Quantum Innovation 2025 in Nagoya, and Pierre-Alain Fouque in the Tavares Lecture at the Selected Area in Cryptography, SAC Conference, Toronto 2025.

The same algorithm can be used to attack the discrete logarithm problem in finite field, such as safe prime field. In the specific case of IKE (Internet Key Exchange), the key exchange algorithm used in IPSEC, with short discrete log, the attack only requires 300 logical qubits to be implemented.

6 Highlights of the year

1. The paper [13], published at Eurocrypt 2025, presents a blockcipher for encrypting program instructions in order to avoid timing attacks on cryptographic implementations.
2. The paper [15], published at CRYPTO 2025, describes a dual attack on Kyber and reassesses the security of the standard.

6.1 Awards

1. The paper [25], published at DSN 2025, has received the best paper award.

7 Latest software developments, platforms, open data

7.1 Latest software developments

7.1.1 TNFS-alpha

Name: alpha for the Tower Number Field Sieve algorithm

Keyword: Cryptography

Functional Description: This library implements a simulation tool for the tower number field sieve algorithm computing discrete logarithms in extension fields of small degree (tested up to 54). The library contains an implementation of the exact computation of alpha, the bias between the expected smoothness of an integer and the expected smoothness of a norm of an algebraic integer in a number field made of two extensions. The algorithm is a generalization to extensions of the exact implementation of alpha in the software CADO-NFS. The software contains an implementation of the E-function of B. A. Murphy (Murphy's E) which estimates the quality of the polynomial selection step in TNFS through a simulation of the yield of the relation collection in the TNFS algorithm. Finally, it contains a database of pairing-friendly curve seeds with the estimated level of security w.r.t. a discrete logarithm computation in the corresponding finite field.

News of the Year: In 2025, new curves in the family Gasnier-Guillevic were added. As part of the PEPR Cryptanalyse, new tables of polynomials with automorphisms were included to the project (degrees 6, 8, 9). Finally, new tables of sparse polynomials of degrees 19 and 26 were included.

URL: <https://gitlab.inria.fr/tnfs-alpha/alpha>

Publications: [hal-04666521](#), [hal-04205681](#), [hal-03667798](#), [hal-03371573](#), [hal-02263098](#), [hal-02396352](#)

Contact: Aurore Guillevic

Participant: Aurore Guillevic

7.1.2 Qarton

Keywords: Quantum programming, Cryptography, Post-quantum, Quantum cryptanalysis

Functional Description: Qarton is a python library to represent, analyze, simulate and optimize medium and large-scale quantum circuits at the logical level, with a focus on circuits arising in cryptanalysis.

Release Contributions: First version of the library.

URL: <https://qarton-10b5d8.gitlabpages.inria.fr/>

Contact: Andre Schrottenloher

8 New results

8.1 Secret-Key Cryptography

8.1.1 Proofs of Security of Symmetric Constructions

Participants: André Schrottenloher.

Post-quantum Security of Key-Alternating Feistel Ciphers [12]

Since Kuwakado and Morii’s work [81, 82] it is known that the classically secure 3-round Luby-Rackoff PRP and Even-Mansour cipher become insecure against an adversary equipped with quantum query access. However, while this query model (the so-called Q2 model) has led to many more attacks, it seems that restricting the adversary to classical query access prevents such breaks (the so-called Q1 model). Indeed, at EUROCRYPT 2022, Alagic et al. [38] proved the Q1-security of the Even-Mansour cipher.

In the paper [12], we focus on Feistel ciphers. More precisely, we consider Key-Alternating Feistels built from random functions or permutations and random independent round keys. We borrow the tools used by Alagic et al. and adapt them to this setting, showing that in the Q1 setting: • the 3-round Key-Alternating Feistel, even when the round functions are the same random oracle, is a pseudo-random permutation; • similarly the 4-round KAF is a strong pseudo-random permutation.

8.1.2 Symmetric Cryptanalysis of Primitives and Tools

Simplified Meet-in-the-middle Preimage Attacks on AES-based Hashing [7]

Participants: Mathieu Degré, Patrick Derbez, André Schrottenloher.

The meet-in-the-middle (MITM) attack is a powerful cryptanalytic technique leveraging time-memory tradeoffs to break cryptographic primitives. Initially introduced for block cipher cryptanalysis, it has since been extended to hash functions, particularly preimage attacks on AES-based compression functions. Over the years, various enhancements such as superposition MITM [39] and bidirectional propagations have significantly improved MITM attacks, but at the cost of increasing complexity of automated search models. In this work, we propose a unified mixed integer linear programming (MILP) model designed to improve the search for optimal pre-image MITM attacks against AES-based compression functions. Our model generalizes previous approaches by simplifying both the modeling and the corresponding attack algorithm. In particular, it ensures that all identified attacks are valid. Our framework not only recovers known attacks on AES and Whirlpool but also discovers new attacks with lower memory complexities, and new quantum attacks.

We made the code of our model, and all applications given in the paper, available on the [Inria GitLab platform](#).

New Models for the Cryptanalysis of ASCON. [6]

Participants: Mathieu Degré, Patrick Derbez, André Schrottenloher.

This paper focuses on the cryptanalysis of the ASCON family using automatic tools. We analyze two different problems with the goal to obtain new modelings, both simpler and less computationally heavy than previous works (all our models require only a small amount of code and run on regular desktop computers).

The first problem is the search for Meet-in-the-middle attacks on reduced-round ASCON-Hash. Starting from a previous MILP modeling of Qin et al. (EUROCRYPT 2023), we rephrase the problem in SAT, which accelerates significantly the solving time and removes the need for the “weak diffusion structure” heuristic. This allows us to reduce the memory complexity of Qin et al.’s attacks and to prove some optimality results.

The second problem is the search for lower bounds on the probability of differential characteristics for the ASCON permutation. We introduce a lossy MILP encoding of the propagation rules based on the Hamming weight, in order to find quickly lower bounds which are comparable to the state of the art. We find a small improvement over the existing bound on 7 rounds.

This paper is the full version, published in Design, Codes and Cryptography 2025. A previous version was presented at [WCC 2024](#).

ChiLow and ChiChi: New Constructions for Code Encryption. [13]

Participants: Patrick Derbez.

We study the problem of embedded code encryption, i.e., encryption for binary software code for a secure microcontroller that is stored in an insecure external memory. As every single instruction must be decrypted before it can be executed, this scenario requires an extremely low latency decryption. We present a formal treatment of embedded code encryption security definitions, propose three constructions, namely ACE1, ACE2 and ACE3, and analyze their security. Further, we present ChiLow, a family of tweakable block ciphers and a related PRF specifically designed for embedded code encryption. At the core of ChiLow, there is ChiChi, a new family of non-linear layers of even dimension based on the well-known χ function. Our fully unrolled hardware implementation of ChiLow, using the Nangate 15nm Open Cell Library, achieves a decryption latency of less than 280 picoseconds.

Improved Cryptanalysis of GIFT-64. [8]

Participants: Patrick Derbez, Baptiste Germon.

In this paper, we propose new differential attacks against the block cipher GIFT-64. First we demonstrate how the parallel matching algorithm proposed by Naya-Plasencia at CRYPTO’11 as an advanced list-merging algorithm can be leveraged to enhance differential attacks, overcoming a previously assumed bottleneck. By reducing the complexity of the pairs generation process whenever a non-linear filter is available, this approach enabled us to mount a new differential attack against 25-round GIFT-64 in the related-key setting. Then we use the differential Meet-in-the-Middle cryptanalysis technique introduced by Boura et al. at CRYPTO’23 to improve the differential attacks recently proposed by Chang et al. at CT-RSA’25, leading to the best known attacks against GIFT-64 in the single-key setting, both in terms of number of rounds and of complexity.

Extending the Quasidifferential Framework: From Fixed-Key to Expected Differential Probability. [5]

Participants: Patrick Derbez, Baptiste Germon.

Beyne and Rijmen proposed in 2022 a systematic and generic framework to study the fixed-key probability of differential characteristics. One of the main challenges for implementing this framework is the ability to efficiently handle very large quasidifferential transition matrices (QDTMs) for big (e.g. 8-bit) S-boxes. Our first contribution is a new MILP model capable of efficiently representing such matrices, by exploiting the inherent block structure of these objects. We then propose two extensions to the original framework. First, we demonstrate how to adapt the framework to the related-key setting. Next, we present a novel approach to compute the average expected probability of a differential characteristic that takes the key schedule into account. This method, applicable to both linear and non-linear key schedules, works in both the single-key and related-key settings. Furthermore, it provides a faster way to verify the validity of characteristics compared to computing the fixed-key probability. Using these extensions and our MILP model, we analyze various (related-key) differential characteristics from the literature. First, we prove the validity of several optimal related-key differential characteristics of AES. Next, we show that this approach permits to obtain more precise results than methods relying on key constraints for SKINNY. Finally, we examine the validity of a differential distinguisher used in two differential meet-in-the-middle attacks on SKINNY-128, demonstrating that its probability is significantly higher than initially estimated.

Minimalist Model for Impossible Differentials. [20]

Participants: Patrick Derbez, Marie Euler.

This paper introduces a new MILP modeling to find impossible differential (ID) distinguishers and attacks. Standard models for ID are negative models, in the sense that a differential is impossible if and only if the model has no solution. Our new modelling technique focuses on probable ID, differentials that are probably impossible. While this might lead to false positives, the main advantage is that searching for such probable ID can be achieved through a positive model. This facilitates the search for the best impossible differential attacks without first exhausting all possible ID distinguishers on a target. We also propose to simplify the modelling by only considering two possible states for internal cells: inactive and unknown. In this case there are no longer direct contradictions but only indirect ones, assuming that it is impossible that all cells are inactive.

With these two simple ideas, we are able to retrieve the longest impossible differentials distinguishers on MIDORI, SKINNY, PRESENT, SIMON, Simeck and SPECK. Furthermore, as the model looking for candidates is based on satisfiability, it can be incorporated in a larger model which looks directly for the best attacks in order to enumerate the distinguishers in the order of the complexity of the associated attacks, which we did for the AES, ARADI, SIMON and SKINNY.

SPEEDY: Caught at Last. [14]

Participants: Patrick Derbez, Baptiste Germon.

SPEEDY is a family of ultra-low-latency block ciphers designed by Leander et al. in 2021. In 2023, Boura et al. proposed a differential attack on the full 7-round variant, SPEEDY-7-192. However, shortly thereafter, Beyne and Neyt demonstrated that this attack was invalid, as the dominant differential characteristic it relied upon had probability zero. A similar issue affects another differential attack proposed the same year by Wang et al., which also targets SPEEDY-7-192 and suffers from the same flaw. As a result, the question of finding a valid attack on this cipher remained an open problem. In this work, we resolve this problem by presenting the first valid differential attack on SPEEDY-7-192. We verify the validity of our distinguisher using the quasidifferential framework. Moreover, our search for the differential distinguisher is significantly

more rigorous than in previous works: starting from a pool of one-round trails, our method explores a larger portion of the search space. We also fully exploit probabilistic extensions of the distinguisher to identify optimal parameters for the key recovery step. Our best attack on SPEEDY-7-192 is a chosen-ciphertext attack with data and time complexity $2^{174.53}$. In addition, we present differential attacks on 4-round SPEEDY-5-192 and 5-round SPEEDY-6-192, which currently represent the best known attacks against these smaller variants.

8.1.3 Quantum Cryptanalysis

Faster Quantum Algorithms for MQ2 and Applications. [9]

Participants: Pierre-Alain Fouque, André Schrottenloher.

In this work, we study quantum algorithms for multivariate quadratic Boolean equation systems by focusing on their precise gate count. While better asymptotic algorithms are known, currently gate counts were only computed for exhaustive search and a variant of Grover’s search using preprocessing [92]. This limits the applicability of Boolean equation solving to cryptanalysis, which considers relatively small numbers of variables (from 40 to 200) and is concerned with the exact complexity of the solver.

