RESEARCH CENTRE

Inria Centre at Rennes University

IN PARTNERSHIP WITH:

Université de Rennes

2023

ACTIVITY REPORT

Project-Team

CAPSULE

Applied Cryptography and Implementation Security

IN COLLABORATION WITH: Institut de recherche en informatique et systèmes aléatoires (IRISA)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Inria

Contents

Project-Team CAPSULE 1

1 Team members, visitors, external collaborators 2

2 Overall objectives 3

3 Research program 3
3.1 Security against post-quantum attackers . . . 3
3.2 Symmetric Cryptography . . . 5
3.3 Security of cryptographic implementation and Real-World Cryptography . . . 7

4 Application domains 8
4.1 Designing, Analyzing and Choosing Cryptographic Standards . . . 8

5 Social and environmental responsibility 9
5.1 Impact of research results . . . 9

6 Highlights of the year 9
6.1 Awards . . . 9

7 New software, platforms, open data 10

8 New results 10
8.1 Symmetric Cryptanalysis . . . 10
8.2 Quantum Algorithms and Cryptanalysis . . . 11
8.3 Public-key cryptography . . . 12
8.4 Side-Channel Attacks . . . 14
8.5 Real-World Cryptography . . . 14

9 Bilateral contracts and grants with industry 15
9.1 Bilateral contracts with industry . . . 15
9.2 Bilateral Grants with Industry . . . 16

10 Partnerships and cooperations 17
10.1 International initiatives . . . 17
10.1.1 Visits to international teams . . . 17
10.2 National initiatives . . . 17

11 Dissemination 19
11.1 Promoting scientific activities . . . 19
11.1.1 Scientific events: organisation . . . 19
11.1.2 Scientific events: selection . . . 19
11.1.3 Journal . . . 19
11.1.4 Invited talks . . . 20
11.1.5 Scientific expertise . . . 20
11.1.6 Research administration . . . 20
11.2 Teaching - Supervision - Juries . . . 20
11.2.1 Teaching . . . 20
11.2.2 Supervision . . . 21
11.2.3 Juries . . . 22
11.2.4 Education . . . 22

12 Scientific production 23
12.1 Major publications . . . 23
12.2 Publications of the year . . . 23
12.3 Cited publications . . . 25

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

- Andre Schrottenloher [INRIA, Researcher]
- Alexandre Wallet [INRIA, Researcher]

Faculty Members

- Pierre-Alain Fouque [Team leader, UNIV RENNES, Professor, HDR]
- Patrick Derbez [UNIV RENNES, Associate Professor, HDR]
- Damien Marion [UNIV RENNES, Associate Professor, from Sep 2023, Previously postdoctorate student in the CAPSULE team]

Post-Doctoral Fellows

- Alexandre Gonzalvez [CNRS]
- Andrea Lesavourey [CNRS, from Mar 2023 until Aug 2023]

PhD Students

- Agathe Cheriere [CNRS, until Nov 2023, DGA grant]
- Clemence Chevignard [UNIV RENNES, from May 2023, PEPR PQ-TLS]
- Mathieu Degre [UNIV RENNES, from May 2023, ANR OREO grant]
- Arthur Gontier [UNIV RENNES, until Nov 2023, DECRYPT grant]
- Aymeric Hiltenbrand [UNIV RENNES, from Oct 2023]
- Corentin Jeudy [ORANGE LABS, CIFRE]
- Thi Thu Quyen Nguyen [IDEMIA, CIFRE, from Oct 2023]
- Phuong Nguyen [UNIV RENNES, Brittany grant, CRYPTAUDIT and DECRYPT grant]
- Lucas Prabel [UNIV RENNES, until Sep 2023]

Interns and Apprentices

- Lucas Giordani [UNIV RENNES, Intern, from May 2023]
- Jerome Guyot [ENS PARIS-SACLAY, Intern, from Jun 2023 until Jul 2023]
- Rayan Lachguel [UNIV RENNES, Intern, from Nov 2023]
- Lucie Lahaye [ENS DE LYON, Intern, from Jun 2023 until Jul 2023]
- Heorhii Pliatsok [UNIV RENNES, Intern, from Apr 2023 until Sep 2023]

Administrative Assistants

- Isobelle Kelly [Inria, from Oct 2023]
- Veronique Martinet [Inria]

External Collaborators

- Julien Devigne [DGA]
- Marie Euler [DGA]
- Benoît Gérard [DGA]
- Tuong-Huy Nguyen [DGA, until Nov 2023]

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 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 [63] 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 is 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 is 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, thank 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 system (“Learning With Errors”, LWE) and computing short vectors in euclidean lattices in the worst case. They both served as the fundation of security to design public-key encryptions, digital signatures, zero-knowledge proof systems, key-encapsulation mechanisms, homomorphic encryptions, ... 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 lat- tices with symmetries. Additionnally, for LWE the noise distributions 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. [35, 61, 32].

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 (sometime 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 seem 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 [29], reducing module lattices as a generalization of the LLL algorithm in the ring of integers of a number field in [55] or in a tower of cyclotomic fields in [52]. We generalized the BKW algorithm to binary LWE setting in [53] and studied the Learning Parities with Noise (LPN) Problem in [56].

We have also attacked concrete cryptographic schemes. We broke some multivariate schemes such as the SFLASH signature schemes in [43] and variants [48], and the ASASA schemes in [58]. We have also broken FHE schemes based on overstretched NTRU parameters in [54] or concrete FHE in [38].

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 number field. It is also interesting to improve the recent work of [27], which suggests that this problem may be weaker than previously thought.

Constructions and practical cryptosystems. Applications of cryptography usually culminates 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 in efficiency.

In this area, members of CAPSULE have worked on the lattice-based signature scheme Falcon and its efficiency-security trade-off ModFalcon [39]. 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 challenge 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 by selecting the lightweight cipher family Ascon [42], 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 so far success, 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.

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

In the past, the members of the team have proposed many tools, for example for improving attacks on round-reduced versions of AES [33], Demirci-Selçuk attacks on AES [41], and impossible differential attacks [40].

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 softwares to particular cryptographic problems.

Finding and optimizing a cryptanalytic attack in its entirety is an especially interesting problem, since it requires to integrate 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 [28], the authenticated ecryption 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 [30].

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 [31]. 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 [9].

