UMR IRISA

Activity Report 2024

Team CAPSULE

Applied Cryptography & Implementation Security

Joint team with Centre Inria de l'Université de Rennes

D1 – Large Scale an Secure Systems

Université de Rennes | rennes | INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES | cnrs | Inria | Inserm | CentraleSupélec | IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom | Université Bretagne Sud ubs

Contents

Project-Team CAPSULE 1

1 Team members, visitors, external collaborators 2

2 Overall objectives 3

3 Research program 4
3.1 Security against post-quantum attackers . . . 4
3.2 Symmetric Cryptography . . . 5
3.3 Elliptic curves for public-key cryptography . . . 7
3.4 Security of cryptographic implementation and Real-World Cryptography . . . 7

4 Application domains 9
4.1 Designing, Analyzing and Choosing Cryptographic Standards . . . 9

5 Social and environmental responsibility 10
5.1 Impact of research results . . . 10

6 Highlights of the year 10

7 New software, platforms, open data 10
7.1 New software . . . 10
7.1.1 TNFS-alpha . . . 10
7.1.2 ALPINAC . . . 11

8 New results 11
8.1 Symmetric Cryptanalysis of Constructions . . . 11
8.2 Symmetric Cryptanalysis of Primitives and Tools . . . 12
8.3 Quantum Algorithms and Cryptanalysis . . . 13
8.4 Public-key cryptography . . . 15
8.4.1 Lattices . . . 15
8.4.2 Elliptic curves . . . 17
8.5 Side-Channel Attacks . . . 17
8.6 Real-World Cryptography . . . 18

9 Bilateral contracts and grants with industry 19
9.1 Bilateral Grants with Industry . . . 19

10 Partnerships and cooperations 20
10.1 European initiatives . . . 20
10.1.1 Horizon Europe . . . 20
10.2 National initiatives . . . 20

11 Dissemination 23
11.1 Promoting scientific activities . . . 23
11.1.1 Scientific events: organisation . . . 23
11.1.2 Scientific events: selection . . . 23
11.1.3 Journal . . . 24
11.1.4 Invited talks . . . 24
11.2 Teaching - Supervision - Juries . . . 25
11.2.1 Teaching . . . 25
11.2.2 Supervision . . . 26
11.2.3 Juries . . . 27
11.3 Popularization . . . 27
11.3.1 Participation in Live events . . . 27

12 Scientific production **27**
12.1 Major publications 27
12.2 Publications of the year 27
12.3 Cited publications 30

Project-Team CAPSULE

Creation of the Project-Team: 2023 January 01

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

1 Team members, visitors, external collaborators

Research Scientists

- Patrick Derbez [INRIA, from Oct 2024, HDR]
- Aurore Guillevic [INRIA, Researcher, from Mar 2024]
- Andre Schrottenloher [INRIA, Researcher]
- Yixin Shen [INRIA, Researcher, from Jul 2024]
- Alexandre Wallet [INRIA, Researcher, until Apr 2024]

Faculty Members

- Pierre-Alain Fouque [Team leader, UNIV RENNES, Professor, HDR]
- Daniel De Almeida Braga [UNIV RENNES, Associate Professor, from Sep 2024]
- Patrick Derbez [UNIV RENNES, Associate Professor, until Sep 2024, HDR]
- Damien Marion [UNIV RENNES, Associate Professor, from Sep 2024]

PhD Students

- Clemence Chevignard [UNIV RENNES]
- Gael Claudel [INRIA, from Oct 2024]
- Mathieu Degre [UNIV RENNES, from Jan 2024]
- Quentin Edme [ORANGE, CIFRE, from Jan 2024]
- Baptiste Germon [UNIV RENNES, from Oct 2024]
- Aymeric Hiltenbrand [UNIV RENNES]
- Corentin Jeudy [ORANGE LABS, CIFRE, until Oct 2024]
- Thi Thu Quyen Nguyen [IDEMIA, CIFRE, until Oct 2024]
- Phuong Nguyen [UNIV RENNES]
- Guilhem Niot [PQSHIELD, CIFRE, from Apr 2024]
- Aurel Pichollet–Mugnier [INRIA, from Nov 2024]

Technical Staff

- Calvin Abou Haidar [UNIV RENNES, from Feb 2024 until Mar 2024]
- Daniel De Almeida Braga [UNIV RENNES, Engineer, from Apr 2024 until Aug 2024]
- Paul Kirchner [UNIV RENNES, from Sep 2024]
- Damien Marion [UNIV RENNES, until Aug 2024]
- Heorhii Pliatsok [INRIA, Engineer, from Apr 2024 until Aug 2024]

Interns and Apprentices

- Todd Cauet-Male [INRIA, Intern, from Jun 2024 until Sep 2024]
- Gael Claudel [UNIV RENNES, Intern, from Mar 2024 until Aug 2024]
- Paul Delhom [INRIA, Intern, from May 2024 until Oct 2024]
- Thibault Didier [UNIV RENNES, Intern, from Jun 2024 until Jul 2024]
- Baptiste Germon [UNIV RENNES, Intern, from Mar 2024 until Sep 2024]
- Rayan Lachguel [UNIV RENNES, Intern, until Mar 2024]
- Laz Panard [INRIA, Intern, from May 2024 until Oct 2024]
- Jules Rousseau [UNIV RENNES, Intern, from Apr 2024 until Sep 2024]

Administrative Assistant

- Isobelle Kelly [Inria, from Jan 2024]

External Collaborators

- Clément Dell'Aiera [DGA-MI, from Apr 2024]
- Marie Euler [DGA-MI, from Jan 2024]
- Mathieu Goessens [UNIV RENNES, from Sep 2024]
- Tuong-Huy Nguyen [DGA-MI, from Apr 2024]

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 or secure messaging, and on the security of databases.

3 Research program

3.1 Security against post-quantum attackers

The seminal paper of Peter Shor at FOCS 1994 [74] 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 on 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 on 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 served 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. [48, 73, 44].

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 [40], reducing module lattices as a generalization of the LLL algorithm in the ring of integers of a number field in [64] or in a tower of cyclotomic fields in [61]. We generalized the BKW algorithm to binary LWE setting in [62] and studied the Learning Parities with Noise (LPN) Problem in [65].

We have also attacked concrete cryptographic schemes. We broke some multivariate schemes such as the SFLASH signature schemes in [54] and variants [58], and the ASASA schemes in [69]. We have also broken FHE schemes based on overstretched NTRU parameters in [63] or concrete FHE in [49].

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 [37], 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 [50]. 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 have 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 NIST[1] in 2017 concluded in 2023

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

by selecting the lightweight cipher family Ascon [53], 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.

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 [45], Demirci-Selçuk attacks on AES [52], and impossible differential attacks [51].

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 [39], 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 [42].

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 [43]. 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 [41].

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 that 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 [60] to prove the security of implementations, secure theoretical foundations have been laid by Prouff and Rivain and later Duc et al. in [72, 55]. Soon after, some tools have been developed such as [31, 32, 30] 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 [33], where generally securing randomness presents an interesting challenge. We aim at extending the results of [33, 34, 68, 57] 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 to work 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) [46], 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 Gonzalvez, 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.

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 depreciate 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 [56], 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 [47]. We also studied the privacy of the EME standard (Encrypted Media Extensions) for Digital Rights Managments in browsers in [70].