In this paper, we introduce two new quantum algorithms: an optimized quantum exhaustive search, which amortizes the cost of polynomial evaluation, and a simple linearization strategy based on [52]. We apply these algorithms to the cryptanalysis of the block ciphers LowMC and RAIN in the single-data setting, which is important in the context of post-quantum digital signatures based on MPC-in-the-head. This allows us to adapt existing classical attacks into the first quantum cryptanalysis results on these ciphers.

We implemented the main building blocks of the circuits presented in this paper, and published this implementation on the [Inria Gitlab platform](#).

Improved Quantum Linear Attacks and Application to CAST. [4]

Participants: André Schrottenloher.

This paper studies quantum linear key-recovery attacks on block ciphers. The first such attacks were last-rounds attacks proposed by Kaplan et al. [77], which combine a linear distinguisher with a guess of a subkey. More recently, the framework which we introduced in [95] uses a quantum *convolution algorithm* to compute a so-called *correlation state*, which is a superposition of subkey candidates where the amplitudes are linear correlations. The main limitation of this approach is that, while the good subkey has the highest correlation, it is not *marked* in the state, and cannot be found immediately by quantum search.

In this paper, we combine the correlation state with a distinguisher, which recognizes the good subkey. From here, we can use quantum search to recover this key. We apply this idea to Feistel ciphers, notably the CAST-128 and CAST-256 ciphers, using two kinds of distinguishers: quantum distinguishers based on Simon’s algorithm [81] and linear distinguishers. The resulting attacks outperform the previous quantum attacks.

8.2 Public-key cryptography

8.2.1 Lattices

Assessing the Impact of a Variant of MATZOV’s Dual Attack on Kyber [15]

Participants: Charles Meyer-Hilfiger, Yixin Shen.

The dual attacks on the Learning With Errors problem are currently a subject of controversy. In particular, the results of [85], which claim to significantly lower the security level of Kyber [96], a lattice-based cryptosystem currently being standardized by NIST, are not widely accepted. The analysis behind their attack depends on a series of assumptions that, in certain scenarios, have been shown to contradict established theorems or well-tested heuristics [68].

In this paper, we introduce a new dual lattice attack on LWE, drawing from ideas in coding theory. Our approach revisits the dual attack proposed by [85], replacing modulus switching with an efficient decoding algorithm. This decoding is achieved by generalizing polar codes over Z_q , and we confirm their strong distortion properties through benchmarks. This modification enables a reduction from small-LWE to plain-LWE, with a notable decrease in the secret dimension. Additionally, we replace the enumeration step in the attack by assuming the secret is zero for the portion being enumerated, iterating this assumption over various choices for the enumeration part.

We make an analysis of our attack without using the flawed independence assumptions used in [85] and we fully back up our analysis with experimental evidence.

Lastly, we assess the complexity of our attack on Kyber; showing that the security levels for Kyber-512/768/1024 are 3.5/11.9/12.3 bits below the NIST requirements (143/207/272 bits) in the same nearest-neighbor cost model as in [96, 85]. All in all the cost of our attack matches and even slightly beat in some cases the complexities originally claimed by the attack of [85].

Discrete gaussian sampling for BKZ-reduced basis [28]

Participants: Yixin Shen.

Discrete Gaussian sampling on lattices is a fundamental problem in lattice-based cryptography. In this paper [28], we revisit the Markov chain Monte Carlo (MCMC)-based Metropolis-Hastings-Klein (MHK) algorithm proposed by Wang and Ling and study its complexity under the Geometric Series Assumption (GSA) when the given basis is BKZ-reduced. We give experimental evidence that the GSA is accurate in this context, and we give a very simple approximate formula for the complexity of the sampler that is accurate over a large range of parameters and easily computable. We apply our results to the dual attack on LWE of [91] and significantly improve the complexity estimates of the attack. Finally, we provide some results of independent interest on the Gaussian mass of a random q -ary lattices.

A reduction from Hawk to the principal ideal problem in a quaternion algebra [19]

Participants: Clémence Chevignard.

In this article we present a non-uniform reduction from rank-2 module-LIP over Complex Multiplication fields, to a variant of the Principal Ideal Problem, in some fitting quaternion algebra. This reduction is classical deterministic polynomial-time in the size of the inputs. The quaternion algebra in which we need to solve the variant of the principal ideal problem depends on the parameters of the module-LIP problem, but not on the problem's instance. Our reduction requires the knowledge of some special elements of this quaternion algebras, which is why it is non-uniform. In some particular cases, these elements can be computed in polynomial time, making the reduction uniform. This is the case for the Hawk signature scheme: we show that breaking Hawk is no harder than solving a variant of the principal ideal problem in a fixed quaternion algebra (and this reduction is uniform).

Ideally HAWKward: How Not to Break Module-LIP [30]

Participants: Clémence Chevignard.

The module-Lattice Isomorphism Problem (module-LIP) was introduced by Ducas et al. in [67], and used within the signature scheme and NIST candidate HAWK. In [88], Mureau et al. pointed out that over certain number fields F , the problem can be reduced to enumerating solutions of $x^2 + y^2 = q$ where $q \in \mathcal{O}_F$ is given and $x, y \in \mathcal{O}_F$ are the unknowns). Moreover one can always reduce to a similar equation which has only few solutions. This key insight led to a heuristic polynomial-time algorithm for solving module-LIP on those specific instances. Yet this result doesn't threaten HAWK for which the problem can be reduced to enumerating solutions of $x^2 + y^2 + z^2 + t^2 = q$ (where $q \in \mathcal{O}_F$ is given and $x, y, z, t \in \mathcal{O}_F$ are the unknowns). We show that, in all likelihood, solving this equation requires the enumeration of a too large set to be feasible, thereby making irrelevant a straightforward adaptation of the approach in [88].

Share the MAYO: Thresholdizing-MAYO [16]

Participants: Guilhem Niot.

Threshold cryptography is a growing field that allows multiple parties to jointly perform cryptographic operations without exposing their individual secret shares. In this paper, we present the first comprehensive study on thresholdizing practical OV-based signature schemes, specifically focusing on MAYO and UOV, which are candidates in the NIST process for standardization of additional digital signature schemes. Our approach begins by addressing the challenges associated with thresholdizing algorithms that sample solutions to linear equation systems of the form $\mathbf{Ax} = y$, which are fundamental to OV-based signature schemes. Previous attempts have introduced levels of leakage that we deem insecure. We propose a novel minimum-leakage solution and assess its practicality. Furthermore, we explore the thresholdization of the entire functionality of these signature schemes, demonstrating their unique applications in networks and cryptographic protocols.

Finally! A Compact Lattice-Based Threshold Signature [27]

Participants: Guilhem Niot.

Threshold signatures split trust among parties, requiring T of N to sign. While common in pre-quantum cryptography, post-quantum threshold schemes remain heavy, with signature sizes an order of magnitude larger than standard PQ signatures.

We propose a novel, highly efficient threshold signature scheme with sizes close to a standard ML-DSA signature for $T \leq 8$. Our construction relies on well-studied assumptions (MLWE and SelfTargetMSIS) and avoids heavy machinery, essentially running T parallel Dilithium executions. Despite its simplicity, achieving this required overcoming technical hurdles like small share distribution and rejecting transcript simulation, delivering a previously out-of-reach efficiency.

Efficient Threshold ML-DSA [17]

Participants: Guilhem Niot.

In this paper, we present the first threshold signature scheme fully compatible with the NIST-standardized ML-DSA. While existing lattice-based threshold solutions either lack practicality or standard compliance, our approach supports secure and efficient production of ML-DSA-compatible signatures for small groups, requiring under 1 MB of communication per party for up to 6 signers. We leverage advanced short secret sharing and optimized rejection sampling to achieve a practical balance between communication efficiency and number of rounds required to output a valid signature. We implement our construction in Go and provide benchmarks across LAN/WAN settings to demonstrate practical deployability for applications such as cryptocurrency wallets, threshold TLS, and Tor directory authorities.

Unmasking TRaccoon: A Lattice-Based Threshold Signature with An Efficient Identifiable Abort Protocol [26]

Participants: Guilhem Niot.

TRaccoon is an efficient 3-round lattice-based threshold signature, recently introduced by del Pino et al. [90]. While the design resembles the classical threshold Schnorr signature Sparkle, it lacks a means to identify malicious behavior—a property of interest in practice. This limitation stems from TRaccoon’s use of masking to resist lattice-specific attacks, which blinds partial signatures with one-time additive masks. del Pino et al. left the addition of an identification mechanism as an open problem.

In this work, we propose TRaccoon-IA, which extends TRaccoon with an efficient identifiable abort protocol to identify malicious signers when the protocol fails. This simple add-on preserves the original design and incurs an added communication cost of $60 + 6.4|T|$ KB only in the event of a failure. Additionally, we provide the first formal security analysis of a zero-knowledge variant of LaBRADOR and introduce a new game-based definition for interactive identifiable abort protocols, extending standard unforgeability definitions.

Practical Deniable Post-Quantum X3DH: A Lightweight Split-KEM for K-Waay [24]

Participants: Guilhem Niot.

The Signal Protocol faces the challenge of migrating to a post-quantum world while preserving critical properties such as asynchrony and deniability. While PQXDH grants post-quantum confidentiality, full migration of the X3DH handshake remains elusive. K-Waay [60] offers a path via split KEMs but suffers from size limitations compared to ring signature-based approaches.

This work introduces Sparrow-KEM and Sym-Sparrow-KEM, novel asymmetric and symmetric split KEMs designed to optimize K-Waay. Leveraging the MLWE assumption, we reduce communication by $5.1\times$ and improve speed by $40\times$ over prior split KEMs. Sym-Sparrow-KEM is the first symmetric split-KEM to offer deniability along with strong implicit authentication properties (IND-1KCA, IND-1BatchCCA). Our results demonstrate the feasibility of a compact, deniable post-quantum X3DH based on split KEMs.

8.2.2 Elliptic curves and isogenies

Participants: Aurore Guillevic.

An algebraic point of view on the generation of pairing-friendly curves The paper [11] with Jean Gasnier from the CANARI Team (Bordeaux) is the achievement of Jean Gasnier’s Masters internship in 2022 co-advised in Bordeaux by Jean-Marc Couveignes and remotely from Denmark by Aurore Guillevic, and Gasnier’s PhD thesis defended in Bordeaux in July 2025. It aims to generalize The Kachisa–Schaefer–Scott technique to find new parameterized families of pairing-friendly curves. The method allowed to obtain new curves for interesting embedding degrees, such as $k = 20$. It comes with two implementations, one written by Jean Gasnier to obtain new curve families (see [Subfield Method Gitlab Project](#)), the other one to implement pairings on the new curves, see [Pairings on Gasnier–Guillevic Curves Gitlab Project](#). Finally the paper is published in the journal SIAGA.

Participants: Pierrick Dartois.

qt-Pegasis: Simpler and Faster Effective Class Group Actions The paper [36] by Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi, and Frederik Vercauteren, revisits the recent Pegasis algorithm that computes an effective group action of the class group of any imaginary quadratic order R on a set of supersingular elliptic curves primitively oriented by R . Although Pegasis was the first algorithm showing the practicality of computing unrestricted class group actions at higher security levels, it is complicated and prone to failures, which leads to many rerandomizations.

In this work, we present a new algorithm, qt-Pegasis, which is much simpler, but at the same time faster and removes the need for rerandomization of the ideal we want to act with, since it never fails. It leverages the main technique of the recent Qlapoti approach. However, Qlapoti solves a norm equation in a quaternion algebra, which corresponds to the full endomorphism ring of a supersingular elliptic curve. We show that the algorithm still applies in the quadratic setting, by embedding the quadratic ideal into a quaternion ideal using a technique similar to the one applied in KLaPoTi. This way, we can reinterpret the output of Qlapoti as four equivalent quadratic ideals, instead of two equivalent quaternion ideals. We then show how to construct a Clapoti-like diagram in dimension 2, which embeds the action of the ideal in a 4-dimensional isogeny. We implemented our qt-Pegasis algorithm in SageMath for the CSURF group action, and we achieve a speedup over Pegasis of $1.8\times$ for the 500-bit parameters and $2.6\times$ for the 4000-bit parameters.

