Implementation security of post-quantum digital signatures

Graduate Internship (Master 2), Summer 2025

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

Internship

Background

Even the most secure cryptographic algorithm can be rendered ineffective if its implementation contains vulnerabilities. A recent example is the PQShield-discovered clangover vulnerability (CVE-2024-37880) in several open-source implementations of ML-KEM, the new NIST standard for post-quantum key exchange.

As part of an effort to mature the implementation maturity of post-quantum cryptography (PQC), this internship aims to evaluate the implementation security of cutting-edge **post-quantum digital signatures**.

Scope of the internship

The student will leverage and extend in-house PQShield security tooling to evaluate the security of publicly available implementations of PQC signatures. The evaluation techniques in scope of this internship are as follows:

- **Constant-time analysis**: Assess whether PQC software implementations expose sensitive data through variations in execution time.
- **Differential fuzzing**: Identify memory corruption issues and functional bugs in PQC software implementations using fuzzing techniques.

This project is primarily hands-on and comprises the following phases:

1. **Literature review**
    - understand the landscape of post-quantum digital signatures
    - understand the working principles behind different leakage detection methodologies
2. **Tool exploration**
    - explore the state of the art in leakage detection and/or differential fuzzing tooling
3. **Practical Evaluations**
    - establish test scenarios for a selection of PQC signatures
    - use (and where relevant: extend) in-house PQShield security tooling to evaluate these signature schemes

A potential (but unpredictable) outcome is the discovery of one or more bugs or vulnerabilities. If this happens, PQShield will, together with the intern, report them to the affected instances.

About PQShield

PQShield is a cybersecurity scaleup that specialises in post-quantum cryptography, protecting information from today's attacks while readying organisations for the threat landscape of tomorrow. PQShield is headquartered in Oxford, with additional teams in the Netherlands, Germany, Belgium and France.

PQShield comprises a world-class collaboration of post-quantum cryptographers, engineers, and researchers. We've helped shape all of the first international PQC NIST standards, and we were the first cybersecurity company to develop quantum-safe cryptography on chips, in applications, and in the cloud.

Requirements and how to apply

Ideal candidates should possess:

- Prior experience or coursework in cryptography
- Strong proficiency in at least one programming language, and at least some familiarity with C
- Proficiency in Linux operating systems, including command-line tools and scripting
- Familiarity with version control systems (e.g., Git)
- Excellent communication skills
- Optional but big plus: familiarity with timing attacks

Supervision and Mentorship: The intern will be mentored remotely by members of PQShield's Product Security Team, with frequent progress meetings to facilitate knowledge exchange and to track progress.