5 Social and environmental responsibility

5.1 Impact of research results

After the discovery of some privacy issues in EME, our findings have been timely communicated to all concerned parties following responsible disclosure processes. Mozilla Firefox was quite responsive, and we got rewarded via their bug bounty program. The Mozilla EME team investigated our findings and released a patch to address the identified privacy issues and acknowledged us in the Mozilla Hall of Fame. Regarding Client ID being in clear in renewal requests, we first contacted the EME Chrome team that reviewed our disclosure report and showed concerns about its privacy consequence, namely the EME user-agent. They confirmed our intuition that the problem is caused by the Widevine CDM. Therefore, we filed a Widevine bug report about missing Privacy Mode on VMP systems, and are still in communication with them.

Concerning our micro-architectural attack on WPA3, we disclosed our findings to the hostap security team in December 2021. We contacted other affected projects (iwd/ell from Intel and FreeRadius) in January 2022. hostap promptly reacted, asking us to review a patch, which later was committed, and a security advisory has been published. Intel decided to fix their cryptographic library, ell, and also asked us to review their patch. Both iwd and hostap released a new stable version patching the vulnerability soon after our disclosure. FreeRadius has committed our patch to their project. We contacted OpenSSL and WolfSSL in May 2022 to disclose our second vulnerability. Both acknowledged our analysis, but argued that it is the developers' responsibility to avoid calling their leaky functions with secret-dependent values.

6 Highlights of the year

Our work on reducing the number of qubits in quantum algorithms for factoring and Discrete Logarithm [1] was accepted to the QIP 2025 (*Quantum information processing*) conference. It will be presented as a short plenary talk (the conference has only 13 plenary talks out of 138 in total).

7 New software, platforms, open data

7.1 New software

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 2024, the new pairing-friendly elliptic curves obtained in the work by Gasnier and Guillevic were included in the library as a few family of curves like BN, BLS or KSS. The library was extended to consider the curves selected in Aranha, Fotiadis and Guillevic at the 192-bit security level.

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 ALPINAC

Name: ALgorithmic Process for Identification of Non-targeted Atmospheric Compounds

Keyword: Chemistry

Functional Description: ALPINAC identifies up to 95% of the measured signal obtained from an Electron-Impact Time-of-Flight High Resolution Mass Spectrometer (EI ToF HRMS) on air sampling, without a-priori knowledge on the encountered chemical compounds, without database search. The software was successfully tested on mass spectrum ranging from 23 m/z to 330 m/z.

URL: https://gitlab.inria.fr/guillevi/alpinac

Publication: hal-03176025

Contact: Aurore Guillevic

Partner: EMPA

8 New results

8.1 Symmetric Cryptanalysis of Constructions

Key Committing Attacks against AES-based AEAD Schemes [7]

Participants: Patrick Derbez, Pierre-Alain Fouque, André Schrottenloher.

The security of authenticated encryption with associated data (AEAD) cryptosystems in the context of key commitment has been the topic of several recent works [67]. In this context, in addition to ensuring authenticity and confidentiality of the data, the cryptosystem should ensure that an adversary cannot produce two sets of key and messages that would be encrypted into the same ciphertext. This property appears to be particularly useful for real-world scenarios such as encrypted messaging. In this work, we show that the schemes AEGIS and Rocca-S are not key-committing.

Part of the results obtained in this work originated from our security analysis of Rocca-S, performed during 2023 under a contract with KDDI (Japan)

Improving Generic Attacks Using Exceptional Functions [11]

Participants: André Schrottenloher.

The paper [11] with Xavier Bonnetain (Inria team CARAMBA), Rachelle Heim Boissier and Gaëtan Leurent (Inria team COSMIQ) proposes new attacks on symmetric constructions using the statistical properties of random functions. The starting point is a technique of Gilbert et al. [59], who gave a new forgery attack on the Duplex authenticated encryption mode by finding exceptional random functions. These exceptional functions are those for which their graph admits a large component with an exceptionally small graph.

This work first improves the attack of Gilbert et al. from an asymptotic complexity $\mathcal{O}(2^{3c/4})$ to $\mathcal{O}(2^{2c/3})$, where c is the capacity of the Duplex, using *nested* exceptional functions. Then, new generic attacks against Merkle-Damgård hash combiners are introduced, which improve the complexities of the best existing attacks on the XOR combiner, Zipper Hash and Hash-Twice.

8.2 Symmetric Cryptanalysis of Primitives and Tools

A Generic Algorithm for Efficient Key Recovery in Differential Attacks - and its Associated Tool [12]

Participants: Patrick Derbez.

The paper [12] presents a new algorithm dedicated to the key recovery of differential attacks. This algorithm, under some assumptions on the ciphers, allows to determine the optimal order in which the key bits involved in the key recovery should be guessed. We also propose an efficient implementation of this algorithm, the KiRiDi tool, and improved several differential attacks. We have made this tool available on the Inria Gitlab platform.

Alternative Key Schedules for the AES [13]

Participants: Patrick Derbez.

In the paper [13] we study alternative key schedules for the different versions of the AES. We focused on permutations and differential cryptanalysis. The main result of this paper is the new framework we introduce to search for the best permutation to be used as a key schedule. Our approach relies on two MILP models, one to generate permutations and a second to search for differential characteristics activating less than b active S-boxes, b being given by the user. Each time the second model finds a differential characteristic, a constraint is added to the first model such that all the next permutations it will generate cannot lead to the same characteristic. As a result we propose new key schedules for all three versions of AES that improve the resistance against differential cryptanalysis.

Revisiting Differential-Linear Attacks via a Boomerang Perspective with Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck, and SERPENT [16]

Participants: Patrick Derbez.

In the paper [16], we show the similarities between two cryptanalysis techniques: boomerang attacks and differential-linear attacks. We then use this to propose new models to search the best differential-linear distinguishers on a large number of ciphers. As a result we found many new distinguishers, improving the best known results regarding this cryptanalysis technique.

Equivalence of Generalised Feistel Networks [6]

Participants: Patrick Derbez, Marie Euler.

Generalized Feistel Networks (GFN) are defined by their internal branch-permutations. To find the best GFN, we thus have to exhaust the space of permutations which grows exponentially with the number of branches. To reduce the number of permutations to study it is important to rely on equivalence classes. Therefore in the work [6] we propose a new equivalence class regarding the diffusion round, which is the number of rounds required to achieve full diffusion. As a result, the search space is much smaller than with previous approaches and we were able to find better permutations for the cipher WARP.

Cryptanalysis of Full-Round BipBip [9]

Participants: Patrick Derbez.

Cryptographic Capability Computing (C3) is the first stateless memory safety mechanism that eliminates the need for additional metadata storage. C3 relies on an ultra-low-latency cipher to prevent load delays, requiring a block size as small as 24 bits. This is the context in which the block cipher BipBip was designed. In the paper [9] we mount an advanced meet-in-the-middle attack against the full cipher, showing that the security offered by BipBip is lower than expected by its designers.

8.3 Quantum Algorithms and Cryptanalysis

Does quantum lattice sieving require quantum RAM? [24]

Participants: Yixin Shen.

This paper studies the requirement for quantum random access memory (QRAM) in quantum lattice sieving, a fundamental algorithm for lattice-based cryptanalysis.

First, we obtain a lower bound on the cost of quantum lattice sieving with a bounded size QRAM. We do so in a new query model encompassing a wide range of lattice sieving algorithms similar to those in the classical sieving lower bound by Kirshanova and Laarhoven [CRYPTO 21]. This implies that, under reasonable assumptions, quantum speedups in lattice sieving require the use of QRAM. In particular, no quantum speedup is possible without QRAM.