8.2.3 Quantum Cryptanalysis

Improved Classical and Quantum Algorithms for the Shortest Vector Problem via Bounded Distance Decoding [3]

Participants: Yixin Shen.

The most important computational problem on lattices is the Shortest Vector Problem (SVP). In this paper, we present new algorithms that improve the state-of-the-art for provable classical/quantum algorithms for SVP. We present the following results.

1. A new algorithm for SVP that provides a smooth tradeoff between time complexity and memory requirement. For any positive integer $4 \leq q \leq \sqrt{n}$, our algorithm takes $q^{13n+o(n)}$ time and requires $\text{poly}(n) \cdot q^{16n/q^2}$ memory. This tradeoff which ranges from enumeration ($q = \sqrt{n}$) to sieving (q constant), is a consequence of a new time-memory tradeoff for Discrete Gaussian sampling above the smoothing parameter.
2. A quantum algorithm for SVP that runs in time $2^{0.950n+o(n)}$ and requires $2^{0.5n+o(n)}$ classical memory and $\text{poly}(n)$ qubits. In Quantum Random Access Memory (QRAM) model this algorithm takes only $2^{0.835n+o(n)}$ time and requires a QRAM of size $2^{0.293n+o(n)}$, $\text{poly}(n)$ qubits and $2^{0.5n}$ classical space. This improves over the previously fastest classical (which is also the fastest quantum) algorithm due to [37] that has a time and space complexity $2^{n+o(n)}$.
3. A classical algorithm for SVP that runs in time $2^{1.669n+o(n)}$ time and $2^{0.5n+o(n)}$ space. This improves over an algorithm of [57] that has the same space complexity.

The time complexity of our classical and quantum algorithms are obtained using a known upper bound on a quantity related to the lattice kissing number which is $2^{0.402n}$. We conjecture that for most lattices this quantity is a $2^{o(n)}$. Assuming that this is the case, our classical algorithm runs in time $2^{1.292n+o(n)}$, our quantum algorithm runs in time $2^{0.750n+o(n)}$ and our quantum algorithm in QRAM model runs in time $2^{0.667n+o(n)}$. As a direct application of our result, using the reduction in [66], we obtain a provable quantum algorithm for the Lattice Isomorphism Problem in the case of the trivial lattice Z^n (ZLIP) that runs in time $2^{0.417n+o(n)}$. Our algorithm requires a QRAM of size $2^{0.147n+o(n)}$, $\text{poly}(n)$ qubits and $2^{0.25n}$ classical space.

A Tight Quantum Algorithm for Multiple Collision Search. [34]

Participants: André Schrottenloher, Yixin Shen.

Searching for collisions in random functions is a fundamental computational problem, with many applications in symmetric and asymmetric cryptanalysis. When one searches for a *single* collision, the known quantum algorithms match the query lower bound. This is not the case for the problem of finding *multiple* collisions, despite its regular appearance as a sub-component in sieving-type algorithms.

At EUROCRYPT 2019, Liu and Zhandry gave a query lower bound $\Omega(2^{m/3+2k/3})$ for finding 2^k collisions in a random function with m -bit output. In a previous paper at EUROCRYPT 2023 [48], we gave a quantum algorithm matching this bound for a large range of m and k , but not all admissible values. This quantum algorithm was based on the MNRS quantum walk framework, with the novelty that walks could be *chained* by reusing the state after outputting a collision.

In this paper, we give a new algorithm that tackles the remaining non-optimal range, closing the problem. Our algorithm is tight (up to a polynomial factor) in queries, and also in time under a quantum RAM assumption. The idea is to extend the chained walk to a regime in which several collisions are returned at each step, and the “walks” themselves contain a single diffusion step.

Reducing the Number of Qubits in Quantum Factoring. [18]

Participants: Clémence Chevignard, Pierre-Alain Fouque, André Schrottenloher.

This paper focuses on the optimization of the number of logical qubits in quantum algorithms for factoring and computing discrete logarithms in \mathbb{Z}_N^* . These algorithms contain an exponentiation circuit modulo N , which is responsible for most of their cost, both in qubits and operations.

In this paper, we show that using only $o(\log N)$ work qubits, one can obtain the least significant bits of the modular exponentiation output. We combine this result with May and Schlieper’s truncation technique (ToSC 2022) and the Ekerå-Håstad variant of Shor’s algorithm (PQCrypto 2017) to solve the discrete logarithm problem in \mathbb{Z}_N^* using only $d + o(\log N)$ qubits, where d is the bit-size of the logarithm. Consequently we can factor n -bit RSA moduli using $n/2 + o(n)$ qubits, while current envisioned implementations require about $2n$ qubits.

Our algorithm uses a Residue Number System and succeeds with a parametrizable probability. Being completely classical, we have implemented and tested it. For RSA factorization, we can reach a gate count $O(n^3)$ for a depth $O(n^2 \log^3 n)$, which then has to be multiplied by $O(\log n)$ (the number of measurement results required by Ekerå-Håstad). To factor an RSA-2048 instance, we estimate that 1730 logical qubits and 2^{36} Toffoli gates will suffice for a single run, and the algorithm needs on average 40 runs. To solve a discrete logarithm instance of 224 bits (112-bit classical security) in a safe-prime group of 2048 bits, we estimate that 684 logical qubits would suffice, and 20 runs with 2^{32} Toffoli gates each.

Our estimations are supported by a full implementation available on the [Inria Gitlab platform](#). This work was presented as a plenary talk in the QIP 2025 conference [29] and published in the proceedings of CRYPTO 2025 [18]. After our work was initially made public in 2024, Gidney [72] performed an extensive estimate of physical estimates for breaking RSA keys, combining an optimized version of our algorithm with up-to-date techniques in error correction. His new estimate of a million physical qubits (down from 20 million in an earlier work [73]) received significant attention.

8.2.4 Protocols

Comprehensive Deniability Analysis of Signal Handshake Protocols: X3DH, PQXDH to Fully Post-Quantum with Deniable Ring Signatures [31]

Participants: Guilhem Niot.

The Signal protocol relies on a handshake (formerly X3DH, now PQXDH) to set up secure conversations, valuing *deniability* so users can deny participation. Prior analyses use varying, ad-hoc models that obscure guarantees and prevent comparison.

Building on the abstraction by Hashimoto et al. [74], we present a unified framework for analyzing Signal handshake deniability. We examine X3DH and PQXDH, clarifying PQXDH’s deniability against *harvest-now-judge-later* quantum adversaries. We also analyze post-quantum alternatives like RingXKEM that use ring signatures. By introducing a deniability metric inspired by differential privacy, we offer relaxed, pragmatic guarantees. This metric further allows us to define *deniable ring signatures* (a relaxation of anonymity), enabling efficient constructions from the NIST standard Falcon and the candidate for standardization MAYO, which are deniable despite not being fully anonymous.

Revisiting PQ WireGuard: A Comprehensive Security Analysis With a New Design Using Reinforced KEMs [22]

Participants: Guilhem Niot.

WireGuard is a high-performance VPN based on the Noise protocol. A recent post-quantum (PQ) variant was proposed by Hülsing et al. [75], however since Wireguard requires the handshake message to fit in one UDP packet of size roughly 1200 B, they rely on Classic McEliece, whose large public keys significantly increase server memory requirements and complicates kernel-level deployment.

In this work, we revisit PQ WireGuard to improve its design, security, and efficiency. We address binding issues in PQ KEMs and prove security in a new computational model. We introduce ‘reinforced KEM’ (RKEM) and a construction named ‘Rebar’ to compress ML-KEM-like ciphertexts. This enables a PQ WireGuard protocol where the server avoids storing large keys, reducing public key memory usage by 190 to 390×.

Subversion-resilient Key-exchange in the Post-quantum World [21]

Participants: Pierre-Alain Fouque, Guilhem Niot.

Subversion-resilient Authenticated Key-Exchange (AKE) ensures security even when parts of the protocol implementation are tampered with. One way to achieve AKE is by using Reverse Firewalls (RFs) to restore security.

In this work, we extend RF-based subversion resilience in security definitions, constructions, and formal verification. First, we introduce a useful relaxation of the notion of security in subversion-resilient AKE with RFs: the goal is no longer to prevent all exfiltration, but rather to restore to the AKE protocol a property lost upon subversion. We focus specifically on authenticating and (key-)securing RFs, and consider a spectrum of compromises, designing a framework in which adversaries can tamper with some components of the implementation but perhaps not others. Aiming for post-quantum security, we define ‘re-randomizable Key Encapsulation Mechanisms’, providing instantiations based on classical Diffie-Hellman and Kyber. Finally, we establish foundations for the formal verification of RF-based protocols, proving our construction secure using the CryptoVerif prover, in addition to computational-security proofs in usual Bellare-Rogaway methodology.

8.3 Side-Channel Attacks

Avengers assemble! Supervised learning meets lattice reduction [10]

Participants: Pierre-Alain Fouque, Damien Marion, Quyen Nguyen, Alexandre Wallet.

In this work, we attack Kyber’s key-generation algorithm using power analysis and lattice reduction. More specifically, we target the Centered Binomial Distribution (CBD) sampler which generates the secret data of

the underlying Learning With Error (LWE) instance. From a side-channel perspective, our attack uses a single trace, leveraging classifiers developed through supervised learning. We assess the block-size in lattice reduction that would complete the key recovery, providing a fine-grained trade-offs between the correctly guessed proportion and the block-size, based on standard estimates. Finally, we conducted large-scale experiments, from power traces to secret key recovery (for most of the instances) under a threshold of 18 hours, targeting all three Kyber's security levels. Our average rate of success across all security level is more than 96%.

On the Success Rate of Simple Side-Channel Attacks Against Masking with Unlimited Attack Traces [23]

Participants: Aymeric Hiltenbrand, Julien Eynard, Romain Poussier.

In this work, we investigate how the masking countermeasure affects the success rate of simple attacks. To this end, we provide theoretical, simulated, and practical experiments. Interestingly, we will see that masking can allow us to asymptotically recover more information on the secret than in the case of an unprotected implementation, depending on the masking type. We will see that this is true for masking encodings that add non-linearity with respect to the leakages, such as arithmetic masking, while it is not for Boolean masking. We believe this context provides interesting results, as the average information of arithmetic encoding is proven less informative than the Boolean one.

GnuZero: A Compiler-Based Zeroization Static Detection Tool for the Masses [25]

Participants: Pierre-Alain Fouque, Pierrick Philippe.

Coding standards for secure programming recommend "scrubbing" sensitive data once it is no longer needed; otherwise, secrets may be recovered, as illustrated in the Heartbleed attack. Despite being an effective software-based countermeasure, zeroization, i.e., overwriting with zeroes, turns out to be challenging and error-prone. Current verification approaches suffer from scalability or precision issues when applied to production software in practice. In this paper, we put forward the GCC Static Analyzer (GSA), which is a symbolic execution engine for error finding. Specifically, we extend the GSA to build GnuZero; our automated tool that detects missing zeroization for all stack/heap variables storing sensitive data, either directly or by derivation. Our experiments confirm GnuZero efficiency and effectiveness in verifying real-world benchmarks. In particular, GnuZero passes all the relevant Juliet's test programs, namely associated to the MITRE's CWE-244 and CWE-226. In addition, GnuZero succeeds in identifying new vulnerabilities in open-source cryptographic modules.

9 Bilateral contracts and grants with industry

9.1 Bilateral Grants with Industry

- **Resque:** (T0: 09/2022 → 08/2026)
BPi France project.
Led by Thales.

Participants: Pierre-Alain Fouque, Guilhem Niot, Daniel De Almeida Braga, Damien Marion, Gaël Claudel.