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 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 [50] to prove the security of implementations, secure theoretical foundations have been laid by Prouff and Rivain and later Duc et al. in [60, 44]. Soon after, some tools have been developed such as [23, 24, 22] 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 [25], where generally securing randomness presents an interesting challenges. We aim at extending the results of [25, 26, 57, 47] 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 litterature that help developers to avoid these leakage, but insecure implementations are stille aplenty. For instance, we recently broke the WPA-3 implementation used in FreeRadius and iwd (iNet Wireless Daemon) [34], 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 [46], 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 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 [8]. We also study the privacy of the EME standard (Encrypted Media Extensions) for Digital Rights Managments in browsers in [18].

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

Pierre-Alain Fouque was appointed Senior member of the IUF (Institut Universitaire de France) for 5 years starting in September 2023.

6.1 Awards

ACNS 2023 Best Student Paper Award [1] Agathe Cheriere, Nicolas Aragon, Tania Richmond, Benoît Gérard, "BIKE Key-Recovery: Combining Power Consumption Analysis and Information-Set Decoding." ACNS 2023 - 21st International Conference on Applied Cryptography and Network Security, Kyoto, Japan, May 29, 2023

ASIACRYPT 2023 Best Paper Award [2] Thomas Espitau, Alexandre Wallet, Yang Yu, "On Gaussian sampling, smoothing parameter: Application to lattice signatures." ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou (Canton), China, Dec 4, 2023

NIST prize To the Falcon Team, "NIST extends its appreciation to the Falcon Team for outstanding contributions to the NIST PQC Standardization process through the design of FN-DSA", University of Maryland, August, 2023.

7 New software, platforms, open data

The code that we develop is for demonstration or specific for some attacks, or implementation. Consequently, we do not work on any software. We do not use a particular platform. Some of the data we use in some work are made available.

8 New results

8.1 Symmetric Cryptanalysis

Participants: Mathieu Degré, Patrick Derbez, Marie Euler, Arthur Gontier, Lucie Lahaye, Phuong Nguyen, André Schrottenloher.

This year we developed a new cryptanalysis technique related to differential cryptanalysis which allowed us to break more rounds of two well-studied block ciphers: the AES and SKINNY. We also developed a new tool permitting to fully automatize the search of the best differential characteristics on a large class of ciphers. Finally, we solved an algorithmic problem related to AES by providing a dynamic-programming based algorithm able to find the best truncated related-key differential characteristics on all versions of AES.

Differential Meet-in-the-middle Attacks. Meet-in-the-middle and differential attacks are two cornerstones of modern cryptanalysis, which have been applied successfully on block ciphers for decades. In [4], we introduced the new framework of *differential meet-in-the-middle* attacks, which combines technique from both meet-in-the-middle and differential cryptanalysis. As such, this technique can be seen both as an extension of meet-in-the-middle attacks, and as a novel way of performing the key-recovery in differential attacks. We applied this technique to two very well studied ciphers, SKINNY and the international standard AES, and obtained new results on weakened (reduced-round) variants, including a related-key attack on 12 rounds out of 14 on AES-256 with only two related keys.

Related-Key Differential Analysis of the AES. The related-key setting, in which a block cipher may be queried with several unknown keys having some known relation, is a scenario in which AES is known to be quite weak. However, finding related-key characteristics is a difficult process which nowadays can be done only with the help of automatic tools. In [10] we gave new tools dedicated to this task, both *ad hoc* and based on MILP. We also built a new tool to search for differential MITM attacks, which improved the 12-rounds attack above to 13 rounds.

A CP-based Automatic Tool for Instantiating Truncated Differential Characteristics. An important criteria to assert the security of a cryptographic primitive is its resistance against differential cryptanalysis. For word-oriented primitives, a common technique to determine the number of rounds required to ensure the immunity against differential distinguishers is to consider truncated differential characteristics and to count the number of active S-boxes. Doing so allows one to provide an upper bound on the probability of the best differential characteristic with a reduced computational cost. However, in order to design very efficient primitives, it might be needed to evaluate the probability more accurately. This is usually done in a second step, during which one tries to instantiate truncated differential characteristics with actual values and computes its corresponding probability. This step is usually done either with ad-hoc algorithms or with CP, SAT or MILP models that are solved by generic solvers. In [12], we present a generic

tool for automatically generating these models to handle all word-oriented ciphers. Furthermore the running times to solve these models are very competitive with all the previous dedicated approaches.

Equivalence of Generalised Feistel Networks. We also focused on equivalences between Generalised Feistel Networks (GFN) of type-II. We introduced a new definition of equivalence which captures the concept that two GFNs are identical up to re-labelling of the inputs/outputs and are therefore cryptographically equivalent for several classes of attacks. It induces a reduction of the space of possible GFNs: the set of the $(k!)^2$ possible even-odd GFNs with $2k$ branches can be partitioned into $k!$ different classes. From a designer perspective, it means that a much wider spectrum of candidates can be explored to choose a good permutation. In particular, using this new equivalence relation led us to five 62-branch permutations performing better than WARP regarding the number of differentially/linearly active S-Boxes and to a new family of permutations with good diffusion properties. This work is under submission.

Cryptanalysis of ASCON. During the internships of Mathieu Degré and Lucie Lahaye, we started studying the cryptanalysis of the ASCON family of lightweight primitives, which is a high-profile target as it has been recently selected for standardization by the NIST. Our goal in this project was to obtain simpler modelings of different types of cryptanalysis, based on MILP and SAT encodings, which were easier not only to describe but also to run. Our results are under submission.

8.2 Quantum Algorithms and Cryptanalysis

Participants: André Schrottenloher.

During this year, we have introduced several advanced quantum algorithms with applications in cryptanalysis (symmetric and asymmetric), as well as new frameworks for symmetric cryptanalysis which we plan to build upon in the next few years.

Applications in Asymmetric Cryptanalysis. In [9] we introduced the new algorithmic technique of **chained quantum walks**. This technique is key to an improvement on quantum algorithms for the *multiple collision search* problem, an extension of the *collision search* problem, which asks to find pairs of colliding outputs generated by a random function. It allowed us to improve the previous best quantum algorithm for lattice sieving [37], reducing its asymptotic time complexity from $2^{0.2570d+o(d)}$ to $2^{0.2563d+o(d)}$ where d is the lattice dimension. These algorithms are of high interest since they underlie the security analyses of lattice-based cryptography at large.