Second, we investigate the trade-off between the size of QRAM and the quantum speedup. We obtain a new interpolation between classical and quantum lattice sieving. Moreover, we show that further improvements require a novel way to use the QRAM by proving the optimality of some subroutines. An important caveat is that this trade-off requires a strong assumption on the efficient replacement of QRAM data, indicating that even speedups with a small QRAM are already challenging.

Finally, we provide a circuit for quantum lattice sieving without using QRAM. Our circuit has a better depth complexity than the best classical algorithms but requires an exponential amount of qubits. To the best of our knowledge, this is the first quantum speedup for lattice sieving without QRAM in the standard quantum circuit model. We explain why this circuit does not contradict our lower bound, which considers the query complexity.

Single-Query Quantum Hidden Shift Attacks [4]

Participants: André Schrottenloher.

This paper with Xavier Bonnetain (Inria team CARAMBA) introduces a new family of quantum attacks in the *superposition* query model (also named Q2 in the literature), which perform forgery or key-recovery for some authenticated encryption (AE) schemes.

Traditionally Q2 attacks use a period-finding algorithm such as Simon's algorithm to recover some secret information. The exponential acceleration offered by such algorithms, they allow to break some classically secure primitives. However, such breaks require superposition query access, which is a rather theoretical model (in particular, the schemes attacked in our paper remain secure against standard quantum adversaries).

In this paper, we use a different period-finding algorithm than Simon's, allowing to succeed in some cases where only *one* such superposition query is allowed, usually as the result of using a *nonce* in the mode. This leads to attacks against Rocca, Rocca-S, Tiaoxin-346 and AEGIS-128L.

Quantum Procedures for Nested Search Problems: with Applications in Cryptanalysis [8]

Participants: André Schrottenloher.

In this paper we study the family of *nested search* algorithms, which often arise in the context of cryptanalysis. These algorithms perform an exhaustive search in several layers, where each layer introduces a new degree of freedom and / or constraints.

While it is well known that Grover's algorithm and Amplitude Amplification speed up generically these nested searches, the analysis of such algorithm has often been performed in a case-by-case manner. To remedy this issue, and allow for an easier estimation of the overall complexities, we introduce a generic framework and tools to transform a classical nested search into a quantum procedure. We give generic complexity formulas and reach further improvements using numerical optimization. We demonstrate our framework by giving a tighter analysis of quantum attacks on reduced-round versions of the block cipher AES.

Reducing the Number of Qubits in Quantum Information Set Decoding. [14]

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

This paper optimizes the number of qubits used in the quantum variant of Prange's Information Set Decoding (ISD) algorithm, which was originally proposed by Bernstein [38]. This algorithm is especially important for post-quantum cryptography, as it largely determines the level of quantum security that one can expect from code-based cryptosystems.

This algorithm has a very simple structure: it performs a Grover search which, at each iteration, inverts a matrix. Our contribution focuses on the matrix inversion circuit. Here, we show that this inversion can be performed in an implicit way, reducing the number of qubits from quadratic to linear in the code length (i.e., the security parameter of the cryptosystem). We give several trade-offs and perform a precise estimation of the resources required by this circuit, which is supported by a full implementation. We have made this implementation available on the Inria Gitlab platform. As an example, while the computational complexity remains asymptotically unchanged, our new trade-offs reduce the number of qubits from millions to tens of thousands in attacking the Classic McEliece scheme.

Reducing the Number of Qubits in Quantum Factoring. [20]

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

This paper obtains a significant reduction in the number of qubits in Shor's factoring algorithm. The main idea of the paper is to realize explicitly the *output compression* technique of May and Schlieper [66]. Indeed, Shor's algorithm needs to find the period of a modular exponentiation function: the space then depends on the size of the input ($\mathcal{O}(n)$ bits), the size of the output (n bits for n-bit numbers) and the additional space needed for performing reversible arithmetic operations. May and Schlieper showed that the algorithm will still work if one reduces the output size. Whether this could be used to reduce the *total space* was so far an open question.

In this work, we designed a new classical reversible circuit for the operation $x \to (a^x \pmod N) \pmod{2^r}$, where a, N, r are fixed, and r is a constant, using only $\mathcal{O}(\log\log N)$ space in addition to the size of x. This circuit, which is based on a Residue Number System, allows the effective compression of the output space in Shor's algorithm, leading to the smallest numbers of qubits for factoring RSA moduli known to date. Indeed we estimate that only 1730 qubits would be needed to factor RSA-2048, at the expense of an increase in gate count (while the asymptotic cost remains $\mathcal{O}((\log N)^3)$).

In order to perform precise resource estimates, we have fully implemented the circuits and made these implementations available on the Inria Gitlab platform. The full version of the paper is currently a preprint and it will be presented as a plenary talk in the upcoming QIP 2025 conference [1].

8.4 Public-key cryptography

8.4.1 Lattices

Smoothing Parameter and Shortest Vector Problem on Random Lattices [27]

Participants: Yixin Shen.

Lattice problems have many applications in various domains of computer science. There is currently a gap in the understanding of these problems with respect to their worst-case complexity and their average-case behaviour. For instance, the Shortest Vector problem (SVP) on an n-dimensional lattice has worst-case complexity $2^{n+o(n)}$ [29]. However, in practice, people rely on heuristic (unproven) sieving algorithms of time complexity $2^{0.292n+o(n)}$ [35] to assess the security of lattice-based cryptography schemes. Those heuristic algorithms are experimentally verified for lattices used in cryptography, which are usually random in some way[2].

In this paper [27], we try to bridge the gap between worst-case and heuristic algorithms. Using the formalism of random real lattices developed by Siegel [75], we show a tighter upper bound on an important lattice parameter called the smoothing parameter that applies to almost all random lattices. This allows us to obtain a $2^{n/2+o(n)}$ time algorithm for an approximation version of the SVP on random lattices with a small constant approximation factor.

Discrete gaussian sampling for BKZ-reduced basis [22]

Participants: Yixin Shen.

Discrete Gaussian sampling on lattices is a fundamental problem in lattice-based cryptography. In this paper [22], 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 Assuption (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 [71] 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.

Flood and Submerse: Distributed Key Generation and Robust Threshold Signature from Lattices [15]

Participants: Guilhem Niot.

We propose a new framework based on random submersions — that is projection over a random subspace blinded by a small Gaussian noise — for constructing verifiable short secret sharing and showcase it to construct efficient threshold lattice-based signatures in the hash-and-sign paradigm, when based on noise flooding. This is, to our knowledge, the first hash-and-sign lattice-based threshold signature. Our threshold signature enjoys the very desirable property of robustness, including at key generation. In practice, we are able to construct a robust hash-and-sign threshold signature for threshold

[2] There exists several formal notions of random lattices.

and provide a typical parameter set for threshold T = 16 and signature size 13kB. Our constructions are provably secure under standard MLWE assumptions in the ROM and only require basic primitives as building blocks. In particular, we do not rely on FHE-type schemes.

Computing e-th roots in number fields [10]

Participants: Pierre-Alain Fouque.

