Post-Quantum Threshold Signature Scheme Without Lattice Assumptions

Masters Internship Proposal, Télécom Paris

2025

Context

As quantum computers pose a threat to current cryptographic systems like RSA and Elliptic Curve Cryptography (which rely on problems easily solvable by quantum algorithms), **post-quantum cryptography** (PQC) aims to create secure alternatives resistant to quantum attacks.

While lattice-based cryptography has been a dominant approach in PQC, using problems like the Shortest Vector Problem (SVP) and Learning With Errors (LWE), it faces challenges such as large key sizes and inefficiency. Finding alternatives is also important in order to be resilient against a major breakthrough in lattice-based cryptanalysis.

For basic primitives (public-key encryption and digital signatures) there exist alternative assumptions that could also provide security in the quantum era, such as **code-based cryptography** (e.g., the McEliece cryptosystem [1] or the SDiTH signature scheme [2]).

However, for **advanced primitives**, there is a lack of diversity, as most of the post-quantum constructions are based on lattice assumptions. An advanced primitive refers to a cryptographic construction that builds upon basic components (encryption, signatures, hashing) to provide more complex and versatile functionalities. They are designed to address sophisticated cryptographic needs and often underpin more specialized or advanced cryptographic protocols.

Recently, there has been a surge of interest for a specific category of advanced primitives: **threshold cryptography**. Threshold cryptography is a technique in cryptography where a secret, such as a private key, is divided into multiple parts, and only a subset (or threshold) of those parts is required to perform a cryptographic operation. The purpose of threshold cryptography is to increase security and fault tolerance by distributing trust among multiple parties, rather than relying on a single individual or system. The **interest of the research community** for threshold cryptography is demonstrated by NIST's First Call for Multi-Party Threshold Schemes [3], which also includes a subcategory focused on quantum-resistant fully homomorphic encryption.

Research project

The main objective of this internship would be to **design** and **analyze** a post-quantum **threshold signature** scheme relying on **code-based assumptions**: specifically the Decoding Problem (DP) or its closely related variant, Learning Parity with Noise (LPN). These assumptions provide robust alternatives to LWE, featuring distinct structural advantages and resilience to specific attack vectors. Both Hamming and rank metric can be explored when switching to

code-based assumptions, potentially yielding innovative solutions.

A threshold signature scheme allows a group of participants to collectively sign a message or transaction in such a way that a subset of the participants (meeting a predefined threshold) can produce a valid signature. Each participant holds a partial secret key. An example of efficient lattice-based threshold signature scheme is TRaccoon [4].

The internship would begin with familiarizing with some code-based (non-threshold) signature schemes, such as:

- Durandal [5], or
- Wave [6]

Then, the intern will focus on adapting one of the chosen signature schemes to support threshold cryptography. This will involve developing **security proofs** for the new constructions, accounting for the unique properties of low-Hamming weight noise typical in DP and LPN, as well as proposing **parameter sets** that ensure both practicality and robust security. Optionally, the intern could propose an **implementation** of the designed scheme to empirically validate their efficiency and feasibility for real-world applications.

Required skills

- Linear algebra, finite fields
- Strong knowledge in cryptography
- (preferred) Basic knowledge of post-quantum cryptography (lattice-based or code-based)
- (optional) C++ and/or Python

Practical information

The intern will be located in Télécom Paris (Paris - Palaiseau), hosted in the Cybersecurity and Cryptography [C²] team. She/he will be co-advised by:

- Victor Dyseryn (`https://victordyseryn.github.io`)
- Duong Hieu Phan (`https://www.di.ens.fr/~phan`)

The intership may be followed by a PhD on advanced primitives in post-quantum cryptography beyond lattice assumtpions.

Contact: victor.dyseryn@telecom-paris.fr

Starting date, duration: February-March 2025 (flexible), 6 months

References

[1] McEliece, R. J. (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory. DSN Progress Report.

[2] Carlos Aguilar Melchor, Thibauld Feneuil, Nicolas Gama, Shay Gueron, James Howe, David Joseph, Antoine Joux, Edoardo Persichetti, Tovohery H. Randrianarisoa, Matthieu Rivain, Dongze Yue (2023). SDiTH. First-round submission to NIST call for additional post-quantum signature schemes (`https://csrc.nist.gov/projects/pqc-dig-sig`)

[3] NIST (2023). First Call for multi-party threshold schemes (initial public draft) (https://csrc.nist.gov/projects/threshold-cryptography)

[4] Rafaël Del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, Markku-Juhani O. Saarinen (2024) Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions. EUROCRYPT 2024.

[5] Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, Gilles Zémor. (2019) Durandal: A Rank Metric Based Signature Scheme. EUROCRYPT 2019.

[6] Thomas Debris-Alazard, Nicolas Sendrier, Jean-Pierre Tillich. (2019) Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes. ASIACRYPT 2019.