Participating entities on the industrial side: Thales SIX and DIS, TheGreenBow, CryptoExperts, CryptoNext. Participating entities on the public side: Inria, ANSSI.

In this project, Inria is represented by two teams: Capsule (Inria Rennes), with Pierre-Alain Fouque as the coordinator; and Cascade (Inria Paris), with Céline Chevalier as collaborator.

Resque project, "Résilience Quantique" aims at combining two use-cases allowing the construction of two software and hardware components: i) VPN [virtual private network] hybrid and agile and a HSM [hardware security module] robust and efficient, providing the security of exchanged information. The cryptographic agility will allow to perform regular and continuous updates of the post-quantum algorithms.

- **Ascon-CAT:** (T0: 10/2024 → 09/2027)

Participants: André Schrottenloher, Aurel Pichollet–Mugnier.

AID "RAPID" project.

Coordinated by Alice&Bob.

Industrial partners: Alice&Bob, Thales SIX. Academic partners: Inria.

The goal of this project is to perform an integrated quantum security analysis of the lightweight symmetric primitive ASCON, recently selected as a NIST standard. The project will combine the development and analysis of new quantum algorithms, as well as a precise estimation of the resources needed to run them, and a study of implementations in the "cat qubits" platform which is developed by Alice&Bob.

10 Partnerships and cooperations

10.1 International initiatives

10.1.1 Visits to international teams

Research stays abroad

Patrick Derbez

Visited institution: Nanyang Technological University (NTU)

Country: Singapore

Dates: 14/12/2025 – 17/12/2025

Context of the visit: Collaboration with Prof. Thomas Peyrin on two particular topics: automated cryptanalysis and cryptanalysis of deep neural networks. I was also invited to give a talk on a recent submitted paper about the cryptanalysis of deep neural networks with non-linear activation functions.

Mobility program/type of mobility: research stay

André Schrottenloher

Visited institution: NTT Social Informatics Laboratories

Country: Japan

Dates: 25 – 29 September 2025

Context of the visit: Visiting Akinori Hosoyamada, who is a regular collaborator on the topic of quantum symmetric cryptanalysis.

10.2 National initiatives

- **The PQTLS** (01/2022 → 12/2027)

Participants: Alexandre Wallet, Pierre-Alain Fouque, André Schrottenloher, Yixin Shen, Clémence Chevignard, Damien Marion.

Post-quantum padlock for web browser

PEPR Quantique

Partners: GREYC (Caen), ENS Lyon, Inria GRACE, Inria Cosmiq, Inria Prosecco, Inria Caramba, Inria Lfant, Inria Capsule, UVSQ, Cryptis, ARCAD, SESAM, CEA LETI, University of Rouen, Rennes, Bordeaux.

The famous "padlock" appearing in browsers when one visits websites whose address is preceded by "https" relies on cryptographic primitives that would not withstand a quantum computer. This integrated project aims to develop in 5 years post-quantum primitives in a prototype of "post-quantum lock" that will be implemented in an open source browser. The evolution of cryptographic standards has already started, the choice of new primitives will be made quickly, and the transition will be made in the next few years. The objective is to play a driving role in this evolution and to make sure that the French actors of post-quantum cryptography, already strongly involved, are able to influence the cryptographic standards of the decades to come.

- **Cryptanalyse** (12/2023 → 12/2028)

Participants: Patrick Derbez, Aurore Guillevic, André Schrottenloher.

PEPR Cybersécurité

Partners: Inria GRACE, Inria Cosmiq, Almasty, Inria Caramba, Inria Lfant, Inria Capsule, Crypto, Eco, Canari, UGA.

The Cryptanalyse project focuses on the study and standardization of cryptographic primitives. Modern cryptography has become an indispensable tool for securing personal, commercial and institutional communications. This project will provide an estimate of the difficulties involved in solving the underlying problems, and deduce the level of security conferred by the use of these primitives. The aim is to evaluate the security of cryptographic algorithms.

- **CROWD** (2023 → 2027).

Participants: Pierre-Alain Fouque, André Schrottenloher, Clémence Chevignard.

Code-based practical cryptography

ANR-DFG

Partners: TU Munich, IRMAR (Rennes), Inria (Rennes)

The aim of this project is the examination of skew metrics and their application in cryptography. These metrics can be considered as a generalization of the so-called rank metric, which has significant applications in coding theory, cryptography, data storage, and network coding. The connection of these metrics lies in the non-commutativity of Euclidean rings, called Ore rings, which extend the classical notation of commutative polynomial rings by 'skewing' (twisting) multiplication. These operations allow the development of metrics and new codes with efficient arithmetic operations. This holds promise for secure and efficient cryptographic implementations. Three avenues are explored:

1) investigates the foundations of algebraic codes in these skew-metrics; 2) design novel decoding algorithms and cryptographic schemes from these codes, and assess their security from a cryptanalytic and side-channel point of view; 3) produce practically efficient implementation of core cryptographic primitive, such as digital signatures.

- **ANR IDROMEL** (2021 → 2025)

Participants: Damien Marion.

Improving the Design of secure systems by a Reduction Of Micro-architectural Effects on side-channel Attacks

Partners: LAAS-CNRS, LIP6, CEA, ARM, IRISA

The IDROMEL project aims to contribute to the design of secure systems against side-channel attacks based on power and electromagnetic observations, for a wide range of computing systems (from IoT devices to mobile phones). IDROMEL will investigate the impact of the processor micro-architecture on power and electromagnetic side-channel attacks as a key concern for the design of secure systems.

- **ANR OREO** (2023 → 2026)

Participants: Patrick Derbez, Andre Schrottenloher.

MILP for Cryptography

Partners: Univ Rennes, UVSQ, Loria

In symmetric-key cryptography, a popular technique for proving resistance against classical attacks is to model the behaviour of the cipher as a Mixed Integer Linear Programming (MILP) problem and solve it by some MILP solver. This method was applied for the first time by Mouha et al. [MWGP11] and by Wu and Wang [WW11] for finding the minimum number of differentially and linearly active Sboxes and provides in such a way a proof of resistance against these two classical attacks. Since then, the use of MILP not only by designers but also by cryptanalysts has increased, the advantage being that many cryptanalytic problems are relatively easy to translate into linear constraints (typically on bits) and available solvers (e.g. Gurobi, CPLEX) are most often very efficient to solve them.

Currently, MILP solvers are mainly used for differential cryptanalysis, including the search for sophisticated boomerang distinguishers, and for integral cryptanalysis by exhausting division trails on a cipher. But we are reaching a point where describing the problem into a MILP model and solving it naively is not enough. Thus there are many open problems related to MILP applied to cryptography and the aim of this new ANR project is to tackle them. Our main objective is to handle more complex cryptographic problems, relying on both a theoretical work on cryptanalysis techniques and an improvement of MILP models. The project is composed of 4 axis: handling more complex cryptographic problems using MILP solvers, automatically searching for key-recovery attacks, side-channels cryptanalysis and conception of cryptographic primitives.

- ANR JCJC QATS (2025 → 2029): *Quantum Attacks and new Tools for Symmetric Cryptanalysis*

Participants: Alisée Lafontaine, Andre Schrottenloher.

Nowadays, symmetric cryptanalysis relies heavily on automatic tools. These tools model the search for an attack as an optimization problem, which is solved using off-the-shelf solvers. Regarding quantum security, at the moment, only a few quantum attacks have been integrated into such tools. Besides,

significant human effort is still required to determine precisely the complexity of the attack, especially in the quantum setting.

The goal of the ANR JCJC QATS project is to synthesize a single toolchain to output fully specified quantum attack algorithms, and their complexities. Primitives such as block ciphers and hash functions will be analyzed, starting from well-established designs and moving towards more recent ones. This toolchain is expected to simplify the study of quantum attacks, especially the computation of their complexity. We aim to produce a toolbox where the quantum security of a primitive can be estimated with only basic knowledge of symmetric cryptanalysis and quantum algorithms. This would be helpful for designers of new algorithms, and more generally, cryptographers interested in quantum security estimates.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

- Patrick Derbez co-organized the [1st Workshop on Symmetric-key Cryptanalysis Automation and Modelling](#). This workshop was held at Università degli Studi Roma Tre, Rome, Italy, the 15th of March 2025.

Member of the organizing committees

Participants: Aurore Guillevic, Damien Marion, André Schrottenloher, Yixin Shen.

- [Séminaire CRYPTO](#) (IRMAR, IRISA, Rennes): Aurore Guillevic and Damien Marion until September 2025, André Schrottenloher, Yixin Shen.

11.1.2 Scientific events: selection

Chair of conference program committees

Participants: Pierre-Alain Fouque, André Schrottenloher.

- [EUROCRYPT 2025](#): Pierre-Alain Fouque (Program co-chair)
- [EUROCRYPT 2025 artifact evaluation committee](#): André Schrottenloher
- [FSE 2025 artifact evaluation committee](#): Patrick Derbez

Member of the conference program committees

Participants: Daniel de Almeida Braga, Patrick Derbez, Aurore Guillevic, André Schrottenloher, Yixin Shen.

- [SAC 2025](#) (August 11–15, 2025, Toronto, Canada): Patrick Derbez, Aurore Guillevic, André Schrottenloher
- [EUROCRYPT 2025 artifact evaluation committee](#): Daniel De Almeida Braga
- [ASIACRYPT 2025](#) (December 8-12, Melbourne, Australia): Patrick Derbez, André Schrottenloher

- **INDOCRYPT 2025** (December 14th-17th, Odisha, India): Yixin Shen
- **IWSEC 2025** (November 25-27, Fukuoka, Japan): André Schrottenloher
- **QUEST-IS 2025** (December 1st-4th, Saclay, France): André Schrottenloher

Reviewer The team members regularly serve as sub-reviewers for the IACR conferences. For anonymity reasons, the details are not provided.

11.1.3 Journal

Member of the editorial boards

Participants: Patrick Derbez, André Schrottenloher.

- *Transactions on Symmetric Cryptology (ToSC)* **associate editor:** Patrick Derbez, André Schrottenloher

Reviewer - reviewing activities Team members regularly review papers submitted to international journals such as Designs, Codes, and Cryptography (DCC), Finite Fields and their Applications (FFA), Journal of Cryptology. For anonymity reasons, the details are not provided.

11.1.4 Invited talks

Participants: Clémence Cheviguard, Pierrick Dartois, Patrick Derbez, Pierre-Alain Fouque, André Schrottenloher, Yixin Shen.

- Pierre-Alain Fouque - *Quantum Factoring* - **Tavares Lecture at SAC 2025**, Toronto, Canada, August 2025.
- André Schrottenloher - *Reducing the Number of Qubits in Quantum Factoring* - **Séminaire de sécurité du LORIA**, Nancy, France, April 2025.
- André Schrottenloher - *La cryptographie à l'épreuve du calcul quantique* - **Journée des sciences et technologies quantiques de Rennes**, Rennes, France, May 2025
- André Schrottenloher - *Reducing the Number of Qubits in Quantum Factoring* - **Quantum Summer Cluster Workshop**, Simon's Institute for the Theory of Computing, Berkeley, USA, July 2025
- Clémence Cheviguard - *Reducing the Number of Qubits in Quantum Factoring* - **Quantum Innovation 2025**, Osaka, July 2025
- André Schrottenloher - *Quantum Attacks on Symmetric Constructions* - **1st Workshop on Generic Attacks and Proofs in Symmetric Cryptography (GAPS 2025)** - NTU Singapore, September 2025
- André Schrottenloher - *Convolution-Based Quantum Cryptanalysis* - **20th Anniversary of the CWI Cryptology Group**, Amsterdam, Netherlands, September 2025
- André Schrottenloher - *Convolution-based Quantum Cryptanalysis* - **Dagstuhl Seminar 25431: Quantum Cryptanalysis** - Schloss Dagstuhl, Germany, October 2025
- Yixin Shen - *Finding many Collisions via Quantum Walks* - **2nd Workshop on Quantum Computing and Quantum Information Theory (SUQUNET Workshop)** - Sabancı Üniversitesi, Istanbul, Turkey, 2025
- Pierrick Dartois - *What you need to know about higher dimensional isogenies* - **Leuven Isogeny Days 6** - KU Leuven, Belgium, September 2025

- Pierrick Dartois - *An introduction to SQIsign* - **Journée du PEPR PQ-TLS** - Paris, France, December 2025
- Patrick Derbez - *Cryptanalytic Extraction of Deep Neural Networks with Non-Linear Activations* - **NTU Seminars**, NTU, Singapore, December 2025

11.1.5 Scientific expertise

Participants: Pierre-Alain Fouque, Aurore Guillevic, André Schrottenloher, Yixin Shen.