We describe several algorithms for computing e-th roots of elements in a number field K, where e is an odd prime-power integer. In particular, we generalize Couveignes' and Thomé's algorithms originally designed to compute square-roots in the context of the General Number Field Sieve algorithm for integer factorization. Our algorithms cover most cases of e and K and their complexity is better than general root finding algorithms. Our (publicly available) Python implementation compares extremely well in performance to the implementation of these generic algorithms in well-known computer algebra softwares, allowing us to obtain reasonable timings even for large degree number fields and huge exponents e, which correspond to previously intractable cases using these softwares.

One important application of our algorithms consists in computing S-unit groups used by the Twisted-PHS algorithm for the cryptanalysis of the Ideal-SVP problem over cyclotomic fields in post-quantum cryptography. Indeed, in order to assess concretely the efficiency of these so-called S-unit attacks, it is necessary to compute S-unit groups in meaningfully large dimensions, say over a few hundreds. As proposed by Bernard et al. in Asiacrypt 2022 [36], in cyclotomic fields this can be achieved by first considering S-units coming from the maximal totally real subfield and Stickelberger generators; then, a saturation step is required, which comes down to computing e-th roots where e is a — potentially huge — prime-power factor of the relative class number, our largest example being a 93-bits prime e. This paper tackles all cases, except for a few small e's, allowing explicitly computing full S-unit groups even in dimension 200. To our knowledge, this had never been achieved before for general (non-smooth) conductors, and clears the path towards further cryptanalytic investigations.

Phoenix: Hash-and-Sign with Aborts from Lattice Gadgets [18]

Participants: Corentin Jeudy.

Preimage sampling is a fundamental tool in lattice-based cryptography, and its performance directly impacts that of the cryptographic mechanisms relying on it. In 2012, Micciancio and Peikert proposed a new way of generating trapdoors (and an associated preimage sampling procedure) with very interesting features. Unfortunately, in some applications such as digital signatures, the performance may not be as competitive as other approaches like Fiat-Shamir with Aborts. In an effort to improve preimage sampling for Micciancio-Peikert (MP) trapdoors, Lyubashevsky and Wichs (LW) introduced a new sampler which leverages rejection sampling but suffers from strong parameter requirements that hampered performance. As a consequence it seemed to be restricted to theoretical applications and has not been, to our knowledge, considered for real-world applications.

Our first contribution is to revisit the LW sampler by proposing an improved analysis which yields much more compact parameters. This leads to gains on the preimage size of about 60% over the LW sampler, and up to 25% compared to the original MP sampling technique. It thus sheds a new light on the LW sampler, opening promising perspectives for the efficiency of advanced lattice-based constructions relying on such mechanisms. To provide further improvements, we show that it perfectly combines with the approximate trapdoors approach by Chen, Genise and Mukherjee, but with a smaller preimage error.

Building upon those results, we introduce a hash-and-sign signature scheme called Phoenix. The scheme is based on the M-LWE and M-SIS assumptions and features attractive public key and signature sizes which are even smaller than those of the most recent gadget-based construction Eagle of Yu, Jia and Wang (Crypto'23). Moreover, Phoenix is designed to support a broad variety of distributions (uniform, spherical Gaussian, etc.) which can facilitate implementation, in particular in constrained environments.

Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields [19]

Participants: Georgii Pliatsok, Alexandre Wallet.

The Lattice Isomorphism Problem (LIP) is a classical topic in the algorithmic geometry of numbers. It consists informally in computing an isometry between two lattices L and L' (if there is one), and it is believed to be hard in general even for quantum attackers. Up to recently, it had not appeared as a hardness assumption in public-key cryptography. At Asiacrypt'2022, Ducas et al. proposed Hawk, a digital signature scheme relying on the hardness of computing an isometry between *algebraic* lattices. The lattices underlying the scheme correspond to rank 2 modules over power-of-two cyclotomic fields. While it can be hoped that the large group of symmetries stemming for the algebraic setting could be leveraged into powerful attacks, the cryptanalysis against this algebraically structured variant of the problem remained essentially unexplored.

Our work proposes a first step in that direction. We break a different, but close, variant of the problem when the lattices correspond to rank 2 modules over a *totally real* number field — such fields appear naturally as a large subfield in any power-of-two cyclotomic field. More precisely, we provide a polynomial time heuristic algorithm to solve the problem, and an implementation mixing `sagemath` and `pari-gp` to support the validity of our attack. This does not affect Hawk, but it provides insights on the hardness of its corresponding problem.

8.4.2 Elliptic curves

Participants: Aurore Guillevic.

A short-list of pairing-friendly curves resistant to the Special TNFS algorithm at the 192-bit security level The paper [2] is an overview of pairing-friendly elliptic curves at the (classical) 192-bit security level, that can be of interest for hybridation. It comes with a security analysis with respect to a discrete logarithm computation with the Tower Number Field Sieve algorithm (TNFS) in the target finite field of the elliptic curves. For practical considerations, the curves are implemented and benchmarked within the open-source library RELIC toolkit.

Embedded Curves and Embedded Families for SNARK-Friendly Curves With Simon Masson, the paper [26] generalizes the Bandersnatch curve construction and analyses the scarcity of such curves. These curves are used in Succinct Non-interactive ARguments of Knowledge (SNARK).

An algebraic point of view on the generation of pairing-friendly curves The paper [25] 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. 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. The paper is under review for a journal and was updated in 2024 to suit the reviewers comments.

8.5 Side-Channel Attacks

Masking the GLP Lattice-Based Signature Scheme at Any Order [3]

Participants: Pierre-Alain Fouque.

This paper is the journal version of a Eurocrypt 2018 paper. Recently, numerous physical attacks have been demonstrated against lattice-based schemes, often exploiting their unique properties such as the reliance on Gaussian distributions, rejection sampling and FFT-based polynomial multiplication. As the call for concrete implementations and deployment of postquantum cryptography becomes more pressing, protecting against those attacks is an important problem. However, few countermeasures have been proposed so far. In particular, masking has been applied to the decryption procedure of some lattice-based encryption schemes, but the much more difficult case of signatures (which are highly nonlinear and typically involve randomness) has not been considered until now. In this paper, we describe the first masked implementation of a lattice-based signature scheme. Since masking Gaussian sampling and other procedures involving contrived probability distributions would be prohibitively inefficient, we focus on the GLP scheme of Güneysu, Lyubashevsky and Pöppelmann (CHES 2012). We show how to provably mask it in the Ishai–Sahai–Wagner model (CRYPTO 2003) at any order in a relatively efficient manner, using extensions of the techniques of Coron et al. for converting between arithmetic and Boolean masking. Our proof relies on a mild generalization of probing security that supports the notion of public outputs. We also provide a proof-of-concept implementation to assess the efficiency of the proposed countermeasure.

8.6 Real-World Cryptography

They're not that hard to mitigate: What Cryptographic Library Developers Think About Timing Attacks [17]

Participants: Daniel de Almeida Braga, Pierre-Alain Fouque.

This paper is a survey we set up to ask 44 developers of 27 widespread cryptographic libraries about their awareness and practices regarding side-channel threats. Side channel attacks have been known for decades, but still plague current cryptographic implementations, and not a year passes without new published attacks, targeting widespread implementation. Most academic work toward solving these issues focuses on suggesting new designs that are not affected by these attacks, or providing analysis tools to detect them. The residual side channel vulnerabilities reflect a gap between academic research and real-world engineering. The goal of this survey is to understand the source of that gap, and identify ways to reduce it, by asking feedback to the very people who will handle the practical deployment of solutions. The main findings highlight a leaky pipeline in the process of treating the cause of side-channels: all candidates were aware of the side-channel threat, but only part of them included it in the threat model, to prioritize other issues. Some of the main aspects hindering the use of academic tools include their usability, and lack of consideration to real-world constraints (CI/CD, delta mode, ...). Based on these observations, we made a list of recommendations addressed to tool developers and library developers.

