Fixed-point implementation of Falcon and FN-DSA

Graduate Internship (Master 2), Summer 2025

Location	PQShield SAS, Paris 8 Rue des Pirogues de Bercy
Contact	Thomas Prest
Starting date and duration	Q2 2025 (flexible), 6 months
Gross salary	1350 € / month

Internship

Background

The Falcon (Fast-Fourier Lattice-based Compact Signatures over NTRU) signature scheme has been selected in 2022 by NIST as the future standard "FN-DSA", after 5 years of scrutiny in its PQC Standardization process. Falcon presents several desirable features such as compact signature sizes and fast verification. However, its reliance on floating-point arithmetic presents implementation challenges, particularly for constrained devices, secure hardware implementations, and environments where floating-point support is limited or unavailable.

The removal of floating-point arithmetic and the adoption of a fully integer-based approach would significantly enhance Falcon's portability, performance, and security on various platforms, and would largely increase its scope of deployment. **The goal of this project is to implement Falcon without floating-point arithmetic.**

Objectives

The main objectives of this internship project are to:

1. Understand the existing Falcon signature scheme and identify the parts where floating-point arithmetic is used.
2. Develop alternative methods using integer arithmetic and fixed-point arithmetic.
3. Implement the modified Falcon scheme and evaluate its performance in terms of speed, memory usage, and security compared to the standard implementation.

About PQShield

PQShield is a cybersecurity scaleup that specialises in post-quantum cryptography, protecting information from today's attacks while preparing organisations for the threat landscape of tomorrow. It demonstrates quantum-safe cryptography on chips, in applications and in the cloud. We are headquartered in Oxford, with additional teams in the Netherlands, Germany and France.

PQShield SAS, based in Paris (France), concentrates the research activities of PQShield. Our mission is to come up with innovative algorithmic and/or protocol-level solutions to real-world cryptographic problems. Besides post-quantum cryptographic primitives, our research interests include implementation security and advanced cryptosystems and protocols such as secure messaging, threshold schemes, and multiparty computation.

Requirements and how to apply

Ideal candidates should possess as many of these qualities as possible:

- Excellent skills in discrete algorithms and the ability to understand and reason with mathematical algorithms such as fast Fourier transforms, linear algebra.
    - In particular, the candidate should be confident in their ability to understand and implement the Falcon signature scheme [1].
- Proficiency in at least one programming language.
- Strong autonomy.
- Good communication skills.

Supervision: The intern will be supervised by Thomas Prest.

References

1. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang. *Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU.* https://falcon-sign.info/