- Pierre-Alain Fouque was the president of the selection committee for a professor position in section 27 at the Université de Rennes.
- Aurore Guillevic was a member of the selection committee for an assistant professor position (MCF252186) in section 27 at Université de Versailles Saint Quentin (UVSQ).
- Yixin Shen was a jury member of the selection committee for INRIA CRCN/ISFP researcher position at the INRIA Saclay center.
- André Schrottenloher reviewed projects for ID4Mobility and for the Czech Science Foundation.

11.1.6 Research administration

Participants: Aurore Guillevic, Yixin Shen.

- Aurore Guillevic is in charge of the young researchers (mission jeunes chercheurs) and at the Commission Personnel.
- Yixin Shen is at the Commission Délégation Inria.

11.2 Teaching - Supervision - Juries - Educational and pedagogical outreach

11.2.1 Teaching

Participants: Daniel de Almeida Braga, Patrick Derbez, Pierre-Alain Fouque, Aurore Guillevic, Damien Marion, André Schrottenloher.

- Master: André Schrottenloher, Enjeux de la cryptographie post-quantique, 3 hours conference, Centrale-Supélec Rennes.
- Master: André Schrottenloher, Cryptanalyse, 7.5 hours lectures, 7.5 hours lab sessions, M2, University of Rennes.
- Bachelor: André Schrottenloher, Introduction à la Cryptologie, 9 hours lectures, ENS de Rennes.
- Master: Aurore Guillevic and Gaël Claudel, Advanced Course in Cryptography for security (BCS), 16.5 hours lab sessions, M2, University of Rennes, France;
- Master: Aurore Guillevic, Mathematics for security (MSEC), 12 hours lectures, 2 × 12 hours lab sessions, M1, University of Rennes, France;
- Master: Aurore Guillevic, Unix refresher crash course, 3 hours lab sessions, M1, University of Rennes, France;

- Master: Pierre-Alain Fouque, Basics for Cryptography, 22h lectures, M1, University of Rennes, France;
- Master: Pierre-Alain Fouque, Advanced Cryptography, 16h lectures, M2, University of Rennes, France;
- Master: Pierre-Alain Fouque, Security Proof, 12h lectures, M2, University of Rennes, France;
- Bachelor: Daniel De Almeida Braga, Introduction à la Sécurité (ISE), 1.5 hour lecture, 3 hours lab session, L1, University of Rennes, France;
- Bachelor: Daniel De Almeida Braga, Enjeux de Sécurité (ESEC), 7.5 hours lectures, L3, University of Rennes, France;
- Master: Daniel De Almeida Braga, Security Project, 24h project supervision, M1, University of Rennes, France;
- Master: Daniel De Almeida Braga, Low Level Programming, 19.5 hours lab sessions, M1, University of Rennes, France;
- Master: Daniel De Almeida Braga, Cybersécurité: Menaces et organisations, hygiène numérique (SENV), 6 hours lectures, 10.5 hours lab sessions, M1, University of Rennes, France;
- Master: Daniel De Almeida Braga, Sécurité avancée des SI d'entreprise (SSYS2), 18 hours lectures, 36 hours lab sessions, M2, University of Rennes, France;
- Master: Daniel De Almeida Braga, Introduction au pentest, 6 hours lectures, 12 hours lab sessions, M1, University of Rennes, France;
- Daniel De Almeida Braga: Co-director of the Master 2 CISO (RSSI), University of Rennes, France.
- Bachelor: Damien Marion, numérique éco-responsable (NEC2), 7.5 hours lectures, 9 hours lab sessions, 9 hours seminars, 9 hours projects, L2, University of Rennes, France;
- Bachelor: Damien Marion, enjeux sociétaux et empreinte écologique du numérique (3EN), 6 hours lectures, 12 hours projects, L3, University of Rennes, France;
- Master: Damien Marion, databases security (SBD), 33 hours lab sessions, M1, University of Rennes, France;
- Master: Damien Marion, cryptography and privacy (SDATA), 12 hours lectures, 21 hours lab sessions, 10.5 hours seminars, M1, University of Rennes, France;
- Master: Damien Marion, secured implementations for cryptography (SIMP), 3.5 hours lectures, 39 hours lab sessions, M2, University of Rennes, France;
- Master: Damien Marion, research project, 24 hours project supervision, M1, University of Rennes, France;
- Damien Marion: contact regarding teaching activities of the ecological transition in computer science at the University of Rennes, France;
- Master: Patrick Derbez, Cryptanalyse, 7.5 hours lectures, 7.5 hours lab sessions, M2, University of Rennes.
- Bachelor: Patrick Derbez, Introduction à la programmation, 15 hours lectures, 16.5 hours lab sessions, L1, University of Rennes.
- Bachelor: Patrick Derbez, Introduction à la Cryptologie, 3 hours lectures, 3 hours lab sessions, L1, University of Rennes.

11.2.2 Supervision

Participants: Daniel de Almeida Braga, Patrick Derbez, Pierre-Alain Fouque, Aurore Guillevic, Damien Marion, André Schrottenloher, Yixin Shen.

- PhD: Phuong Hoa Nguyen, *MILP and symmetric-key cryptanalysis* [33], started October 2021, defended February 2025. Supervisors: Patrick Derbez and Pierre-Alain Fouque.
- PhD: Paul Kirchner, *Cryptanalysis of public-key cryptography* [32], defended May 2025. Supervisors: Pierre-Alain Fouque, with Aurore Guillevic in 2024–2025.
- PhD: Pierrick Philippe, *Secrets in Compiler: Detection of Secret-related Weaknesses in GCC Static Analyzer*, started October 2022, defended December 2025. Supervisors: Mohamed Sabt (IRISA) and Pierre-Alain Fouque.
- PhD in progress: Clémence Chevignard, *Module-LIP: réductions, cryptanalyse, algorithmes*, started November 2023. Supervisors: Pierre-Alain Fouque, Alexandre Wallet and Rémi Giraud (Qualcomm).
- PhD in progress: Mathieu Degré, *Nouveaux modèles MILP adaptés aux problèmes cryptographiques*, started January 2024. Supervisors: Patrick Derbez, André Schrottenloher.
- PhD in progress: Aurel Pichollet–Mugnier, *Security of ASCON and Lightweight Symmetric Primitives against Quantum Attackers*, started November 2024. Supervisors: Patrick Derbez, André Schrottenloher, Zoé Amblard (Thales SIX)
- PhD in progress: Baptiste Germon, *Independence hypothesis in differential cryptanalysis*, started October 2024. Supervisors: Patrick Derbez, Christina Boura (IRIF)
- PhD in progress: Roderick Asselineau, *Cryptanalyse d’algorithmes symétriques utilisés dans la vie réelle*, started April 2025. Supervisors: Patrick Derbez, Pierre-Alain Fouque, Brice Minaud (Inria Paris).
- PhD in progress: Bastien Michel, *Optimisation de la cryptanalyse de primitives symétrique*, started October 2024. Supervisors: Patrick Derbez, Maria Naya-Plasencia (Inria Paris).
- PhD in progress: Marie Euler, *Outils pour la cryptanalyse et la conception de primitives cryptographiques*, VAE. Supervisors: Patrick Derbez.
- PhD in progress: Gaël Claudel, *Analyse des attaques par canaux auxiliaires de schémas de signature post quantique : approches combinées*. Supervisors: Patrick Derbez, Damien Marion, Aurore Guillevic, Benoît Gérard (ANSSI).
- PhD in progress: Aymeric Hiltenbrand, *Attaques par canaux auxiliaires sur la cryptographie post-quantique*, from December 2023. Supervisors: Guenaël Renault (ANSSI), Pierre-Alain Fouque, Romain Poussier (ANSSI), Damien Marion.
- PhD in progress: Guilhem Niot, *Threshold Post-Quantum Cryptography*. Supervisors: Pierre-Alain Fouque and Thomas Prest (PQShield).
- PhD in progress: Mathias Boucher. *Improved Quantum Cryptanalysis on Lattices*, started September 2025. Supervisors: Yixin Shen and Pierre-Alain Fouque.
- PhD in progress: Alisée Lafontaine, *New tools for quantum symmetric cryptanalysis*, started October 2025. Supervisors: André Schrottenloher and Patrick Derbez.
- PhD in progress: Paul Delhom, *Signatures Avancées Post-Quantiques*, started November 2025. Supervisors: Corentin Jeudy (Orange), Olivier Sanders (Orange) and Pierre-Alain Fouque.

- PhD in progress: Théo Goureau, *ARMADA: ARM Microarchitectural Attacks Discovery and Analysis*, started October 2025. Supervisors: Daniel De Almeida Braga, Pierre-Alain Fouque, Guillaume Hiet (SUSHI) and Thomas Rokicki (SUSHI).
- Internship: Mathias Boucher (M2) *Regev's reduction on a family of easily decodable lattices* (March-July 2025). Supervisor: Yixin Shen.
- Internship: Alisée Lafontaine (M2) *New tools for quantum symmetric cryptanalysis* (March-September 2025). Supervisor: André Schrottenloher.
- Internship: Babacar Ndiaye (M2 Université de Limoges) *Polynomial selection for the Tower Number Field Sieve* (April-August 2025). Supervisor: Aurore Guillevic.
- Internship: Hubert de Groote (M2 MPRI) *Security proof for Falcon sampler* (April-August 2025). Supervisor: Pierre-Alain Fouque.
- Internship: Adrian Lagasse (M1 Université de Rennes) *Analysis and Exploitation of Intel's Instruction Prefetcher* (May-August 2025). Supervisor: Daniel De Almeida Braga.

11.2.3 Juries

Participants: Pierre-Alain Fouque, Aurore Guillevic, André Schrottenloher, Yixin Shen.

- Pierre-Alain Fouque was a reviewer of the PhD thesis of Philipp Gajland (June 4, 2025, Bochum-Universität, Germany).
- Pierre-Alain Fouque was a reviewer of the HDR thesis of Yann Rotella (February 6, 2025, Université de Versailles-Saint-Quentin-en-Yvelines, France).
- Pierre-Alain Fouque was the President of the PhD thesis of Tristan Claverie (June 6, 2025, Université de Rennes, France).
- Pierre-Alain Fouque was an examiner of the PhD thesis of Paul Kirchner (May 22, 2025, Université de Rennes, France).
- Pierre-Alain Fouque was the President of the PhD thesis of Charles Meyer-Hilfiger (September 30, 2025, Université de Sorbonne University, France).
- Pierre-Alain Fouque was a reviewer of the PhD thesis of Nicolas Bon (November 14, 2025, École normale supérieure, France).
- Pierre-Alain Fouque was a reviewer of the PhD thesis of Henry Bambury (November 18, 2025, École normale supérieure, France).
- Pierre-Alain Fouque was an examiner of the PhD thesis of Guirec Lebrun (December 1, 2025, École normale supérieure, France).
- Pierre-Alain Fouque was the President of the PhD thesis of Pierre Pébureau (December 16, 2025, Université de Sorbonne University, France).
- Pierre-Alain Fouque was an examiner of the PhD thesis of Pierrick Philippe (December 10, 2025, Université de Rennes, France).
- Pierre-Alain Fouque was a reviewer of the PhD thesis of Viet-Sang Nguyen (December 19, 2025, Université de Saint-Étienne, France).
- André Schrottenloher was a reviewer of the PhD thesis of Nathalie Lang (July 14, 2025, Bauhaus-Universität Weimar, Germany).