"These results must be false": A usability evaluation of constant-time analysis tools [21]

Participants: Daniel de Almeida Braga, Pierre-Alain Fouque.

The paper [21] is a follow-up study on our previous work [17]. In the first work, we higlighted usability as one of the main hinderance to the constant-time anlysis tool's deployment. The goal of this paper is to study the elements that make this specific class of tool "usable". As the previous paper focused on a survey, asking theoretical questions, we designed this study to gain knowledge on practical elements related to tools usage. To do so, we conducted a two-part usability study on 6 tools across various tasks that emulate the learning of each tool on textbook exercises, and on real-world contexts. We found that

all tools face similar usability issues at different levels, hindering their use in all cases. Based on these observations, we addressed a series of recommendations, as a checklist for future tool developers, and complemented the documentation and bootstrapping of the tools involved in our study, to ease future use.

9 Bilateral contracts and grants with industry

9.1 Bilateral Grants with Industry

- **Resque**: (T0: 09/2022 –> 08/2026)
  BPi France project.
  Lead by Thales.

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

  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.

- **Hyperform**: (T0: 09/2022 –> 08/2026)

  Participants: Alexandre Wallet, Heorhii Pliatsok.

  BPi France project.
  Lead by Idemia.
  Participating entities on the industrial side: Idemia, Atempo, PrimX, CryptoNext, Sinacktiv. Participating entities on the public side: Inria, ANSSI, CEA.
  In this project, Inria is represented by two teams: Grace (Inria Saclay), with Ben Smith as the coordinator; and Capsule (Inria Rennes), with Alexandre Wallet as collaborator.
  Hyperform aims at being an international leading force in the development of quantum-resilient secure elements for embedded systems, as well as a primary actor in the design of hybrid solutions at scale, that is, mixing pre- and post-quantum cryptography in a provably secure way, formally verified, into industrial products. One essential goal of the project is to produce a demonstrator: a secure element with dedicated hardware/software embedding post-quantum cryptographic algorithms, providing a level of resilience against side-channel attackers while maintaing a high level of performance on par with the demands of real-world situations.

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

  Participants: Andre 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 European initiatives

10.1.1 Horizon Europe

- **ERC SoBaSyC** (2024 –> 2029)

Participants: Patrick Derbez (Expert Contributor, involved at 20%).

Symmetric cryptography, essential for enabling secure communications, has benefited from an explosion of new results in the last two decades, in big part due to several standardization efforts: many public competitions have been launched since 1997, where the community proposes cryptographic constructions and simultaneously evaluates their security and performance. The security of symmetric cryptography is based on cryptanalysis: we only gain confidence in a symmetric cryptographic function through extensive and continuous scrutiny. However, the current context has not allowed the community to digest all the new findings, as can be seen from several recurrent issues. The two main ones are: 1) primitives proposed at top-tier venues often get broken by slight modifications of already known techniques; 2) published cryptanalysis at top conferences sometimes include mistakes, are not optimal, or are often re-invented and re-named. The main challenge of SoBaSyC is to establish solid bases for symmetric cryptography.

Using cryptanalysis as the starting point, the aim is to unify the knowledge obtained through the years on the different families of attacks, to transform it with an algorithmic approach and to endow it with optimizations. The final result will be a toolbox congregating all our newly proposed optimized algorithms, that will provide the best known attacks on a given construction, through an easy application. Next, the plan is to derive from this algorithmic approach some theoretical bounds, as well as some properties that will be included in the security proofs of symmetric constructions, providing more meaningful and realistic security arguments. This would allow, for the first time, to ensure that any newly proposed primitive or construction is already resistant to all known attacks, and will considerably increase the confidence on these functions. It will also save a considerable amount of time and allow the field to advance, at last, on solid ground.

The PI of this project is María Naya-Plasencia from the Inria team COSMIQ.

10.2 National initiatives

- **The PQTLS** (01/2022 –> 12/27)

Participants: Alexandre Wallet, Pierre-Alain Fouque, André Schrottenloher, Yixin Shen, Clemence Chevignard.

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 –> 12/28)

  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.

- **ANR AMIRAL** (01/2022 –> 12/2024)
  Digital signatures from lattice-based assumptions
  ANR ASTRID, Appel 2021
  Partners: GREYC (Caen), Inria Lyon
  The focus of AMIRAL is the improvement of lattice-based digital signature schemes at large. More precisely, three research axes are considered. First, we will design concrete improvements and novel tweaks for the optimization of NIST's selected candidates (Falcon and Dillithium) or to extend their use cases to a larger surface of scenarios. Second is the conception and study of signatures with advanced properties (such as: aggregated, threshold, ...) in order to substantially improve the state-of-the-art. Third, the study of the interplay between the improvements in the design of signatures and the efficiency of broader, more complex cryptographic primitives such as attribute-based encryption.

- **CROWD** (2023 –> 2027).

  Participants: Pierre-Alain Fouque, Andre Schrottenloher, Clemence 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, with the goal of entering the next turn of the NIST standardization.

- **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. IDROMEL will produce:

- **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: 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 a 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

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

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

Member of the organizing committees

- Séminaire CRYPTO (IRMAR, IRISA, Rennes): Aurore Guillevic, Damien Marion, André Schrottenloher, Yixin Shen
- Séminaire Joint CRYPTO en ligne (ENSL, CWI, KCL, IRISA): Yixin Shen

11.1.2 Scientific events: selection

Chair of conference program committees

- EUROCRYPT 2025: Pierre-Alain Fouque (Program co-chair)

Member of the conference program committees

- EUROCRYPT 2024 (May 26-30, 2024, Zurich, Switzerland): Patrick Derbez, Pierre-Alain Fouque (Area Chair), André Schrottenloher
- CRYPTO 2024 (August 18-22, 2024, Santa Barbara, USA): André Schrottenloher
- CRYPTO 2024 artifact evaluation committee: André Schrottenloher
- Inscrypt 2024 (December 14-16, 2024, Kunming, China): Patrick Derbez, André Schrottenloher
- INDOCRYPT 2024 (December 18-21, 2024, Chennai, INDIA): Yixin Shen
- QUEST-IS 2025 (December 1-4th, 2025, Saclay, France): André Schrottenloher
- Selected Areas in Cryptography 2024 (August 26-30, 2024, Montréal, Québec): Aurore Guillevic
- PKC 2025 (May 12-15, 2025, Røros, Norway): Aurore Guillevic

Reviewer

- André Schrottenloher: INDOCRYPT 2024, QIP 2024, TQC 2024, Nature Scientific Reports

11.1.3 Journal

Member of the editorial boards

- *Transactions on Symmetric Cryptology (ToSC)* associate editor: André Schrottenloher (2023-2024 and 2024-2025)