In [19], we gave new quantum trade-offs for the **Dihedral Coset Problem**, which is a computational problem of high interest. In particular, its hardness underlies the security of post-quantum cryptosystems based on Abelian group actions such as CSIDH [36]. These cryptosystems are the only high-profile post-quantum proposals for which a quantum attacker enjoys a large speedup (from exponential classical time to subexponential quantum time). Thus their security analysis relies primarily on the quantum side.

Applications in Symmetric Cryptanalysis. In [20] we introduced a new framework of **quantum linear key-recovery attacks** on block ciphers. In classical cryptanalysis, *linear cryptanalysis* is a powerful key-recovery attack exploiting the linear biases which may appear in reduced-round ciphers. While modern linear key-recovery attacks rely on the Fast Fourier Transform, a potential application of the Quantum Fourier Transform remained an open question in previous works [51]. In this work, we showed that this was possible, and could lead to new quantum attacks on block ciphers. The new framework relies on computing correlations of Boolean functions "analogically" in the amplitudes of quantum states, which generates technical difficulties and new open questions that need further investigation. Despite the

current limitations, this framework may reach up to a super-quadratic speedup in key-recovery attacks, which coïncides with the current best speedup reported in [31] for specific constructions of block ciphers.

In [6] we described a generic framework of **quantum impossible differential attacks** on block ciphers, with a generic formula from their time complexity and a procedure to easily translate classical attacks into quantum ones.

In [7] we introduced an automatic search and optimization tool for **quantum meet-in-the-middle key-recovery attacks** on block ciphers. This tool expands a previous modeling technique which we introduced in the past year [62].

8.3 Public-key cryptography

Participant: Alexandre Wallet, Pierre-Alain Fouque, Corentin Jeudy, Lucas Prabel.

This year we proposed new designs and trade-offs for the core building blocks of hash-then-sign lattice-based signatures. This is in direct continuation with the results obtained last year, and initiated a participation to a national standardization competition (namely, South Korea's KPQC) as a direct application of our new results. We also submitted two Multivariate Cryptography signature schemes, PROV and VOX, to the recent call in June 2023. Finally, we obtained new results in the construction of advanced cryptographic protocols.

Optimal trapdoors for practical lattice-based hash-then-sign Last year we described in [45] MITAKA, a variant of Falcon with much simpler implementation, larger parameter space, better parallelism and easier to protect from side-channel adversaries. One of the drawback of our scheme was its slightly lower security level. Indeed, finding good trapdoors in the key-generation process for Mitaka remained a costly task, and we had to sacrifice security for concrete efficiency. In [13] we propose a completely novel approach to find good trapdoors in an essentially optimal way, with much freedom in the quality that we impose on them. Our method stems from the geometric identification of the space where one can find them, and the design of a simple, natural sampler to draw from. It combines Fast Fourier Transform techniques with fine-grained error rounding analysis into a key-generation algorithm called ANTRAG, achieving the same efficiency as Falcon's, *without* sacrificing any bit-security.

Concretely, this technique make MITAKA as secure as Falcon. This prompted its use into a candidate for standardization in a national process (as mentioned above), called SOLMAE (Falcon in Korean), and submitted for the first round of evaluation. Despite SOLMAE having the minimal bandwith consumption of all candidates and concrete signing speed on par with the other lattice contender HAETAE (DILITHIUM's natural update), it was not selected to advance to the second round[2].

Unifying Lattice Gaussian sampling. Lattice Gaussian sampling is nowaday a pervasive technique in all aspects of the field: reductions between problems (in the complexity theory sense), as a concrete building block for primitives, in security arguments,... Many methods to sample lattice Gaussians existed in the toolbox of the cryptographers, but perhaps surprisingly, most of them felt unrelated one to another. This made it rather difficult to understand where improvement vectors could be found. In [14] we proposed a generic, abstract framework allowing to recover almost if not all known approaches, while opening-up the design space for further explorations. Among samplers we recover naturally are the important approach of as [49, 59]. We provided novel samplers following this new avenues, illustrating how to use our framework. Some of our new designs demonstrated important security improvements in concrete schemes (such as MITAKA), while also displaying more simplicity in their description. On a more foundational aspect, we gave a new *exact* expansion of the so-called smoothing parameter of a lattice.

[2] This is to our surprise, since Falcon and Dilithium, the pioneers in these designs, both advanced to be ultimately selected by the NIST.

This important quantity is used in many security arguments, where the finer the estimate, the better control over security one gets. We believe that this new expression has application in more mathematical aspects of lattice theory, such as improved transference bounds.

Reductions between variants of the Module-LWE problem. The Module Learning With Errors problem (M-LWE) is a core computational assumption of lattice-based cryptography which offers an interesting trade-off between guaranteed security and concrete efficiency. The problem is parameterized by a secret distribution as well as an error distribution. There is a gap between the choices of those distributions for theoretical hardness results (standard formulation of M-LWE, i.e., uniform secret modulo q and Gaussian error) and practical schemes (small bounded secret and error). In [3], we make progress towards narrowing this gap. More precisely, we prove that M-LWE with uniform η-bounded secret for any $1 \leq \eta \ll q$ and Gaussian error, in both its search and decision variants, is at least as hard as the standard formulation of M-LWE, provided that the module rank d is at least logarithmic in the ring degree n. We also prove that the search version of M-LWE with large uniform secret and uniform η-bounded error is at least as hard as the standard M-LWE problem, if the number of samples m is close to the module rank d and with further restrictions on η. The latter result can be extended to provide the hardness of M-LWE with uniform η-bounded secret and error under specific parameter conditions. Overall, the results apply to all cyclotomic fields, but most of the intermediate results are proven in more general number fields.

Lattice Signature with Efficient Protocols, Application to Anonymous Credentials. Digital signature is an essential primitive in cryptography, which can be used as the digital analogue of handwritten signatures but also as a building block for more complex systems. In the latter case, signatures with specific features are needed, so as to smoothly interact with the other components of the systems, such as zero-knowledge proofs. This has given rise to so-called signatures with efficient protocols, a versatile tool that has been used in countless applications. Designing such signatures is however quite difficult, in particular if one wishes to withstand quantum computing. We are indeed aware of only one post-quantum construction, proposed by Libert et al. at Asiacrypt'16, yielding very large signatures and proofs.