- Aurore Guillevic was a reviewer of the PhD thesis of François Palma (December 12, 2025, Université de Toulon, France).
- Yixin Shen was an examiner of the PhD thesis of Joseph Cunningham (September 5, 2025, Université Libre de Bruxelles, Belgique).

11.2.4 Educational and pedagogical outreach

Participants: Daniel de Almeida Braga, Patrick Derbez, Pierre-Alain Fouque, Yixin Shen.

- Yixin Shen gave a talk at the [ENS Rennes student research seminar](#) about "Collision finding, random walks and quantum algorithms" in November 2025.
- Daniel De Almeida Braga organized a Capture The Flag (CTF) event for students at University of Rennes in April 2025, to bridge bachelor and master, with around 70 participants.
- Patrick Derbez gave a 3 hours lecture on "Differential Cryptanalysis" at the summer school collocated to the SAC 2025 conference in August 2025. [SAC 2025 Summer School](#)
- Pierre-Alain Fouque gave a 3 hours lecture on "Quantum algorithms for cryptanalysis" at the CEMRACS 2025 in July 2025. [CIRM Luminy](#)

11.3 Popularization

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

Participants: Damien Marion, Yixin Shen.

- Yixin Shen was featured in an interview by the French media [CURIEUX!](#) discussing post-quantum cryptography.
- Damien Marion was interviewed by a french journal, [Cryptographie : les algorithmes du futur. Sciences Ouest, october.](#)

11.3.2 Participation in Live events

Participants: André Schrottenloher, Yixin Shen.

- Yixin Shen and André Schrottenloher were panelists of Amphi Métier R&D, at Ecole polytechnique, Palaiseau, France, 2025

12 Scientific production

12.1 Major publications

- [1] Y. Belkheyar, P. Derbez, S. Ghosh, G. Leander, S. Mella, L. Perrin, S. Rasoolzadeh, L. Stennes, S. Sun, G. van Assche and D. Vizár. ‘ChiLow and ChiChi: New Constructions for Code Encryption’. In: *Advances in Cryptology – EUROCRYPT 2025: 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4–8, 2025, Proceedings, Part III*. EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS-15601. Lecture Notes in Computer Science. Madrid, Spain: Springer Nature Switzerland, 27th Apr. 2025, pp. 212–243. doi: [10.1007/978-3-031-91107-1_8](https://doi.org/10.1007/978-3-031-91107-1_8). URL: <https://hal.science/hal-05435256>.
- [2] K. Carrier, C. Meyer-Hilfiger, Y. Shen and J.-P. Tillich. ‘Assessing the Impact of a Variant of MATZOV’s Dual Attack on Kyber’. In: *Advances in Cryptology - CRYPTO 2025*. CRYPTO 2025 - 45th Annual International Cryptology Conference. Santa Barbara, United States: Springer, 2025, pp. 1–36. URL: <https://hal.science/hal-05406481>.

12.2 Publications of the year

International journals

- [3] D. Aggarwal, Y. Chen, R. Kumar and Y. Shen. ‘Improved Classical and Quantum Algorithms for the Shortest Vector Problem via Bounded Distance Decoding’. In: *SIAM Journal on Computing* 54.2 (3rd Mar. 2025), pp. 233–278. doi: [10.1137/22M1486959](https://doi.org/10.1137/22M1486959). URL: <https://hal.science/hal-05406608> (cit. on p. 21).
- [4] K. Bashiri, X. Bonnetain, A. Hosoyamada, N. Lang and A. Schrottenloher. ‘Improved Quantum Linear Attacks and Application to CAST’. In: *IACR Transactions on Symmetric Cryptology* 2025.2 (11th June 2025), pp. 124–165. doi: [10.46586/tosc.v2025.i2.124-165](https://doi.org/10.46586/tosc.v2025.i2.124-165). URL: <https://inria.hal.science/hal-05243650> (cit. on p. 17).
- [5] C. Boura, P. Derbez and B. Germon. ‘Extending the Quasidifferential Framework: From Fixed-Key to Expected Differential Probability’. In: *IACR Transactions on Symmetric Cryptology* 2025.1 (7th Mar. 2025), pp. 515–541. doi: [10.46586/tosc.v2025.i1.515-541](https://doi.org/10.46586/tosc.v2025.i1.515-541). URL: <https://hal.science/hal-05022864> (cit. on p. 15).
- [6] M. Degré, P. Derbez, L. Lahaye and A. Schrottenloher. ‘New models for the cryptanalysis of ASCON’. In: *Designs, Codes and Cryptography* 93.6 (8th Feb. 2025), pp. 2055–2072. doi: [10.1007/s10623-025-01572-5](https://doi.org/10.1007/s10623-025-01572-5). URL: <https://inria.hal.science/hal-05243652> (cit. on p. 15).
- [7] M. Degré, P. Derbez and A. Schrottenloher. ‘Simplified Meet-in-the-middle Preimage Attacks on AES-based Hashing’. In: *IACR Communications in Cryptology* 2.4 (2025). URL: <https://inria.hal.science/hal-05404180>. In press (cit. on p. 14).
- [8] P. Derbez, B. Germon, B. Michel and M. Naya Plasencia. ‘Improved Cryptanalysis of GIFT-64’. In: *IACR Transactions on Symmetric Cryptology* 2025.4 (2025), pp. 284–307. doi: [10.46586/tosc.v2025.i4.284-307](https://doi.org/10.46586/tosc.v2025.i4.284-307). URL: <https://hal.science/hal-05432869> (cit. on p. 15).
- [9] Q. Edme, P.-A. Fouque and A. Schrottenloher. ‘Faster Quantum Algorithms for MQ2 and Applications’. In: *IACR Communications in Cryptology* 2.1 (8th Apr. 2025), pp. 1–28. doi: [10.62056/anjbksc2](https://doi.org/10.62056/anjbksc2). URL: <https://inria.hal.science/hal-05243647> (cit. on p. 17).
- [10] P.-A. Fouque, D. Marion, Q. Nguyen and A. Wallet. ‘Avengers assemble! Supervised learning meets lattice reduction’. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025 (5th Sept. 2025), pp. 409–436. doi: [10.46586/tches.v2025.i4.409-436](https://doi.org/10.46586/tches.v2025.i4.409-436). URL: <https://hal.science/hal-05455454> (cit. on p. 23).
- [11] J. Gasnier and A. Guillevic. ‘An Algebraic Point of View on the Generation of Pairing-Friendly Curves’. In: *SIAM Journal on Applied Algebra and Geometry* 9.2 (27th June 2025), pp. 456–480. doi: [10.1137/23M1601961](https://doi.org/10.1137/23M1601961). URL: <https://hal.science/hal-04205681> (cit. on p. 20).

International peer-reviewed conferences

- [12] J. Basak, R. Bhaumik, A. K. Chauhan, R. Jejurikar, A. Jha, A. Roy, A. Schrottenloher and S. Talnikar. ‘Post-quantum Security of Key-Alternating Feistel Ciphers’. In: *Lecture Notes in Computer Science. ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security*. Vol. LNCS-16245. Lecture Notes in Computer Science. Melbourne, Australia: Springer Nature Singapore, 8th Dec. 2026, pp. 446–478. doi: [10.1007/978-981-95-5018-0_15](https://doi.org/10.1007/978-981-95-5018-0_15). URL: <https://inria.hal.science/hal-05406482> (cit. on p. 14).
- [13] Y. Belkheyar, P. Derbez, S. Ghosh, G. Leander, S. Mella, L. Perrin, S. Rasoolzadeh, L. Stennes, S. Sun, G. van Assche and D. Vizár. ‘ChiLow and ChiChi: New Constructions for Code Encryption’. In: *Advances in Cryptology – EUROCRYPT 2025: 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4–8, 2025, Proceedings, Part III*. EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. LNCS-15601. Lecture Notes in Computer Science. Madrid, Spain: Springer Nature Switzerland, 27th Apr. 2025, pp. 212–243. doi: [10.1007/978-3-031-91107-1_8](https://doi.org/10.1007/978-3-031-91107-1_8). URL: <https://hal.science/hal-05435256> (cit. on pp. 13, 15).
- [14] C. Boura, P. Derbez, B. Germon, R. H. Boissier and M. Naya-Plasencia. ‘SPEEDY: Caught at Last’. In: ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security. Vol. LNCS-16245. Lecture Notes in Computer Science. Melbourne, Australia: Springer Nature Singapore, 8th Dec. 2026, pp. 189–220. doi: [10.1007/978-981-95-5018-0_7](https://doi.org/10.1007/978-981-95-5018-0_7). URL: <https://hal.science/hal-05461455> (cit. on p. 16).
- [15] K. Carrier, C. Meyer-Hilfiger, Y. Shen and J.-P. Tillich. ‘Assessing the Impact of a Variant of MATZOV’s Dual Attack on Kyber’. In: *Advances in Cryptology - CRYPTO 2025*. CRYPTO 2025 - 45th Annual International Cryptology Conference. Santa Barbara, United States: Springer, 2025, pp. 1–36. URL: <https://hal.science/hal-05406481> (cit. on pp. 13, 17).
- [16] S. Celi, D. Escudero and G. Niot. ‘Share the MAYO: Thresholdizing MAYO’. In: PQCrypto 2025 - 16th International Conference on Post-Quantum Cryptography. Vol. 15577. Lecture Notes in Computer Science. Taipei, Taiwan: Springer Nature Switzerland, 15th Mar. 2025, pp. 165–198. doi: [10.1007/978-3-031-86599-2_6](https://doi.org/10.1007/978-3-031-86599-2_6). URL: <https://hal.science/hal-05230600> (cit. on p. 19).
- [17] S. Celi, R. del Pino, T. Espitau, G. Niot and T. Prest. ‘Efficient Threshold ML-DSA’. In: 35th USENIX Security Symposium (USENIX Security 2026). Baltimore, United States, 12th Aug. 2026. URL: <https://inria.hal.science/hal-05442192> (cit. on p. 19).
- [18] C. Cheviguard, P.-A. Fouque and A. Schrottenloher. ‘Reducing the Number of Qubits in Quantum Factoring’. In: *45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2025, Proceedings, Part V*. CRYPTO 2025 - Advances in Cryptology. Vol. LNCS-16001. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 17th Aug. 2025, pp. 384–415. doi: [10.1007/978-3-032-01878-6_13](https://doi.org/10.1007/978-3-032-01878-6_13). URL: <https://inria.hal.science/hal-05436363> (cit. on p. 22).
- [19] C. Cheviguard, G. Mureau, T. Espitau, A. Pellet-Mary, H. Pliatsok and A. Wallet. ‘A reduction from Hawk to the principal ideal problem in a quaternion algebra’. In: Eurocrypt 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science. Madrid, Spain, 5th May 2025. doi: [10.1007/978-3-031-91124-8_6](https://doi.org/10.1007/978-3-031-91124-8_6). URL: <https://hal.science/hal-05233972> (cit. on p. 18).
- [20] P. Derbez and M. Euler. ‘Minimalist Model for Impossible Differentials’. In: SAC 2025 - 32nd International Conference on Selected Areas in Cryptography. Vol. LNCS 16207. Lecture Notes in Computer Science. Toronto, Canada: Springer Nature Switzerland, 2nd Jan. 2026, pp. 113–143. doi: [10.1007/978-3-032-10536-3_5](https://doi.org/10.1007/978-3-032-10536-3_5). URL: <https://hal.science/hal-05461429> (cit. on p. 16).
- [21] K. Duverger, P.-A. Fouque, C. Jacomme, G. Niot and C. Onete. ‘Subversion-resilient Key-exchange in the Post-quantum World’. In: CCS 2025 - 32nd ACM Conference on Computer and Communications Security. Taipei, Taiwan, 5th Sept. 2025, pp. 1–49. URL: <https://inria.hal.science/hal-05242187> (cit. on p. 23).

