Master internship: Zero-Knowledge proofs based on lattice problems, with applications to threshold signatures

Matthieu Rambaud[†] and Weiqiang Wen[†]

[†]@telecom-paris.fr

Mundane context. "Threshold cryptography" are mechanisms enabling a number n distrustful participants to obtain the output of some computation on secret data as soon as a threshold number $t < n$ of them participates, but reveals nothing otherwise. The most known mechanism, apart from the mere storing of the secrets, is called *threshold signatures*. It enables n machines to produce a single signature on behalf of a client, such that any colluding t machines are unable to create a signature which was not queried by the client. This technique is used by Coinbase (32Bn$ market cap) to manage the crypto-wallets of more than 5M clients [3, 10], as well as by Fireblocks (8Bn$ market cap) [7]. Threshold signatures enable to solve the trilemma of a client needing to quickly sign transactions, but at the same time not leaking its secret signing-key to the adversary nor having its key erased by accident (if it was stored only on a single machine). Hence, they are one of the main building blocks of the so-called "crypto-custody" market, which is 450Bn$ worth [4, 8]. The leader in France is Dfns, and the startup Zama is specialized in decentralized contracts with confidential inputs.

Goals of the internship. The first proposed goal is to describe and prove a threshold signature which is resilient to adversaries having quantum computers, ideally detailed enough to be submitted to the NIST competition (national institute of standards and technology) [13]. The construction which we have in mind is based on the hardness of lattice problems. Despite intense international activity towards this same goal [15, 14, 6, 5, 2], we have a new angle of attack for practical applications. Hence, the internship should naturally lead to international collaborations, before or after the start of the intended PhD. The second proposed goal revolves around anonymity, we can share more details during the interview. The main technical tool which will be used in the construction are the so-called zero-knowledge (ZK) proofs. A ZK proof enables the holder of a secret s to exhibit y and a function f to anyone, dubbed a verifier, and convince the verifier that $y = f(s)$ without having to reveal s. Lattice-based ZKs are now well documented and implemented ([11, 1, 12], as well as clear M2 reports of previous internships). Nevertheless, there exists elaborate optimizations based on advanced arithmetics, e.g., [9]. Hence, there is much room for initiatives of improvements by the intern(s), in particular, when applied to the proposed constructions.

References

[1] W. Beullens and G. Seiler. "LaBRADOR: Compact Proofs for R1CS from Module-SIS". In: *CRYPTO*. 2023.
[2] R. Chairattana-Apirom, S. Tessaro, and C. Zhu. "Partially Non-Interactive Two-Round Lattice-Based Threshold Signatures". In: *Asiacrypt*. 2024.
[3] Coinbase. *Building user-focused web3 wallets at Coinbase*. link. 2023.
[4] Cointelegraph. *Crypto custody market reached $448 billion in 2022: Report*. link. 2024.
[5] T. Espitau, S. Katsumata, and K. Takemure. "Two-Round Threshold Signature from Algebraic One-More Learning with Errors". In: *CRYPTO*. 2024.
[6] T. Espitau, G. Niot, and T. Prest. "Flood and Submerse: Distributed Key Generation and Robust Threshold Signature from Lattices". In: *CRYPTO*. 2024.
[7] Fireblocks. link.
[8] M. Geihs and H. Montgomery. "LaKey: Efficient Lattice-Based Distributed PRFs Enable Scalable Distributed Key Management". In: *USENIX*. 2024.

[9] M. Klooß, R. W. F. Lai, N. K. Nguyen, and M. Osadnik. “RoK, Paper, SISsors – Toolkit for Lattice-based Succinct Arguments”. In: *Asiacrypt*. 2024.
[10] Y. Lindell. *Cryptography and MPC in CoinbaseWallet as a Service (WaaS)*. link. 2023.
[11] V. Lyubashevsky, N. K. Nguyen, and M. Plancon. “Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General”. In: *CRYPTO*. 2022.
[12] V. Lyubashevsky, G. Seiler, and P. Steuer. *The LaZer Library: Lattice-Based Zero Knowledge and Succinct Proofs for Quantum-Safe Privacy*. ePrint 2024/1846. 2024.
[13] NIST. *First Call for Multi-Party Threshold Schemes*. link. 2023.
[14] R. D. Pino, S. Katsumata, M. Maller, F. Mouhartem, T. Prest, and M. O. Saarinen. “Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions”. In: *EUROCRYPT*. 2024.
[15] G. Tang, B. Pang, L. Chen, and Z. Zhang. “Efficient Lattice-Based Threshold Signatures With Functional Interchangeability”. In: *IEEE Trans. Inf. Forensics Secur.* (2023).