In [17], we propose a new construction that can be instantiated both in standard lattices and structured ones, resulting in each case in dramatic performance improvements. In particular, the size of a proof of message-signature possession, which is one of the main metrics for such schemes, can be brought down to less than 650 KB. As our construction retains all the features expected from signatures with efficient protocols, it can be used as a drop-in replacement in all systems using them, which mechanically improves their own performance, and has thus a direct impact on many applications. It can also be used to easily design new privacy-preserving mechanisms. As an example, we provide the first lattice-based anonymous credentials system.

Identity-Based Encryption from Lattices Using Approximate Trapdoors. Practical implementations of advanced lattice-based constructions have received much attention since the first practical identity-based encryption scheme instantiated over NTRU-lattices, proposed by Prest et al. (Asiacrypt 2014). This particular design uses powerful lattice-based building blocks to allow efficient Gaussian preimage sampling and trapdoor generation. In [16], we propose two different constructions and implementations of identity-based encryption schemes (IBE) using Chen et al. (Asiacrypt 2019)approximate variants of "gadget-based" trapdoors. Both constructions are proven secure.

Our first IBE scheme is an adaptation of the Bert et al. scheme (PQCrypto 2021) to the approximate setting, relying on the Module-NTRU hardness assumption and making use of the Micciancio-Peikert paradigm for approximate trapdoors. The second IBE relies on a variant of the NTRU hardness assumption.

We provide several timings and a comparison analysis to explain our results. The two different instantiations give interesting trade-offs in terms of security and efficiency and both benefit from the use of approximate trapdoors. Though our second IBE construction is less efficient than other NTRU-based

IBEs, we believe our work provides useful insights into efficient advanced lattice-based constructions.

New Security Proof in the QROM model. In [15], we present a new generic transform that takes a multi-round interactive proof for the membership of a language L and outputs a non-interactive zero-knowledge proof (not of knowledge) in the common reference string model. Similar to the Fiat-Shamir transform, it requires a hash function H. However, in our transform the zero-knowledge property is in the standard model, and the adaptive soundness is in the non-programmable random oracle model (NPROM). Behind this new generic transform, we build a new generic OR-composition of two multi-round interactive proofs. Note that the two common techniques for building OR-proofs (parallel OR-proof and sequential OR-proof) cannot be naturally extended to the multi-round setting. We also give a proof of security for our OR-proof in the quantum oracle model (QROM), surprisingly the security loss in QROM is independent from the number of rounds.

Factorization Algorithms. In [21], we study new factorization algorithms. The Number Field Sieve (NFS) is the state-of-the art algorithm for integer factoring, and sieving is its most crucial step. It is a very time-consuming operation, aiming at collecting many relations. The ultimate goal is to generate random smooth integers mod N together with their prime decomposition, where smooth is defined on the rational and algebraic sides according to two prime factor bases.

In modern factorization tools, such as Cado-NFS, sieving is split into different stages depending on the size of the primes, but defining good parameters for all stages is based on heuristic and practical arguments. At the beginning, candidates are sieved by small primes on both sides, and if they pass the test, they continue to the next stages with bigger primes, up to the final one where the remaining part is factored using the ECM algorithm. On the one hand, first stages are fast but many false relations pass them, and we spend a lot of time with useless relations. On the other hand final stages are more time demanding but outputs less relations. It is not easy to evaluate the performance of the best strategy on the overall sieving step since it depends on the distribution of numbers that results at each stage.

In [21], we examine different sieving strategies to speed-up this step, since many improvements have been done on all other steps of the NFS. Based on the relations collected during the record RSA-250 factorization and all its parameters, we study the many different strategies that have been defined for NFS. Our result is an experimental evaluation of them.

8.4 Side-Channel Attacks

Participant: Pierre-Alain Fouque, Agathe Cheriere, Damien Marion.

BIKE Key-Recovery: Combining Power Consumption Analysis and Information-Set Decoding. In [11] , we present a single-trace attack on a BIKE Cortex-M4 implementation proposed by Chen et al. at CHES 2021. BIKE is a key-encapsulation mechanism, candidate to the NIST post-quantum cryptography standardisation process. We attack by exploiting the rotation function that circularly shifts an array depending on the private key. Chen et al. implemented two versions of this function, one in C and one in assembly. Our attack uses subtraces clustering combined with a combinatorial attack to recover the full private key. We obtained a high clustering accuracy in our experiments, and we provide ways to deal with the errors. We are able to recover all the private keys for the C implementation, and while the assembly version is harder to attack using our technique, we still manage to reduce BIKE Level-1 security from 128 to 65 bits for a significant proportion of the private keys.

8.5 Real-World Cryptography

Participant: Pierre-Alain Fouque.

From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake. In [8] we develop a new software attack on the WPA3. It is universally acknowledged that Wi-Fi communications are important to secure. Thus, the Wi-Fi Alliance published WPA3 in 2018 with a distinctive security feature: it leverages a Password-Authenticated Key Exchange (PAKE) protocol to protect users' passwords from offline dictionary attacks. Unfortunately, soon after its release, several attacks were reported against its implementations, in response to which the protocol was updated in a best-effort manner. In this paper, we show that the proposed mitigations are not enough, especially for a complex protocol to implement even for savvy developers. Indeed, we present Dragondoom, a collection of side-channel vulnerabilities of varying strength allowing attackers to recover users' passwords in widely deployed Wi-Fi daemons, such as hostap in its default settings. Our findings target both password conversion methods, namely the default probabilistic hunting-and-pecking and its newly standardized deterministic alternative based on SSWU. We successfully exploit our leakage in practice through microarchitectural mechanisms, and overcome the limited spatial resolution of Flush+Reload. Our attacks outperform previous works in terms of required measurements. Then, driven by the need to end the spiral of patch-and hack in Dragonfly implementations, we propose Dragonstar, an implementation of Dragonfly leveraging a formally verified implementation of the underlying mathematical operations, thereby removing all the related leakage vector. Our implementation relies on HACL*, a formally verified crypto library guaranteeing secret-independence. We design Dragonstar, so that its integration within hostap requires minimal modifications to the existing project. Our experiments show that the performance of HACL*-based hostap is comparable to OpenSSL-based, implying that Dragonstar is both efficient and proved to be leakage-free.

Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME. In [18], we study the security of Digital Rights Management Systems. Thanks to HTML5, users can now view videos on Web browsers without installing plug-ins or relying on specific devices. In 2017, W3C published Encrypted Media Extensions (EME) as the first official Web standard for Digital Rights Management (DRM), with the overarching goal of allowing seamless integration of DRM systems on browsers. EME has prompted numerous voices of dissent with respect to the inadequate protection of users. Of particular interest, privacy concerns were articulated, especially that DRM systems inherently require uniquely identifying information on users' devices to control content distribution better. Despite this anecdotal evidence, we lack a comprehensive overview of how browsers have supported EME in practice and what privacy implications are caused by their implementations. In this paper, we fill this gap by investigating privacy leakage caused by EME relying on proprietary and closed-source DRM systems. We focus on Google Widevine because of its versatility and wide adoption. We conduct empirical experiments to show that browsers diverge when complying EME privacy guidelines, which might undermine users' privacy. For instance, we find that many browsers gladly give away the identifying Widevine Client ID with no or little explicit consent from users. Moreover, we characterize the privacy risks of users tracking when browsers miss applying EME guidelines regarding privacy. Because of being closed-source, our work involves reverse engineering to dissect the contents of EME messages as instantiated by Widevine. Finally, we implement EME Track, a tool that automatically exploits bad Widevine-based implementations to break privacy.

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

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

- **KDDI**: (T0: 11/2022 –> 02/2023)
  Lead by University of Rennes.
  KDDI (Japan) would like to propose the Rocca-S encryption scheme to some international standardization process. However, such organization require an external evaluation provided by an independent third parties. KDDI contacted us to perform this analysis. Some outputs of this work are currently under review.

9.2 Bilateral Grants with Industry

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

- **Supervision of Quentin Edme's PhD** (T0: 12/2023 -> 12/2026) Funding provided by Orange Labs Caen for the supervision of the CIFRE PhD thesis

- **Supervision of Roderick Asselineau's PhD** (T0: 12/2023 -> 12/2026) Funding provided by Airbus Security for the supervision of the PhD thesis

- **Resque**: (T0: 09/2022 –> 08/2026)
  BPi France project.
  Lead by Thales.
  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 to construct 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 update of the post-quantum algorithms.

- **Hyperform**: (T0: 09/2022 –> 08/2026)
  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: an 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 performances on par with the demands of real-world situations.

10 Partnerships and cooperations

10.1 International initiatives

10.1.1 Visits to international teams

Research stays abroad

Patrick Derbez

Visited institution: University of Chinese Academy of Sciences

Country: China

Dates: 11/25 - 11/30

Context of the visit: Invited by Prof. Siwei Sun to intiate collaboration and give a talk.

Mobility program/type of mobility: research stay

Phuong Hoa Nguyen

Visited institution: University of Graz

Country: Austria

Dates: 09/01 - 12/31

Context of the visit: Collaboration with Maria Eichlseder to initiate collaboration on automatic tools.

Mobility program/type of mobility: research stay

10.2 National initiatives

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

- **The PQTLS** (01/2022 –> 12/27)
  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)
  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 signatures 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 usecases 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).
  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.

Participants: Damien Marion.

- **ANR IDROMEL** (2021 –> 2025)
  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:
  - Leakage sources characterization: a methodology to evaluate leakage sources from detailed description of the micro-architecture (grey-box approach) or from public information (black-box approach), with reproducible characterization based on public test vectors;
  - Security assessment methods: formal code verification, leakage simulators and vulnerability analysis;
  - Automated security tools: a compiler for the application of software countermeasures;
  - Hardware hardening techniques: configurable design technique for the application of hardware countermeasures.

11 Dissemination

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

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

The PQTLS, project of the PEPR Quantique, has organized a workshop at the École normale supérieure on the security of recently submitted post-quantum signature in June 2023, and another workshop with the French companies that are developing a quantum computer in June 2023 at the Cyber Campus in Paris.

Member of the organizing committees

- Séminaire CRYPTO (IRMAR, IRISA, Rennes): Alexandre Wallet, André Schrottenloher.

11.1.2 Scientific events: selection

Chair of conference program committees

- EUROCRYPT 2024 (May 26-30, 2024, Zurich, Switzerland): Pierre-Alain Fouque (Area Chair)

Member of the conference program committees

- ACNS 2023 (June 19-22, 2023, Kyoto, Japan): Alexandre Wallet;
- CRYPTO 2023 (August 19-24, 2023, Santa Barbara, USA): Pierre-Alain Fouque, André Schrottenloher;
- CFAIL 2023 (August 19, 2023, Santa Barbara, USA): Alexandre Wallet;
- Journées Nationales de Codages et Cryptographie (JC2), October 15-20, 2023, Najac, France): Alexandre Wallet
- ASIACRYPT 2023 (December 4-8, 2023, Guangzhou, China): Patrick Derbez, Alexandre Wallet
- INDOCRYPT 2023 (December 10-13 , 2023, Goa, India): Alexandre Wallet
- EUROCRYPT 2024 (May 26-30, 2024, Zurich, Switzerland): Patrick Derbez, Pierre-Alain Fouque (Area Chair), André Schrottenloher;
- AAC 2024 (March 5-8, 2024, Abu Dhabi, UAE): Alexandre Wallet;

External Reviewer

- EUROCRYPT 2023: Alexandre Wallet;
- EUROCRYPT 2024: Alexandre Wallet;

11.1.3 Journal

Member of the editorial boards

- *IACR Transactions on Symmetric Cryptology*, associate editors: Patrick Derbez, André Schrottenloher

Reviewer - reviewing activities

- *Journal of Cryptology*: Alexandre Wallet;
- *Design, Codes, Cryptography*: André Schrottenloher, Alexandre Wallet;
- *Finite fields and applications*: Alexandre Wallet;

11.1.4 Invited talks

- Alexandre Wallet was invited at PQ Shield (Paris, France) to present his work accepted at Asiacrypt 2023: *On Gaussian sampling, smoothing parameter, applications to signatures* — October 2023.

11.1.5 Scientific expertise

We evaluated research projects for many research funding agencies.

11.1.6 Research administration

Pierre-Alain Fouque is the scientific coordinator of the PEPR project PQTLS.