- [22] K. Hashimoto, S. Katsumata, G. Niot and T. Wiggers. ‘Revisiting PQ WireGuard: A Comprehensive Security Analysis With a New Design Using Reinforced KEMs’. In: 47th IEEE Symposium on Security and Privacy (S&P ’26). SAN FRANCISCO, United States, 18th May 2026. URL: <https://inria.hal.science/hal-05444065> (cit. on p. 23).
- [23] A. Hiltenbrand, J. Eynard and R. Poussier. ‘On the Success Rate of Simple Side-Channel Attacks Against Masking with Unlimited Attack Traces’. In: *Lecture Notes in Computer Science, vol 15952*. CASCADE 2025 - International Conference on Constructive Approaches for Security Analysis and Design of Embedded Systems. Vol. 15952. Lecture Notes in Computer Science. Saint-Etienne (FR), France: Springer Nature Switzerland; Springer Nature Switzerland, 15th Oct. 2026, pp. 343–366. DOI: [10.1007/978-3-032-01405-4_14](https://hal.science/hal-05456476). URL: <https://hal.science/hal-05456476> (cit. on p. 24).
- [24] G. Niot. ‘Practical Deniable Post-Quantum X3DH: A Lightweight Split-KEM for K-Waay’. In: *ASIA CCS ’25: Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*. ASIACCS 2025 - 20th ACM Asia Conference on Computer and Communications Security. Hanoi, Vietnam: ACM, 25th Aug. 2025, pp. 298–312. DOI: [10.1145/3708821.3736192](https://hal.science/hal-05230618). URL: <https://hal.science/hal-05230618> (cit. on p. 20).
- [25] P. Philippe, M. Sabt and P.-A. Fouque. ‘GnuZero: A Compiler-Based Zeroization Static Detection Tool for the Masses’. In: DSN 2025 - 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Naples, Italy, 23rd June 2025, pp. 1–14. URL: <https://inria.hal.science/hal-05065294> (cit. on pp. 13, 24).
- [26] R. del Pino, S. Katsumata, G. Niot, M. Reichle and K. Takemure. ‘Unmasking TRaccoon: A Lattice-Based Threshold Signature with An Efficient Identifiable Abort Protocol’. In: CRYPTO 2025 - 45th Annual International Cryptology Conference. Vol. 16005. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 17th Aug. 2025, pp. 423–456. DOI: [10.1007/978-3-032-01887-8_14](https://hal.science/hal-05230612). URL: <https://hal.science/hal-05230612> (cit. on p. 20).
- [27] R. del Pino and G. Niot. ‘Finally! A Compact Lattice-Based Threshold Signature’. In: PKC 2025 - International Conference on Practice and Theory in Public Key Cryptography. Vol. 15676. Lecture Notes in Computer Science. Roros, Norway: Springer Nature Switzerland, 5th May 2025, pp. 169–199. DOI: [10.1007/978-3-031-91826-1_6](https://hal.science/hal-05230606). URL: <https://hal.science/hal-05230606> (cit. on p. 19).
- [28] A. Pouly and Y. Shen. ‘Discrete gaussian sampling for BKZ-reduced basis’. In: Post-Quantum Cryptography - 16th International Workshop, PQCrypto 2025. Taipei, Taiwan, 2025, pp. 63–88. DOI: [10.1007/978-3-031-86602-9_3](https://inria.hal.science/hal-04823293). URL: <https://inria.hal.science/hal-04823293> (cit. on p. 18).

Conferences without proceedings

- [29] C. Cheviguard, P.-A. Fouque and A. Schrottenloher. ‘Reducing the Number of Qubits in Quantum Factoring’. In: QIP 2025 - 28th Annual Conference on Quantum Information Processing. Raleigh, North Carolina, United States, 2025, pp. 384–415. URL: <https://inria.hal.science/hal-04848612> (cit. on pp. 13, 22).
- [30] C. Cheviguard and G. Mureau. ‘Ideally HAWKward: How Not to Break Module-LIP’. In: CFAIL 2025 - Conference for Failed Approaches and Insightful Losses in Cryptology (an affiliated workshop to Crypto 2025). Santa Barbara (CA), United States, 2025, pp. 1–7. URL: <https://hal.science/hal-05235811> (cit. on p. 18).
- [31] S. Katsumata, G. Niot, I. Tucker and T. Wiggers. ‘Comprehensive Deniability Analysis of Signal Handshake Protocols: X3DH, PQXDH to Fully Post-Quantum with Deniable Ring Signatures’. In: 34th USENIX Conference on Security Symposium (USENIX Security ’25). Seattle, United States, 13th Aug. 2025. DOI: [10.5555/3766078.3766427](https://hal.science/hal-05444090). URL: <https://hal.science/hal-05444090> (cit. on p. 22).

Doctoral dissertations and habilitation theses

- [32] P. Kirchner. ‘Cryptanalysis of public-key cryptography’. Université de Rennes, 23rd May 2025. URL: <https://theses.hal.science/tel-05261946> (cit. on p. 32).
- [33] P.-H. Nguyen. ‘New automated approaches in cryptanalysis’. Université de Rennes, 11th Feb. 2025. URL: <https://theses.hal.science/tel-05369410> (cit. on p. 32).

Reports & preprints

- [34] X. Bonnetain, J. Loyer, A. Schrottenloher and Y. Shen. *A Tight Quantum Algorithm for Multiple Collision Search*. 2025. URL: <https://hal.science/hal-05265077> (cit. on p. 21).
- [35] K. Boudgoust, C. Jeudy, E. Tairi and W. Wen. *Hardness of M-LWE with General Distributions and Applications to Leaky Variants*. 14th Aug. 2025. URL: <https://hal-lirmm.ccsd.cnrs.fr/lirmm-05396885>.
- [36] P. Dartois, J. K. Eriksen, R. Invernizzi and F. Vercauteren. *qt-Pegasis: Simpler and Faster Effective Class Group Actions*. 2nd Oct. 2025. URL: <https://hal.science/hal-05404059> (cit. on p. 21).

12.3 Cited publications

- [37] D. Aggarwal, D. Dadush, O. Regev and N. Stephens-Davidowitz. ‘Solving the Shortest Vector Problem in 2^n Time Using Discrete Gaussian Sampling: Extended Abstract’. In: *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*. 2015, pp. 733–742. DOI: [10.1145/2746539.2746606](https://doi.org/10.1145/2746539.2746606). URL: <https://doi.org/10.1145/2746539.2746606> (cit. on p. 21).
- [38] G. Alagic, C. Bai, J. Katz and C. Majenz. ‘Post-Quantum Security of the Even-Mansour Cipher’. In: *EUROCRYPT (3)*. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 458–487 (cit. on p. 14).
- [39] Z. Bao, J. Guo, D. Shi and Y. Tu. ‘Superposition Meet-in-the-Middle Attacks: Updates on Fundamental Security of AES-like Hashing’. In: *CRYPTO (1)*. Vol. 13507. Lecture Notes in Computer Science. Springer, 2022, pp. 64–93 (cit. on p. 14).
- [40] G. Barthe, S. Belaïd, G. Cassiers, P.-A. Fouque, B. Grégoire and F.-X. Standaert. ‘maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults’. In: *ESORICS (1)*. Vol. 11735. Lecture Notes in Computer Science. Springer, 2019, pp. 300–318 (cit. on p. 11).
- [41] G. Barthe, S. Belaïd, F. Dupressoir, P.-A. Fouque, B. Grégoire and P.-Y. Strub. ‘Verified Proofs of Higher-Order Masking’. In: *EUROCRYPT (1)*. Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 457–485 (cit. on p. 11).
- [42] G. Barthe, S. Belaïd, F. Dupressoir, P.-A. Fouque, B. Grégoire, P.-Y. Strub and R. Zucchini. ‘Strong Non-Interference and Type-Directed Higher-Order Masking’. In: *CCS*. ACM, 2016, pp. 116–129 (cit. on p. 11).
- [43] G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, B. Grégoire, M. Rossi and M. Tibouchi. ‘Masking the GLP Lattice-Based Signature Scheme at Any Order’. In: *EUROCRYPT (2)*. Vol. 10821. Lecture Notes in Computer Science. Springer, 2018, pp. 354–384 (cit. on p. 11).
- [44] G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi and M. Tibouchi. ‘GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures, Revisited’. In: *CCS*. ACM, 2019, pp. 2147–2164 (cit. on p. 11).
- [45] O. Bernard and A. Roux-Langlois. ‘Twisted-PHS: Using the Product Formula to Solve Approx-SVP in Ideal Lattices’. In: *ASIACRYPT (2)*. Vol. 12492. Lecture Notes in Computer Science. Springer, 2020, pp. 349–380 (cit. on p. 8).
- [46] G. Bertoni, J. Daemen, S. Hoffert, M. Peeters, G. V. Assche and R. V. Keer. ‘Farfalle: parallel permutation-based cryptography’. In: *IACR Trans. Symmetric Cryptol.* 2017.4 (2017), pp. 1–38 (cit. on p. 9).

- [47] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. G elin and P. Kirchner. ‘Computing Generator in Cyclotomic Integer Rings - A Subfield Algorithm for the Principal Ideal Problem in $L_{\Delta_{\mathbb{K}}}(1/2)$ and Application to the Cryptanalysis of a FHE Scheme’. In: *EUROCRYPT (1)*. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 60–88 (cit. on p. 8).
- [48] X. Bonnetain, A. Chailloux, A. Schrottenloher and Y. Shen. ‘Finding Many Collisions via Reusable Quantum Walks - Application to Lattice Sieving’. In: *EUROCRYPT (5)*. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 221–251 (cit. on pp. 10, 22).
- [49] X. Bonnetain, M. Naya-Plasencia and A. Schrottenloher. ‘Quantum Security Analysis of AES’. In: *IACR Trans. Symmetric Cryptol.* 2019.2 (2019), pp. 55–93. doi: [10.13154/TOSC.V2019.I2.55-93](https://doi.org/10.13154/TOSC.V2019.I2.55-93). URL: <https://doi.org/10.13154/tosc.v2019.i2.55-93> (cit. on p. 10).
- [50] X. Bonnetain, A. Schrottenloher and F. Sibleyras. ‘Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes’. In: *EUROCRYPT (3)*. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 315–344 (cit. on p. 10).
- [51] K. Boudgoust, C. Jeudy, A. Roux-Langlois and W. Wen. ‘Towards Classical Hardness of Module-LWE: The Linear Rank Case’. In: *ASIACRYPT (2)*. Vol. 12492. Lecture Notes in Computer Science. Springer, 2020, pp. 289–317 (cit. on p. 7).
- [52] C. Bouillaguet, C. Delaplace and M. Trimoska. ‘A Simple Deterministic Algorithm for Systems of Quadratic Polynomials over \mathbb{F}_2 ’. In: *SOSA*. SIAM, 2022, pp. 285–296 (cit. on p. 17).
- [53] C. Bouillaguet, P. Derbez and P.-A. Fouque. ‘Automatic Search of Attacks on Round-Reduced AES and Applications’. In: *CRYPTO*. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, pp. 169–187 (cit. on p. 9).
- [54] D. D. A. Braga, P.-A. Fouque and M. Sabt. ‘Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild’. In: *ACSAC*. ACM, 2020, pp. 291–303 (cit. on p. 11).
- [55] D. D. A. Braga, N. Kulatova, M. Sabt, P. Fouque and K. Bhargavan. ‘From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake’. In: *EuroS&P*. IEEE, 2023, pp. 707–723 (cit. on p. 12).
- [56] Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehl e. ‘Classical hardness of learning with errors’. In: *STOC*. ACM, 2013, pp. 575–584 (cit. on p. 7).
- [57] Y. Chen, K. Chung and C. Lai. ‘Space-efficient classical and quantum algorithms for the shortest vector problem’. In: *Quantum Information & Computation* 18.3&4 (2018), pp. 285–306. URL: <http://www.rintonpress.com/xxqic18/qic-18-34/0285-0306.pdf> (cit. on p. 21).
- [58] J. H. Cheon, P.-A. Fouque, C. Lee, B. Minaud and H. Ryu. ‘Cryptanalysis of the New CLT Multilinear Map over the Integers’. In: *EUROCRYPT (1)*. Vol. 9665. Lecture Notes in Computer Science. Springer, 2016, pp. 509–536 (cit. on p. 8).
- [59] C. Chuengsatiansup, T. Prest, D. Stehl e, A. Wallet and K. Xagawa. ‘ModFalcon: Compact Signatures Based On Module-NTRU Lattices’. In: *AsiaCCS*. ACM, 2020, pp. 853–866 (cit. on p. 8).
- [60] D. Collins, L. Huguenin-Dumittan, N. K. Nguyen, N. Rolin and S. Vaudenay. ‘K-waay: fast and deniable post-quantum X3DH without ring signatures’. In: *Proceedings of the 33rd USENIX Conference on Security Symposium*. SEC ’24. Philadelphia, PA, USA: USENIX Association, 2024 (cit. on p. 20).
- [61] P. Derbez and P.-A. Fouque. ‘Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks’. In: *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*. Ed. by M. Robshaw and J. Katz. Vol. 9815. Lecture Notes in Computer Science. Springer, 2016, pp. 157–184. doi: [10.1007/978-3-662-53008-5_6](https://doi.org/10.1007/978-3-662-53008-5_6) (cit. on p. 9).
- [62] P. Derbez and P.-A. Fouque. ‘Exhausting Demirci-Sel uk Meet-in-the-Middle Attacks Against Reduced-Round AES’. In: *FSE*. Vol. 8424. Lecture Notes in Computer Science. Springer, 2013, pp. 541–560 (cit. on p. 9).
- [63] C. Dobraunig, M. Eichlseder, F. Mendel and M. Schl affer. ‘Ascon v1.2: Lightweight Authenticated Encryption and Hashing’. In: *J. Cryptol.* 34.3 (2021), p. 33 (cit. on p. 8).