Reviewer - reviewing activities

- *Design, Codes and Cryptography*: André Schrottenloher

11.1.4 Invited talks

- Pierre-Alain Fouque - Summer School on PQC co-organized with IACR, 2 talks on Quantum Factorization and Falcon signature, July 14-17, 2024, Warsaw, Poland
- Pierre-Alain Fouque - Summer School on PQC - *Introduction to lattice-based cryptography*, 2 courses, September 9-13, 2024, Corsica, France
- Pierre-Alain Fouque - *Post-Quantum Cryptography* Journée Scientifique Inria, August 28-30, 2024, Grenoble, France
- Pierre-Alain Fouque - *Transition Post-Quantique* - Journée scientifique du PEPR Cybersécurité, December 11, 2024, Campus Cyber, Paris, France
- Patrick Derbez - *KiRiDi Tool for Key recovery in Differential attacks* - Dagsthul Seminar, January 21-26, 2024, Dagsthul, Germany
- Aurore Guillevic - *Elliptic curves for SNARK and proof systems* - Journées Numération, Arithmétique, Cryptographie February 29 – March 1st 2024, Jussieu, Paris, to celebrate the retirement of Jean-Claude Bajard
- André Schrottenloher - *Quantum Security of Symmetric Cryptosystems* - QSI Spring School on post-quantum cryptography, March 12-15, 2024, Porto (Portugal)
- Patrick Derbez - *Alternative Key Schedules for the AES* - September 25, 2024, NTT, Japan
- Aurore Guillevic - *Introduction on Elliptic Curves, Introduction on Pairings and on the CM Method* - School on Elliptic Curve Cryptography (ECC), Taipei, Taiwan, October 28-29, 2024
- Aurore Guillevic - *Elliptic Curves for SNARK and Proof Systems* - ECC 2024, Taipei, Taiwan, October 30 - November 1, 2024
- André Schrottenloher - *Single-query Quantum Hidden Shift Attacks* - ASK 2024, Kolkata, India, December 14-17, 2024
- Patrick Derbez - *Alternative Key Schedules for the AES* - ASK 2024, Kolkata, India, December 14-17, 2024

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Master: Pierre-Alain Fouque, Advanced Course in Cryptography for security (BCS), 16 hours, M2, University of Rennes, France;
- Master: Pierre-Alain Fouque, Basic Course in Cryptography (BC), 12 hours, M1, University of Rennes, France;
- Master: Pierre-Alain Fouque, Design and Analysis of Algorithm (ADA), 32 hours, M1, University of Rennes, France;
- Master: Pierre-Alain Fouque, Security Proof, 7,5 hours, M2, University of Rennes, France;
- Master: Pierre-Alain Fouque, Security of Data (SDATA), 12 hours, M1, University of Rennes.
- Master: André Schrottenloher, Enjeux de la cryptographie post-quantique, 7.5h eqTD, Centrale-Supélec Rennes
- Engineer cycle: André Schrottenloher, Théorie de la cryptologie - Introduction à la cryptographie post-quantique, 15h eqTD, IMT Atlantique
- Master: Aurore Guillevic, 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, 6 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, Low Level Programming (LLP), 19.5 hours lab sessions, M1, University of Rennes, France;
- Master: Daniel De Almeida Braga, Project Security, 24 hours eqTD, M1, University of Rennes, France;
- Master: Daniel De Almeida Braga, Basic Course in Cryptography (BC), 12 hours lab sessions, M1, University of Rennes, France;
- Bachelor: Daniel De Almeida Braga, Introduction à la Securité (ISE), 1.5 hour lecture, 3 hours lab sessions, L1, University of Rennes, France;
- Bachelor: Patrick Derbez, Introduction à la Sécurité (ISE), 5.25 hours eqTD, L1, University of Rennes, France;
- Bachelor: Patrick Derbez, Introduction à la Programmation Impérative (IPI), 28.5 hours eqTD, L1, University of Rennes, France;
- Bachelor: Patrick Derbez, Algorithmique et Complexité (ACO), 56.25 hours eqTD, L2, University of Rennes, France;
- Bachelor: Patrick Derbez, Arithmétique pour la cybersecurite (ARIC), 18 hours eqTD, L2, University of Rennes, France;
- Master: Patrick Derbez, Project Security, 24 hours eqTD, M1, University of Rennes, France;

- Master: Patrick Derbez, Cryptanalyse, 24 hours eqTD, M2, University of Rennes, France;
- Master: Damien Marion, Security of Data (SDATA), 32 hours, M1, University of Rennes;
- Master: Damien Marion, Secured Implementation for Cryptography (SIMP), 25 hours, M2, University of Rennes (with students from INSA, IMT-Atlantique and CentraleSupélec rennes).
- Bachelor: Damien Marion, Enjeux sociétaux et empreinte écologique du numérique (3EN), 18 hours, L3, University of Rennes, France;
- Master: Damien Marion, project supervision, 12 hours, M1, University of Rennes;
- Master: Damien Marion, database security, 12 hours, M1, University of Rennes;
- André Schrottenloher was Oral examiner for fundamental computer science in the entrance examinations of the ENS (Écoles Normales Supérieures). (20 hours of examinations).

11.2.2 Supervision

- PhD: Corentin Jeudy, *Design of Advanced Post-Quantum Signature Schemes*, Defended on June 18th, 2024. Supervisors: Pierre-Alain Fouque and Adeline Roux-Langlois.
- PhD: Thi Thu Quyen Nguyen, *Déploiements des signatures fondées sur les réseaux euclidiens*, Defended on December 12, 2024. Supervisors: Adeline Roux-Langlois (GREYC, Caen), Paul Dischamp (Idemia) and Alexandre Wallet.
- PhD in progress: Phuong Hoa Nguyen, *MILP and symmetric-key cryptanalysis*, started October 2021. Supervisors: Patrick Derbez 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: 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: Guenael Renault (ANSSI), Pierre-Alain Fouque.
- PhD in progress: Guilhem Niot, Threshold Post-Quantum Cryptography. Supervisors: Pierre-Alain Fouque and Thomas Prest (PQShield).
- Internship: Baptiste Germon (M2): *On the quasidifferential framework* (April - September 2024). Supervisor: Patrick Derbez
- Internship: Gaël Claudel (M2)
- Internship: Todd Cauet-Male
- Internship: Jules Rousseau (M2): *Cube cryptanalysis of Ascon and Gift* (April-September 2024). Supervisors: André Schrottenloher, Patrick Derbez

- Internship: Laz Panard (M2): *Se débarrasser de l'arithmétique à virgule flottante : Preuve de concept et benchmarking du cryptosystème de signature numérique $\mathbb{Z}$alcon* (May-October 2024). Supervisors: Aurore Guillevic, Daniel De Almeida Braga, Pierre-Alain Fouque
- Internship: Thibault Didier (L3): *Optimisation d'un circuit multi-somme réversible pour la factorisation quantique* (June-July 2024). Supervisor: André Schrottenloher

11.2.3 Juries

- Pierre-Alain Fouque was a reviewer of the PhD thesis of Clara Pernot (February 2, 2024, Inria Paris and Université Paris Cité, France).
- Pierre-Alain Fouque was a member (advisor) for the Ph.D. thesis committee of Corentin Jeudy (June 18, 2024, Université de Rennes, France).
- Pierre-Alain Fouque was reviewer for the Ph.D. thesis of Augustin Bariant (June 27, 2024, Sorbonne Université, France).
- Pierre-Alain Fouque was reviewer for the Ph.D. thesis of Pouria Fallahpour (July 5, 2024, École normale supérieure de Lyon, France).
- Pierre-Alain Fouque was member for the Ph.D. thesis committee of Margot Funk (October 14, 2024, Université de Versailles-Saint-Quentin-en-Yvelines, France).
- Pierre-Alain Fouque was president of the Ph.D. thesis committee of Rachelle Heim Boissier (October 15, 2024, Université Paris-Saclay, France).
- Pierre-Alain Fouque was member for the Ph.D. thesis committee of Hugo Beguinet (November 18, 2024, Université Paris sciences et lettres, France).
- Yixin Shen was member (examinor) for the Ph.D. thesis committee of Clément Ducros (November 12, 2024, Université Paris Cité).