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

- Master: Alexandre Wallet, Euclidean Lattices in Cryptography (REC), 12 hours, M2, University of Rennes, France;
- Master: Alexandre Wallet, Cryptanalysis (CRA), 8h, M2, University of Rennes and ISTIC, France;
- 1st year of engineer cycle: Alexandre Wallet, Introduction to Programming with Java (INF361), 40h, École polytechnique, France;
- 3rd year of engineer cycle: Alexandre Wallet, Cybersecurity (INF565), 12h, École polytechnique, France;
- André Schrottenloher was Oral examiner for fundamental computer science in the entrance examinations of the ENS (Écoles Normales Supérieures).
- Master: Pierre-Alain Fouque, Advanced Course in Cryptography for security (BCS), 16 hours, M2, University of Rennes, France;
- Master: Damien Marion, Advanced Course in Cryptography for security (BCS), 16 hours, M2, University of Rennes, France;
- Master: Pierre-Alain Fouque, Basic Course in Cryptographhy (BC), 16 hours, M1, University of Rennes, France;
- Master: Damien Marion, Basic Course in Cryptographhy (BC), 12 hours, M1, University of Rennes, France;
- Master: Pierre-Alain Fouque, Design and Analysis of Algorithm (ADA), 16 hours, M1, University of Rennes, France;
- Master: Damien Marion, Design and Analysis of Algorithm (ADA), 12 hours, M1, University of Rennes, France;
- Master: Alexandre Gonzalvez, Cryptography in Java, 30 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: Damien Marion, Security of Data (SDATA), 32 hours, M1, University of Rennes.
- Master: Damien Marion, Low-level Programming (LLP), 20 hours, M1, University of Rennes.
- Master: Damien Marion, network security, 20 hours, M1, University of Rennes.
- Master: Damien Marion, Secured Implementation for Cryptography (SIMP), 25 hours, M2, University of Rennes.
- Master: Damien Marion, research project, 24 hours, M1, University of Rennes.
- Bachelor: Damien Marion, Enjeux sociétaux et empreinte écologique du numérique (3EN), 12 hours, L3, University of Rennes, France;
- Bachelor: Damien Marion, Algorithmique et complexité (ACO), 16 hours, L2, University of Rennes, France;

11.2.2 Supervision

- PhD: Agathe Cheriere, *Side-Channel Resistance of Cryptographic Primitives Based on Error-Correcting Codes*, defense in December 2023. Supervisors: Benoît Gérard and Pierre Loidreau.
- PhD: Lucas Prable, *Trappes en Cryptographie Basée sur les Réseaux Euclidiens : Applications et Implémentation*, defense in October 2023. Supervisors: Adeline Roux-Langlois and Pierre-Alain Fouque.
- PhD: Arthur Gontier, *Utilisation de solveurs génériques pour la cryptanalyse de chiffrements symétriques*, defense in November 2023. Supervisors:
- PhD in progress: Phuong Hoa Nguyen, *MILP and symmetric-key cryptanalysis*, started October 2021. Supervisors: Patrick Derbez and Pierre-Alain Fouque.
- PhD in progress: Corentin Jeudy, *Advanced Post-Quantum Protocol*, started October 2021. Supervisors: Pierre-Alain Fouque and Adeline Roux-Langlois.
- PhD in progress: Thi Thu Quyen Nguyen, *Déploiements des signatures fondées sur les réseaux Euclidiens*, started November 2021. Supervisors: Adeline Roux-Langlois (GREYC, Caen), Paul Dischamp (Idemia) and Alexandre Wallet.
- PhD in progress: Léo Ackermann, *Constructions cryptographiques fondées sur les réseaux Euclidiens: nouvelles hypothèses*, started Septembre 2022. Supervisors: Adeline Roux-Langlois (GREYC, Caen) and Alexandre Wallet.
- 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*, starting January 2024. Supervisors: Patrick Derbez, André Schrottenloher.
- PhD in progress: Quentin Edme, *Preuves et attaques quantiques contre les primitives et protocoles cryptographiques*, starting January 2024. Supervisors: Loïc Ferreira (Orange Labs, Caen), Pierre-Alain Fouque, André Schrottenloher.
- PhD in progress: Aymeric Hiltenbrand, *Attaques par canaux auxiliaires sur la cryptographie post-quantique*, starting December 2023. Supervisors: Guenael Renault (ANSSI), Pierre-Alain Fouque.
- PhD in progress: Roderick Asselineau, *Symmetric System in Real-World Cryptography*, starting December 2023. Supervisors: Patrick Derbez.
- Internship: Clémence Chevignard, *Cryptanalyse du schéma Hawk*, March-September 2023. Supervisors: Pierre-Alain Fouque and Alexandre Wallet.

- Internship: Heorhii Pliatsok (M2), *Hermitian Decompositions in Cyclotomic Fields*, April-October 2023. Supervisor: Alexandre Wallet.
- Internship: Mathieu Degré (M2), *A new approach to MILP modeling to reduce the differential gap of ASCON*, April-October 2023. Supervisor: Patrick Derbez.
- Internship: Jérome Guyot (L3), *Algorithmes pour le problème des rotations du réseau cubique*, June-August 2023. Supervisors: Pierre-Alain Fouque and Alexandre Wallet.
- Internship: Lucie Layahe (L3), *Attaques algébriques sur des fonctions de hachage*, June-July 2023. Supervisor: André Schrottenloher.
- Internship: Rayan Lachguel (M1), *Implémentation du schéma de signature post-quantique Falcon*, November 2023-March 2024. Supervisor: Pierre-Alain Fouque.