- [64] V. Dubois, P.-A. Fouque, A. Shamir and J. Stern. ‘Practical Cryptanalysis of SFLASH’. In: *CRYPTO*. Vol. 4622. Lecture Notes in Computer Science. Springer, 2007, pp. 1–12 (cit. on p. 8).
- [65] A. Duc, S. Dziembowski and S. Faust. ‘Unifying Leakage Models: From Probing Attacks to Noisy Leakage’. In: *EUROCRYPT*. Vol. 8441. Lecture Notes in Computer Science. Springer, 2014, pp. 423–440 (cit. on p. 11).
- [66] L. Ducas. ‘Provable lattice reduction of Zn with blocksize $n/2$ ’. In: *Designs, Codes and Cryptography* (Nov. 2023). doi: [10.1007/s10623-023-01320-7](https://doi.org/10.1007/s10623-023-01320-7) (cit. on p. 21).
- [67] L. Ducas, E. W. Postlethwaite, L. N. Pulles and W. P. J. van Woerden. ‘Hawk: Module LIP Makes Lattice Signatures Fast, Compact and Simple’. In: *ASIACRYPT (4)*. Vol. 13794. Lecture Notes in Computer Science. Springer, 2022, pp. 65–94 (cit. on p. 19).
- [68] L. Ducas and L. N. Pulles. ‘Does the Dual-Sieve Attack on Learning with Errors even Work?’ In: 2023. Ed. by H. Handschuh and A. Lysyanskaya. Vol. 14083. Santa Barbara, CA, USA: Springer, Aug. 2023, pp. 37–69. doi: [10.1007/978-3-031-38548-3_2](https://doi.org/10.1007/978-3-031-38548-3_2). URL: https://doi.org/10.1007/978-3-031-38548-3_2 (cit. on p. 18).
- [69] P.-A. Fouque, P. Kirchner, T. Pornin and Y. Yu. ‘BAT: Small and Fast KEM over NTRU Lattices’. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.2 (2022), pp. 240–265. doi: [10.46586/TCHES.V2022.I2.240-265](https://doi.org/10.46586/TCHES.V2022.I2.240-265). URL: <https://doi.org/10.46586/tches.v2022.i2.240-265> (cit. on p. 12).
- [70] P.-A. Fouque, P. Kirchner, M. Tibouchi, A. Wallet and Y. Yu. ‘Key Recovery from Gram-Schmidt Norm Leakage in Hash-and-Sign Signatures over NTRU Lattices’. In: *EUROCRYPT (3)*. Vol. 12107. Lecture Notes in Computer Science. Springer, 2020, pp. 34–63 (cit. on p. 11).
- [71] P.-A. Fouque, G. Macario-Rat and J. Stern. ‘Key Recovery on Hidden Monomial Multivariate Schemes’. In: *EUROCRYPT*. Vol. 4965. Lecture Notes in Computer Science. Springer, 2008, pp. 19–30 (cit. on p. 8).
- [72] C. Gidney. ‘How to factor 2048 bit RSA integers with less than a million noisy qubits’. In: *arXiv preprint arXiv:2505.15917* (2025) (cit. on pp. 13, 22).
- [73] C. Gidney and M. Ekerå. ‘How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits’. In: *Quantum* 5 (2021), p. 433. doi: [10.22331/q-2021-04-15-433](https://doi.org/10.22331/q-2021-04-15-433). URL: <https://doi.org/10.22331/q-2021-04-15-433> (cit. on p. 22).
- [74] K. Hashimoto, S. Katsumata and T. Wiggers. ‘Bundled authenticated key exchange: a concrete treatment of signal’s handshake protocol and post-quantum security’. In: *Proceedings of the 34th USENIX Conference on Security Symposium*. USA: USENIX Association, 2025 (cit. on p. 23).
- [75] A. Hülsing, K.-C. Ning, P. Schwabe, F. J. Weber and P. R. Zimmermann. ‘Post-quantum WireGuard’. In: *2021 IEEE Symposium on Security and Privacy (SP)*. 2021, pp. 304–321. doi: [10.1109/SP40001.2021.00030](https://doi.org/10.1109/SP40001.2021.00030) (cit. on p. 23).
- [76] Y. Ishai, A. Sahai and D. A. Wagner. ‘Private Circuits: Securing Hardware against Probing Attacks’. In: *CRYPTO*. Vol. 2729. Lecture Notes in Computer Science. Springer, 2003, pp. 463–481 (cit. on p. 11).
- [77] M. Kaplan, G. Leurent, A. Leverrier and M. Naya-Plasencia. ‘Quantum Differential and Linear Cryptanalysis’. In: *IACR Trans. Symmetric Cryptol.* 2016.1 (2016), pp. 71–94 (cit. on p. 17).
- [78] P. Kirchner, T. Espitau and P.-A. Fouque. ‘Fast Reduction of Algebraic Lattices over Cyclotomic Fields’. In: *CRYPTO (2)*. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 155–185 (cit. on p. 8).
- [79] P. Kirchner and P.-A. Fouque. ‘An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices’. In: *CRYPTO (1)*. Vol. 9215. Lecture Notes in Computer Science. Springer, 2015, pp. 43–62 (cit. on p. 8).
- [80] P. Kirchner and P.-A. Fouque. ‘Revisiting Lattice Attacks on Overstretched NTRU Parameters’. In: *EUROCRYPT (1)*. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 3–26 (cit. on p. 8).
- [81] H. Kuwakado and M. Morii. ‘Quantum distinguisher between the 3-round Feistel cipher and the random permutation’. In: *ISIT. IEEE*, 2010, pp. 2682–2685 (cit. on pp. 14, 17).

- [82] H. Kuwakado and M. Morii. ‘Security on the quantum-type Even-Mansour cipher’. In: *ISITA*. IEEE, 2012, pp. 312–316 (cit. on p. 14).
- [83] C. Lee, A. Pellet-Mary, D. Stehlé and A. Wallet. ‘An LLL Algorithm for Module Lattices’. In: *ASIACRYPT (2)*. Vol. 11922. Lecture Notes in Computer Science. Springer, 2019, pp. 59–90 (cit. on p. 8).
- [84] É. Levieil and P.-A. Fouque. ‘An Improved LPN Algorithm’. In: *SCN*. Vol. 4116. Lecture Notes in Computer Science. Springer, 2006, pp. 348–359 (cit. on p. 8).
- [85] MATZOV. *Report on the Security of LWE: Improved Dual Lattice Attack*. Apr. 2022. DOI: [10.5281/zenodo.6412487](https://doi.org/10.5281/zenodo.6412487). URL: <https://doi.org/10.5281/zenodo.6412487> (cit. on p. 18).
- [86] V. Migliore, B. Gérard, M. Tibouchi and P.-A. Fouque. ‘Masking Dilithium - Efficient Implementation and Side-Channel Evaluation’. In: *ACNS*. Vol. 11464. Lecture Notes in Computer Science. Springer, 2019, pp. 344–362 (cit. on p. 11).
- [87] B. Minaud, P. Derbez, P.-A. Fouque and P. Karpman. ‘Key-Recovery Attacks on ASASA’. In: *J. Cryptol.* 31.3 (2018), pp. 845–884 (cit. on p. 8).
- [88] G. Mureau, A. Pellet-Mary, G. Pliatsok and A. Wallet. ‘Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields’. In: *EUROCRYPT (6)*. Vol. 14656. Lecture Notes in Computer Science. Springer, 2024, pp. 226–255 (cit. on p. 19).
- [89] G. Patat, M. Sabt and P. Fouque. ‘Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME’. In: *Proc. Priv. Enhancing Technol.* 2023.4 (2023), pp. 306–321 (cit. on p. 12).
- [90] R. del Pino, S. Katsumata, M. Maller, F. Mouhartem, T. Prest and M.-J. Saarinen. ‘Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions’. In: *Advances in Cryptology - EUROCRYPT 2024: 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part II*. Zurich, Switzerland: Springer-Verlag, 2024, pp. 219–248. DOI: [10.1007/978-3-031-58723-8_8](https://doi.org/10.1007/978-3-031-58723-8_8). URL: https://doi.org/10.1007/978-3-031-58723-8_8 (cit. on p. 20).
- [91] A. Pouly and Y. Shen. ‘Provable Dual Attacks on Learning with Errors’. In: *EUROCRYPT (6)*. Vol. 14656. Lecture Notes in Computer Science. Springer, 2024, pp. 256–285 (cit. on p. 18).
- [92] B. Pring. ‘Exploiting Preprocessing for Quantum Search to Break Parameters for *MQ* Cryptosystems’. In: *WAIFI*. Vol. 11321. Lecture Notes in Computer Science. Springer, 2018, pp. 291–307 (cit. on p. 17).
- [93] E. Prouff and M. Rivain. ‘Masking against Side-Channel Attacks: A Formal Security Proof’. In: *EUROCRYPT*. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 142–159 (cit. on p. 11).
- [94] M. Rosca, D. Stehlé and A. Wallet. ‘On the Ring-LWE and Polynomial-LWE Problems’. In: *EUROCRYPT (1)*. Vol. 10820. Lecture Notes in Computer Science. Springer, 2018, pp. 146–173 (cit. on p. 7).
- [95] A. Schrottenloher. ‘Quantum Linear Key-Recovery Attacks Using the QFT’. In: *CRYPTO (5)*. Vol. 14085. Lecture Notes in Computer Science. Springer, 2023, pp. 258–291 (cit. on p. 17).
- [96] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler and D. Stehlé. *CRYSTALS-KYBER*. Tech. rep. available at <https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions>. National Institute of Standards and Technology, 2020 (cit. on p. 18).
- [97] P. W. Shor. ‘Algorithms for Quantum Computation: Discrete Logarithms and Factoring’. In: *FOCS*. IEEE Computer Society, 1994, pp. 124–134 (cit. on p. 7).