11.3 Popularization

11.3.1 Participation in Live events

- André Schrottenloher was a panelist at the event Techno conférence Voyage au centre du Quantique - Capteurs, Communications, Informatique organized by Images et Réseaux (April 4th, 2024)

12 Scientific production

12.1 Major publications

[1] C. Chevignard, 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, 24th Feb. 2025. URL: https://inria.hal.science/hal-04848612 (cit. on pp. 10, 15).

12.2 Publications of the year

International journals

[2] D. F. Aranha, G. Fotiadis and A. Guillevic. 'A short-list of pairing-friendly curves resistant to the Special TNFS algorithm at the 192-bit security level'. In: *IACR Communications in Cryptology* 1.3 (4th Oct. 2024), p. 44. URL: https://inria.hal.science/hal-04666521 (cit. on p. 17).

[3] 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: *Journal of Cryptology* 37.1 (1st Jan. 2024), p. 5. DOI: 10.1007/s00145-023-09485-z. URL: https://hal.science/hal-04832806 (cit. on p. 17).

[4] X. Bonnetain and A. Schrottenloher. 'Single-Query Quantum Hidden Shift Attacks'. In: *IACR Transactions on Symmetric Cryptology* 2024.3 (6th Sept. 2024), pp. 266–297. DOI: 10.46586/tosc.v2024.i3.266-297. URL: https://inria.hal.science/hal-04773920 (cit. on p. 13).

[5] D. Chakraborty, H. Hadipour, P. H. Nguyen and M. Eichlseder. 'Finding Complete Impossible Differential Attacks on AndRX Ciphers and Efficient Distinguishers for ARX Designs'. In: *IACR Transactions on Symmetric Cryptology* 2024.3 (6th Sept. 2024), pp. 84–176. DOI: 10.46586/tosc.v2024.i3.84-176. URL: https://inria.hal.science/hal-04869476.

[6] P. Derbez and M. Euler. 'Equivalence of Generalised Feistel Networks'. In: *IACR Transactions on Symmetric Cryptology* 2024 (1st Mar. 2024), pp. 412–440. DOI: 10.46586/tosc.v2024.i1.412-440. URL: https://inria.hal.science/hal-04827042 (cit. on p. 12).

[7] P. Derbez, P.-A. Fouque, T. Isobe, M. Rahman and A. Schrottenloher. 'Key Committing Attacks against AES-based AEAD Schemes'. In: *IACR Transactions on Symmetric Cryptology* 2024.1 (1st Mar. 2024), pp. 135–157. DOI: 10.46586/tosc.v2024.i1.135-157. URL: https://inria.hal.science/hal-04773876 (cit. on p. 11).

[8] A. Schrottenloher and M. Stevens. 'Quantum Procedures for Nested Search Problems: with Applications in Cryptanalysis'. In: *IACR Communications in Cryptology* (7th Oct. 2024), pp. 1–38. DOI: 10.62056/aee0fhbmo. URL: https://inria.hal.science/hal-04773898 (cit. on p. 14).

[9] J. Wang, C. Boura, P. Derbez, K. Hu, M. Li and M. Wang. 'Cryptanalysis of Full-Round BipBip'. In: *IACR Transactions on Symmetric Cryptology* 2024.2 (2024), pp. 68–84. DOI: 10.46586/tosc.v2024.i2.68-84. URL: https://hal.science/hal-04645510 (cit. on p. 13).

International peer-reviewed conferences

[10] O. Bernard, P.-A. Fouque and A. Lesavourey. 'Computing e -th roots in number fields'. In: ALENEX 2024 - SIAM Symposium on Algorithm Engineering and Experiments. Alexandria, United States: Society for Industrial and Applied Mathematics, 4th Jan. 2024, pp. 207–219. DOI: 10.1137/1.9781611977929.16. URL: https://hal.science/hal-04832783 (cit. on p. 16).

[11] X. Bonnetain, R. Heim Boissier, G. Leurent and A. Schrottenloher. 'Improving Generic Attacks Using Exceptional Functions'. In: *LNCS*. CRYPTO 2024 - 44th Annual International Cryptology Conference. Vol. 14923. Santa Barbara, United States: Springer, 2024, pp. 105–138. DOI: 10.1007/978-3-031-68385-5_4. URL: https://hal.science/hal-04724605 (cit. on p. 11).

[12] C. Boura, N. David, P. Derbez, R. Heim Boissier and M. Naya Plasencia. 'A Generic Algorithm for Efficient Key Recovery in Differential Attacks – and its Associated Tool'. In: EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14651. Lecture Notes in Computer Science. Zurich, Switzerland: Springer Nature Switzerland, 29th Apr. 2024, pp. 217–248. DOI: 10.1007/978-3-031-58716-0_8. URL: https://hal.science/hal-04598635 (cit. on p. 12).

[13] C. Boura, P. Derbez and M. Funk. 'Alternative Key Schedules for the AES'. In: *LNCS : Applied Cryptography and Network Security*. ACNS 2024 - 22nd International Conference on Applied Cryptography and Network Security. Vol. 14584. Abu Dhabi, United Arab Emirates, 2024, pp. 485–506. DOI: 10.1007/978-3-031-54773-7_19. URL: https://hal.science/hal-04683785 (cit. on p. 12).

[14] C. Chevignard, P.-A. Fouque and A. Schrottenloher. 'Reducing the Number of Qubits in Quantum Information Set Decoding'. In: *Lecture Notes in Computer Science*. ASIACRYPT 2024 - International Conference on the Theory and Application of Cryptology and Information Security. Kolkata, India: Springer, 2024, pp. 1–36. URL: https://inria.hal.science/hal-04823059 (cit. on p. 14).

[15] T. Espitau, G. Niot and T. Prest. 'Flood and Submerse: Distributed Key Generation and Robust Threshold Signature from Lattices'. In: CRYPTO 2024 - Annual International Cryptology Conference. Vol. 14926. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 18th Aug. 2024, pp. 425–458. DOI: 10.1007/978-3-031-68394-7_14. URL: https://inria.hal.science/hal-04710250 (cit. on p. 15).

[16] H. Hadipour, P. Derbez and M. Eichlseder. 'Revisiting Differential-Linear Attacks via a Boomerang Perspective with Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck, and SERPENT'. In: *LNCS*. CRYPTO 2024 - 44th Annual International Cryptology Conference. Vol. 14923. Lecture Notes in Computer Science. Santa barbara, United States: Springer Nature Switzerland, 17th Aug. 2024, pp. 38–72. DOI: 10.1007/978-3-031-68385-5_2. URL: https://inria.hal.science/hal-04827105 (cit. on p. 12).

[17] J. Jancar, M. Fourné, D. de Almeida Braga, M. Sabt, P. Schwabe, G. Barthe, P.-A. Fouque and Y. Acar. 'They're not that hard to mitigate: What Cryptographic Library Developers Think About Timing Attacks'. In: ASE 2024 - 21st Workshop on Automotive Software Engineering. Linz (AUSTRIA), Austria: Gesellschaft für Informatik e.V., 2024. DOI: 10.18420/sw2024_47. URL: https://hal.science/hal-04832863 (cit. on p. 18).