11.2.3 Juries

- Chloé Gravouil, June 27th, 2023, Pierre-Alain Fouque (Examiner)
- Julien Devevey, September 18th, 2023, Pierre-Alain Fouque (President of the jury)
- Christophe Genevey-Metat, September 28th, 2023, Pierre-Alain Fouque (Examiner)
- Lucas Prabel, October 5th, 2023, Pierre-Alain Fouque (Supervisor)
- Michael Reichle, October 9th, 2023, Pierre-Alain Fouque (Examiner)
- Nicolas David, November 8th, 2023, Patrick Derbez (Examiner)
- Clémence Bouvier, November 27th, 2023, Pierre-Alain Fouque (President of the jury)
- Léonard Assouline, December 1st, 2023, Pierre-Alain Fouque (Examiner)
- Pierre Briaud, December 11th, 2023, Pierre-Alain Fouque (President of the jury)
- Gwendal Patat, December 15th, 2023, Pierre-Alain Fouque (Supervisor)
- Johanna Loyer, December 18th, 2023, André Schrottenloher (Examiner)
- Agathe Cheriere, December 19th, 2023, Pierre-Alain Fouque (Supervisor)
- Samuel Tap, December 19th, 2023, Pierre-Alain Fouque (Examiner)
- Pierre Galissant, December 21th, 2023, Pierre-Alain Fouque (Examiner)

11.2.4 Education

- Alexandre Wallet, *Petit panorama de la cryptographie post-quantique*, École polytechnique, March 6, 2023. General talk on the upcoming standardization of post-quantum cryptography for students in cybersecurity.
- Pierre-Alain Fouque and André Schrottenloher participated at the first Spring School of the Cyber-School at University of Rennes.

12 Scientific production

12.1 Major publications

[1] ***Best Paper***
A. Cheriere, N. Aragon, T. Richmond and B. Gérard. 'BIKE Key-Recovery: Combining Power Consumption Analysis and Information-Set Decoding'. In: *Lecture Notes in Computer Science*. ACNS 2023 - 21st International Conference on Applied Cryptography and Network Security. Vol. 13905. Lecture Notes in Computer Science. Kyoto, Japan: Springer Nature Switzerland, 29th May 2023, pp. 725–748. DOI: 10.1007/978-3-031-33488-7_27. URL: https://hal.science/hal-04166679.

[2] ***Best Paper***
T. Espitau, A. Wallet and Y. Yu. 'On Gaussian sampling, smoothing parameter: Application to lattice signatures'. In: *Lecture notes in Computer Science*. ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security. Guangzhou (Canton), China, 4th Dec. 2023, pp. 1–56. URL: https://inria.hal.science/hal-04258598.

12.2 Publications of the year

International journals

[3] K. Boudgoust, C. Jeudy, A. Roux-Langlois and W. Wen. 'On the Hardness of Module Learning with Errors with Short Distributions'. In: *Journal of Cryptology* 36.1 (Jan. 2023), pp. 1–72. DOI: 10.1007/s00145-022-09441-3. URL: https://hal.science/hal-04028217.

[4] C. Boura, P. Derbez and M. Funk. 'Related-Key Differential Analysis of the AES'. In: *IACR Transactions on Symmetric Cryptology* 2023.4 (8th Dec. 2023), pp. 215–243. DOI: 10.46586/tosc.v2023.i4.215-243. URL: https://hal.science/hal-04346377.

[5] A. Cheriere, L. Mortajine, T. Richmond and N. El Mrabet. 'Exploiting ROLLO's constant-time implementations with a single-trace analysis'. In: *Designs, Codes and Cryptography* Special Issue: Coding and Cryptography 2022 (29th Apr. 2023). DOI: 10.1007/s10623-023-01227-3. URL: https://hal.science/hal-04166638.

[6] N. David, M. Naya-Plasencia and A. Schrottenloher. 'Quantum Impossible Differential Attacks: Applications to AES and SKINNY'. In: *Designs, Codes and Cryptography* (2023), pp. 1–33. DOI: 10.1007/s10623-023-01280-y. URL: https://inria.hal.science/hal-04321756.

[7] A. Schrottenloher and M. Stevens. 'Simplified Modeling of MITM Attacks for Block Ciphers: New (Quantum) Attacks'. In: *IACR Transactions on Symmetric Cryptology* 2023.3 (19th Sept. 2023), pp. 146–183. DOI: 10.46586/tosc.v2023.i3.146-183. URL: https://inria.hal.science/hal-04261017.

International peer-reviewed conferences

[8] D. de Almeida Braga, N. Kulatova, M. Sabt, P.-A. Fouque and K. Bhargavan. 'From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake'. In: EuroS&P 2023 - IEEE 8th European Symposium on Security and Privacy. Delft, Netherlands: IEEE, 3rd July 2023, pp. 707–723. DOI: 10.1109/EuroSP57164.2023.00048. URL: https://hal.science/hal-04175322.

[9] X. Bonnetain, A. Chailloux, A. Schrottenloher and Y. Shen. 'Finding many Collisions via Reusable Quantum Walks: Application to Lattice Sieving'. In: *Lecture Notes in Computer Science*. EUROCRYPT 2023 - International Conference on the Theory and Applications of Cryptographic Techniques. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer Nature Switzerland, 16th Apr. 2023, pp. 221–251. DOI: 10.1007/978-3-031-30589-4_8. URL: https://inria.hal.science/hal-04261002.

[10] C. Boura, N. David, P. Derbez, G. Leander and M. Naya-Plasencia. 'Differential Meet-In-The-Middle Cryptanalysis'. In: *LNCS - Lecture Notes in Computer Science*. CRYPTO 2023 - 43rd International Cryptology Conference. Vol. 14083. Lecture Notes in Computer Science. Santa Barabara, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 240–272. DOI: 10.1007/978-3-031-38548-3_9. URL: https://inria.hal.science/hal-04276899.

[11] ***Best Paper***
A. Cheriere, N. Aragon, T. Richmond and B. Gérard. 'BIKE Key-Recovery: Combining Power Consumption Analysis and Information-Set Decoding'. In: *Lecture Notes in Computer Science*. ACNS 2023 - 21st International Conference on Applied Cryptography and Network Security. Vol. 13905. Lecture Notes in Computer Science. Kyoto, Japan: Springer Nature Switzerland, 29th May 2023, pp. 725–748. DOI: 10.1007/978-3-031-33488-7_27. URL: https://hal.science/hal-04166679.

[12] F. Delobel, P. Derbez, A. Gontier, L. Rouquette and C. Solnon. 'A CP-based Automatic Tool for Instantiating Truncated Differential Characteristics ⋆'. In: *LNCS*. INDOCRYPT 2023 - 24th International Conference on Cryptology in India. Goa, India: Springer, Dec. 2023, pp. 1–23. URL: https://hal.science/hal-04343593.

[13] T. Espitau, Q. T. T. Nguyen, C. Sun, M. Tibouchi and A. Wallet. 'Antrag: Annular Ntru Trapdoor Generation: Making Mitaka As Secure As Falcon'. In: *Lecture notes in Computer Science*. ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security. Guangzhou (Canton), China: Springer, 2023, pp. 1–56. URL: https://inria.hal.science/hal-04258578.

