CRYPTOEXPERTS

WE INNOVATE TO SECURE YOUR BUSINESS

Offre de stage - Internship Offer

Side-Channel Analysis of a post-quantum encryption scheme without re-encryption

6-months master internship anytime in 2026

Education:	Master's degree
Field:	Cryptography
Company:	CryptoExperts
Workplace:	41 boulevard des Capucines, 75002 Paris

1 Company Presentation

CryptoExperts is a private research lab providing R&D services in cryptography. The company has a team of experts from industry and academia, with PhDs in cryptography, and specialized in various fields. They include public key cryptography (both post- and pre-quantum), symmetric cryptography, efficient and secure implementations, security protocols and proofs, side-channel attacks, and security of embedded systems. CryptoExperts develops innovative cryptographic solutions for various applications, and offers security auditing, custom conception of cryptographic protocols and implementation of cryptographic libraries. The company is also very active in the field of scientific research in cryptography, producing every year several publications in the main conferences in the field, and taking part in various academic and industrial projects on advanced research issues (such as post-quantum cryptography, white-box cryptography, homomorphic encryption, proven security against physical attacks and zero-knowledge proofs).

2 Internship Subject

The potential advent of large-scale quantum computing poses a retroactive threat to current cryptography, making widely deployed encryption and signature schemes such as RSA and elliptic curves vulnerable. In response to this threat, practical post-quantum algorithms have emerged in the past decade to design new cryptographic schemes conjectured resistant to quantum attacks. Among the various approaches explored, schemes based on lattices stand out for their theoretical robustness and practical efficiency. These schemes exploit the hardness of certain lattice problems, such as the Shortest Vector Problem (SVP) or the Learning With Errors (LWE) problem, which are believed to be hard even for quantum adversaries. Constructions such as ML-KEM, now standardized by NIST [fip24], illustrate the potential of this approach. However, the secure implementation of these schemes on embedded devices remains a major challenge, particularly in the presence of side-channel attacks that exploit the physical leakages of devices, notably through execution time, power consumption, or electromagnetic emissions.

In many settings of public key encryption, one should take into account active attackers. In these attacks, malicious attackers could modify the ciphertexts in transit, potentially leading to unauthorized decryption. To avoid such attacks, the transform that is named Fujisaki-Okamoto (FO) [FO99] is commonly applied. However, this transformation introduces an additional re-encryption phase inside the decryption, which significantly complicates implementations and increases the number of potential physical leakage points. These leakages, measurable at the hardware level, can be exploited using side-channel attacks to extract sensitive information, even when the scheme is theoretically secure. The above cited post-quantum standard ML-KEM indeed relies on this FO transformation and this step has been the target of numerous physical attacks in the literature.

Therefore, exploring alternatives to the FO transform remains essential for constrained environments, such as smart cards or IoT devices, where mitigating physical leakages is

crucial. The POLKA scheme, presented in [HLM+23], proposes an alternative construction to ML-KEM that replaces the dependence on FO with another simpler mechanism denoted norm check. This new design has also been analyzed in [HHMS25]. This norm check mechanism thus offers a more direct path to implementations that are potentially less exposed to physical leakages by design.

Nevertheless, an evaluation of potential leakages and experimental validation is necessary to confirm practical robustness. This internship aims to conduct a comprehensive study of POLKA's resistance to side-channel attacks, combining theoretical analysis and practical experimentation.

The objective of the internship is to validate the resistance of POLKA to physical attacks and, depending on the theoretical and empirical results, to propose attacks, countermeasures, and/or concrete improvements.

2.1 Objectives

The internship will be structured around several phases in order to provide a comprehensive analysis of POLKA's resistance to side-channel attacks.

1. Understanding the POLKA scheme. The first phase will focus on gaining a deep understanding of the POLKA cryptographic scheme as opposed to the future standardized ML-KEM. The first phase will involve studying and implementing a Python proof of concept of the key generation, encryption, and decryption algorithms, with particular attention to the differences from ML-KEM and the replacement of the FO transform. This will be followed by systematic identification of all sensitive variables manipulated during execution, including secret keys, intermediate values, and temporary variables that could leak secret information exploitable through side-channel attacks. Finally, a study on the underlying mathematical assumptions, particularly the Ring Learning With Errors (RLWE) and Learning With Physical Rounding (LWPR) problems and the current cryptanalysis techniques, will be conducted.

2. Implementation analysis and side-channel attacks. Building on the theoretical understanding, this phase will examine the concrete implementation and existing work on side-channel weaknesses, in order to propose performance improvements or new attack targets. This phase will begin with studying and reproducing existing side-channel attacks on POLKA's implementation. While the literature on this subject is not yet well developed, some preliminary attacks already exist. The intern will first collect traces with simulation and/or with a side-channel measurement platform (*e.g.*Chipwhisperer). Next, these attacks will be implemented and their performance and success rate will be analyzed. Subsequently, the intern will work on potentially improving these attacks, either by optimizing the existing techniques or by proposing new strategies based on the understanding of the scheme and its implementation.

3. Additional contributions. Depending on the results of the attack phase and the remaining time, several complementary directions can be explored. POLKA is a recent scheme

with many new interesting design directions to explore. Possible directions include: the proposal and evaluation of specific countermeasures, the design of more generic countermeasures, or even modifications to the core design of POLKA.

4. Final report and dissemination. The internship will conclude with the writing of a detailed technical report and presentation of results to CryptoExperts' team and potentially to the broader cryptographic community.

3 Candidates

This internship offer is for a Master student who has a taste for cryptography and research. The candidate will have to demonstrate a solid background in mathematics and/or computer science with a specialization in cryptography. The technical background required for this internship combines skills in algebra (finite fields, polynomials, etc.) as well as ease in programming (mostly in Python). The candidate will have to demonstrate autonomy and dynamism. A good level of English will also be a plus. After a first interview, selected candidates will be given a challenge to carry out at home before a second technical interview.

4 Internship Conditions

The intern will be supervised by Mélissa Rossi and Gabriel Zaid, researchers in cryptography. The internship duration is 6 months and can start anytime in 2026. The candidate will have an office in our open space in CryptoExperts' premises located in Paris (41 boulevard des Capucines, 75002 Paris). The location allows an interesting emulation among our team composed of researchers, PhD students and other interns. Remote work is also possible most of the time. The company offers many advantages (1 week holiday for interns, flexible hours, restaurant vouchers, public transport refund). The intern is also an integral part of the team and is invited to any social event of the company. The monthly stipend is €1801.80 gross.

5 Contact

To apply for this internship offer, please send your résumé to

Mélissa Rossi: `melissa.rossi@cryptoexperts.com`,

References

[fip24] *Module-lattice-based key-encapsulation mechanism standard*. August 2024.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554. Springer, Berlin, Heidelberg, August 1999.

[HHMS25] Kathrin Hövelmanns, Andreas Hülsing, Christian Majenz, and Fabrizio Sisinni. (Un)breakable curses - re-encryption in the Fujisaki-Okamoto transform. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part II*, volume 15602 of *LNCS*, pages 245–274. Springer, Cham, May 2025.

[HLM+23] Clément Hoffmann, Benoît Libert, Charles Momin, Thomas Peters, and François-Xavier Standaert. POLKA: Towards leakage-resistant post-quantum CCA-secure public key encryption. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023, Part I*, volume 13940 of *LNCS*, pages 114–144. Springer, Cham, May 2023.