[18] C. Jeudy, A. Roux-Langlois and O. Sanders. 'Phoenix: Hash-and-Sign with Aborts from Lattice Gadgets'. In: PQCrypto 2024 - 15th International Conference on Post-Quantum Cryptography. Vol. 14771. Lecture Notes in Computer Science. Oxford, United Kingdom: Springer Nature Switzerland, 11th June 2024, pp. 265–299. DOI: 10.1007/978-3-031-62743-9_9. URL: https://hal.science/hal-04689228 (cit. on p. 16).

[19] G. Mureau, A. Pellet-Mary, G. Pliatsok and A. Wallet. 'Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields'. In: *Advances in Cryptology – EUROCRYPT 202443rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26–30, 2024, Proceedings, Part VII*. Eurocrypt 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14657. Lecture Notes in Computer Science. Zurich, Switzerland: Springer Nature Switzerland, 28th Apr. 2024, pp. 226–255. DOI: 10.1007/978-3-031-58754-2_9. URL: https://hal.science/hal-04701342 (cit. on p. 17).

Conferences without proceedings

[20] C. Chevignard, 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, 24th Feb. 2025. URL: https://inria.hal.science/hal-04848612 (cit. on p. 14).

[21] M. Fourné, D. de Almeida Braga, J. Jancar, M. Sabt, P. Schwabe, G. Barthe, P.-A. Fouque and Y. Acar. '"These results must be false": A usability evaluation of constant-time analysis tools'. In: 2024 - 33rd USENIX Security Symposium. Philadelphia, Pennsylvania, USA, United States, 14th Aug. 2024, pp. 1–18. URL: https://inria.hal.science/hal-04712302 (cit. on p. 18).

[22] A. Pouly and Y. Shen. 'Discrete gaussian sampling for BKZ-reduced basis'. In: ArcticCrypt 2025. Longyearbyen, Svalbard, Norway, 6th July 2025. URL: https://inria.hal.science/hal-04823293 (cit. on p. 15).

Doctoral dissertations and habilitation theses

[23] C. Jeudy. 'Design of advanced post-quantum signature schemes'. Université de Rennes, 18th June 2024. URL: https://theses.hal.science/tel-04696615.

Reports & preprints

[24] B. Cho, M. Hhan, T. Kim, J. Lee and Y. Shen. *Does quantum lattice sieving require quantum RAM?* 2024. DOI: 10.48550/arXiv.2410.15565. URL: https://hal.science/hal-04747841 (cit. on p. 13).

[25] J. Gasnier and A. Guillevic. *An Algebraic Point of View on the Generation of Pairing-Friendly Curves*. 16th Dec. 2024. URL: https://hal.science/hal-04205681 (cit. on p. 17).

[26] A. Guillevic and S. Masson. *Embedded Curves and Embedded Families for SNARK-Friendly Curves*. 23rd Oct. 2024. URL: https://inria.hal.science/hal-04750802 (cit. on p. 17).

[27] A. Pouly and Y. Shen. *Smoothing Parameter and Shortest Vector Problem on Random Lattices*. 2024. URL: https://inria.hal.science/hal-04823287 (cit. on p. 15).

[28] J. ROUSSEAU. *Cube-based cryptanalysis of Ascon and Gift*. Université de rennes; Irisa Institut de Recherche en Informatique et Systèmes Aléatoires, Sept. 2024, p. 32. URL: https://hal.science/hal-04692191.

12.3 Cited publications

[29] 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: *STOC*. ACM, 2015, pp. 733–742 (cit. on p. 15).

[30] 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. 8).

[31] 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. 8).

[32] 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. 8).

[33] 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. 8).

[34] 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. 8).

[35] A. Becker, L. Ducas, N. Gama and T. Laarhoven. 'New directions in nearest neighbor searching with applications to lattice sieving'. In: *SODA*. SIAM, 2016, pp. 10–24 (cit. on p. 15).

[36] O. Bernard, A. Lesavourey, T. Nguyen and A. Roux-Langlois. 'Log-S-unit Lattices Using Explicit Stickelberger Generators to Solve Approx Ideal-SVP'. In: *ASIACRYPT (3)*. Vol. 13793. Lecture Notes in Computer Science. Springer, 2022, pp. 677–708 (cit. on p. 16).

[37] 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. 5).

[38] D. J. Bernstein. 'Grover vs. McEliece'. In: *PQCrypto*. Vol. 6061. Lecture Notes in Computer Science. Springer, 2010, pp. 73–80 (cit. on p. 14).

[39] 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. 7).

[40] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin 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. 5).

[41] 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 p. 7).

[42] 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. URL: https://doi.org/10.13154/tosc.v2019.i2.55-93 (cit. on p. 7).

[43] 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. 7).

[44] 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. 4).

[45] 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. 6).

[46] 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. 8).

[47] 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. 9).

[48] Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehlé. 'Classical hardness of learning with errors'. In: *STOC*. ACM, 2013, pp. 575–584 (cit. on p. 4).

[49] 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. 5).

[50] C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet and K. Xagawa. 'ModFalcon: Compact Signatures Based On Module-NTRU Lattices'. In: *AsiaCCS*. ACM, 2020, pp. 853–866 (cit. on p. 5).

[51] 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 (cit. on p. 6).

[52] P. Derbez and P.-A. Fouque. 'Exhausting Demirci-Selçuk 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. 6).

[53] C. Dobraunig, M. Eichlseder, F. Mendel and M. Schläffer. 'Ascon v1.2: Lightweight Authenticated Encryption and Hashing'. In: *J. Cryptol.* 34.3 (2021), p. 33 (cit. on p. 6).

[54] 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. 5).

[55] 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. 8).

[56] 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. URL: https://doi.org/10.46586/tches.v2022.i2.240-265 (cit. on p. 9).

[57] 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. 8).

[58] 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. 5).

[59] H. Gilbert, R. H. Boissier, L. Khati and Y. Rotella. 'Generic Attack on Duplex-Based AEAD Modes Using Random Function Statistics'. In: *EUROCRYPT (4)*. Vol. 14007. Lecture Notes in Computer Science. Springer, 2023, pp. 348–378 (cit. on p. 11).

[60] 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. 8).

[61] 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. 5).

[62] 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. 5).

[63] 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. 5).

[64] 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. 5).

[65] 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. 5).

[66] A. May and L. Schlieper. 'Quantum Period Finding is Compression Robust'. In: *IACR Trans. Symmetric Cryptol.* 2022.1 (2022), pp. 183–211 (cit. on p. 14).

[67] S. Menda, J. Len, P. Grubbs and T. Ristenpart. 'Context Discovery and Commitment Attacks - How to Break CCM, EAX, SIV, and More'. In: *EUROCRYPT (4)*. Vol. 14007. Lecture Notes in Computer Science. Springer, 2023, pp. 379–407 (cit. on p. 11).

[68] 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. 8).

[69] 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. 5).

[70] 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. 9).

[71] 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. 15).

[72] 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. 8).

[73] 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. 4).

[74] P. W. Shor. 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring'. In: *FOCS*. IEEE Computer Society, 1994, pp. 124–134 (cit. on p. 4).

[75] C. L. Siegel. 'A mean value theorem in geometry of numbers'. In: *Annals of Mathematics* 46.2 (1945), pp. 340–347 (cit. on p. 15).