[14] ***Best Paper***
T. Espitau, A. Wallet and Y. Yu. 'On Gaussian sampling, smoothing parameter: Application to lattice signatures'. In: *Lecture notes in Computer Science*. ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security. Guangzhou (Canton), China, 4th Dec. 2023, pp. 1–56. URL: https://inria.hal.science/hal-04258598.

[15] P.-A. Fouque, A. Georgescu, C. Qian, A. Roux-Langlois and W. Wen. 'A Generic Transform from Multi-Round Interactive Proof to NIZK'. In: *Lecture Notes in Computer Science*. PKC 2023 - International Conference on Practice and Theory of Public-Key Cryptography. Vol. 13941. Lecture Notes in Computer Science. Atlanta, United States: Springer Nature Switzerland, 2nd May 2023, pp. 461–481. DOI: 10.1007/978-3-031-31371-4_16. URL: https://hal.science/hal-04163128.

[16] M. Izabachène, L. Prabel and A. Roux-Langlois. 'Identity-Based Encryption from Lattices Using Approximate Trapdoors'. In: ACISP 2023 - 28th Australasian Conference on Information Security and Privacy. Vol. 13915. Lecture Notes in Computer Science. Brisbane, Australia: Springer Nature Switzerland, 15th June 2023, pp. 270–290. DOI: 10.1007/978-3-031-35486-1_13. URL: https://hal.science/hal-04163136.

[17] C. Jeudy, A. Roux-Langlois and O. Sanders. 'Lattice Signature with Efficient Protocols, Application to Anonymous Credentials'. In: Crypto 2023 - 43rd Annual International Cryptology Conference. Vol. 14082. Lecture Notes in Computer Science. Santa Barbara, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 351–383. DOI: 10.1007/978-3-031-38545-2_12. URL: https://hal.science/hal-04242499.

[18] G. Patat, M. Sabt and P.-A. Fouque. 'Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME'. In: PETS 2023 - Privacy Enhancing Technologies Symposium. Vol. 2023. 4. Lausanne, Switzerland, Oct. 2023, pp. 306–321. DOI: 10.56553/popets-2023-0112. URL: https://hal.science/hal-04179324.

[19] M. Remaud, A. Schrottenloher and J.-P. Tillich. 'Time and Query Complexity Tradeoffs for the Dihedral Coset Problem'. In: *LNCS - Lecture Notes in Computer Science*. PQCrypto 2023 - 14th International Conference on Post-Quantum Cryptography. Vol. 14154. Lecture Notes in Computer Science. College Park, United States: Springer Nature Switzerland, 10th Aug. 2023, pp. 505–532. DOI: 10.1007/978-3-031-40003-2_19. URL: https://inria.hal.science/hal-04276584.

[20] A. Schrottenloher. 'Quantum Linear Key-Recovery Attacks Using the QFT'. In: *Lecture Notes in Computer Science*. CRYPTO 2023 - 43rd International Cryptology Conference. Vol. 14085. Lecture Notes in Computer Science. Santa Barbara, CA, United States: Springer Nature Switzerland, 9th Aug. 2023, pp. 258–291. DOI: 10.1007/978-3-031-38554-4_9. URL: https://inria.hal.science/hal-04260886.

Reports & preprints

[21] C. Bouillaguet, A. Fleury, P.-A. Fouque and P. Kirchner. *We Are on the Same Side. Alternative Sieving Strategies for the Number Field Sieve*. 31st May 2023. URL: https://inria.hal.science/hal-04112671.

12.3 Cited publications

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

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

[36] W. Castryck, T. Lange, C. Martindale, L. Panny and J. Renes. 'CSIDH: An Efficient Post-Quantum Commutative Group Action'. In: *ASIACRYPT (3)*. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427.

[37] A. Chailloux and J. Loyer. 'Lattice Sieving via Quantum Random Walks'. In: *ASIACRYPT (4)*. Vol. 13093. Lecture Notes in Computer Science. Springer, 2021, pp. 63–91.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] T. Espitau, P.-A. Fouque, F. Gérard, M. Rossi, A. Takahashi, M. Tibouchi, A. Wallet and Y. Yu. 'MITAKA: A Simpler, Parallelizable, Maskable Variant of FALCON'. In: *Eurocrypt 2022 - International Conference on the Theory and Applications of Cryptographic Techniques*. Trondheim, Norway, May 2022, pp. 1–50. URL: https://hal.science/hal-03618678.

[46] 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.

[47] 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.

[48] 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.

[49] C. Gentry, C. Peikert and V. Vaikuntanathan. 'Trapdoors for hard lattices and new cryptographic constructions'. In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. Ed. by C. Dwork. ACM, 2008, pp. 197–206.

[50] 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.

[51] M. Kaplan, G. Leurent, A. Leverrier and M. Naya-Plasencia. 'Quantum Differential and Linear Cryptanalysis'. In: *IACR Trans. Symmetric Cryptol.* 2016.1 (2016), pp. 71–94.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] É. Levieil and P.-A. Fouque. 'An Improved LPN Algorithm'. In: *SCN*. Vol. 4116. Lecture Notes in Computer Science. Springer, 2006, pp. 348–359.

[57] 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.

[58] B. Minaud, P. Derbez, P.-A. Fouque and P. Karpman. 'Key-Recovery Attacks on ASASA'. In: *J. Cryptol.* 31.3 (2018), pp. 845–884.

[59] C. Peikert. 'An Efficient and Parallel Gaussian Sampler for Lattices'. In: *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*. Ed. by T. Rabin. Vol. 6223. Lecture Notes in Computer Science. Springer, 2010, pp. 80–97. DOI: 10.1007/978-3-642-14623-7_5. URL: https://doi.org/10.1007/978-3-642-14623-7%5C_5.

[60] 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.

[61] 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.

[62] A. Schrottenloher and M. Stevens. 'Simplified MITM Modeling for Permutations: New (Quantum) Attacks'. In: *CRYPTO (3)*. Vol. 13509. Lecture Notes in Computer Science. Springer, 2022, pp. 717–747.

[63] P. W. Shor. 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring'. In: *FOCS*. IEEE Computer Society, 1994, pp. 124–134.