Improving the memory footprint of MPCitH

Graduate Internship (Master 2), Summer 2025

Location	PQShield SAS, Paris 8 Rue des Pirogues de Bercy
Contact	Rafael Del Pino, Morgane Guerreau
Starting date, duration	Q2 2026 (flexible), 6 months
Gross salary	1350 € / month

Internship

Background

The **NIST call for additional post-quantum signature schemes** has sparked a surge of candidates based on the **MPC-in-the-Head (MPCitH)** paradigm. Among these, **FAEST** stands out for its solid security foundation built on **AES**. MPCitH-based schemes are attractive due to their **competitive signature and key sizes**, making them strong contenders for future cryptographic standards.
However, their **efficiency remains a challenge**, particularly regarding **memory consumption**—current implementations can require tens of megabytes of memory to achieve reasonable performance. Improving the **memory footprint** of MPCitH schemes is therefore a key step toward making them practical for **real-world deployment**.

Objectives

The main objectives of this internship project are to:

1. **Understand** the fundamentals of the MPCitH paradigm and acquire in-depth knowledge of the **FAEST** scheme and its components (notably **VOLEitH** and the **Quicksilver** proof system).
2. **Implement** a proof-of-concept version of FAEST and use **profiling tools** to identify major memory bottlenecks.
3. **Optimize** these bottlenecks using more efficient algorithms (e.g., **streaming algorithms**) and primitives (e.g., **lightweight pseudorandom generators**).
4. **Explore** potential improvements to the VOLEitH framework or develop new techniques to achieve **more efficient signatures**.

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:

- Proficiency in C programming language.
    - Basic knowledge of profiling tools.
- Basic knowledge in cryptography
- Strong autonomy.
- Good communication skills.

Supervision: The intern will be supervised by Rafael Del Pino and Morgane Guerreau

References

1. https://csrc.nist.gov/projects/pqc-dig-sig
2. https://faest.info/