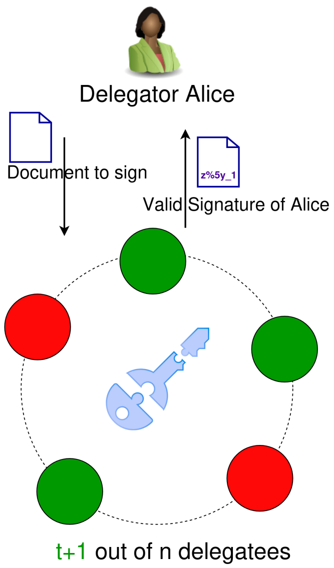
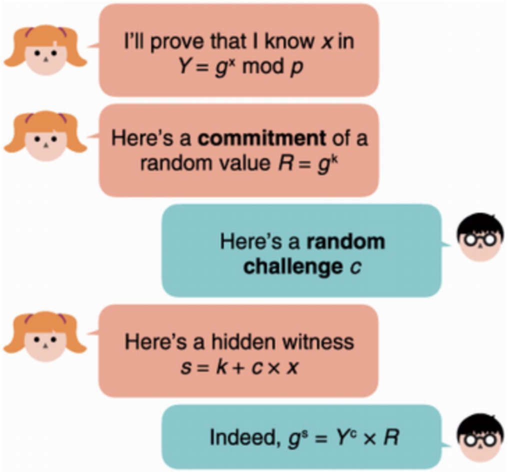
(Research Internship) Threshold (homomorphic) encryption and signatures from lattice-based cryptography

Katharina Boudgoust* Anamaria Costache† Matthieu Rambaud‡




I'll prove that I know x in $Y = g^x \bmod p$
Here's a **commitment** of a random value $R = g^k$
Here's a **random challenge** c
Here's a hidden witness $s = k + c \times x$
Indeed, $g^s = Y^c \times R$

"Threshold cryptography" refers to cryptographic systems that enable a number n of participants to collectively evaluate some function over all their secret inputs, without disclosing their inputs to one another (as can be seen in the picture above). They deliver an output as soon as a threshold number $t+1 < n$ of them participate honestly, and do not leak the secrets inputs as long as at most t participants maliciously collude. The main goals of threshold cryptography are to distribute trust and to increase the robustness.

Among the most known threshold primitives are ***threshold signatures*** [CdPE+26a]. They enable 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. Threshold signatures are used by Coinbase (32Bn$ market cap) to manage the crypto-wallets of more than 5M clients [Coi23], by Fireblocks (8Bn$ market cap) [Fir21], and by their French competitor Dfns in collaboration with Matthieu Rambaud. These deployments are part of the market of digital asset custody, which was worth over 600 Billion dollars in 2024 and is expected to skyrocket in the coming years [Gra25]. A more advanced example is ***threshold fully homomorphic encryption (ThFHE)*** [BC25, HLW+26], of which a flagship application is to enable a group of distrustful nodes to validate confidential transactions on the blockchain without seeing their amounts (e.g. JP Morgan + the French startup Zama [Kin24], and the concurrent system of Circle [Inc24]).

Various possible internship goals. The internship is motivated by the NIST call [NIS26] for designing threshold signatures to become standardized. The broad goal would be to aim at threshold signatures based on (post-quantum) lattice problems, enabling more participants and/or offering increased security & robustness guarantees, than the state of the art. Indeed, the only lattice-based threshold signature which enjoys a small standard size ("ML-DSA") [CdPE+26a] operates for at most

*CNRS, Univ Montpellier, LIRMM. Email: katharina.boudgoust@lirmm.fr
†École Polytechnique. Email: costache@lix.polytechnique.fr
‡Télécom Paris. Email: matthieu.rambaud@telecom-paris.fr

6 participants. There exists propositions to NIST for scalable threshold signatures [CdPE+26b], but with drawbacks preventing practical use.

An alternative project which would be interesting is to design a post-quantum *distributed key generation (DKG)*. DKG is a protocol which is used to set up the participants in a threshold system. In particular, this is when the key shares for each participant are generated. Specifically, the internship would continue our ongoing research work on *non-interactive* DKG, such as [KMM+24], based sharing on non-interactive sharing of a secret key [GHL22]. One of the many possibilities would be to specialize in re-sharing key shares to new participants [CdPE+26b].

One technical tool to make the constructions complete, although not necessary for the internship, are the so-called zero-knowledge (ZK) proofs [QSL+25]. A ZK proof enables the holder of a secret x to exhibit Y and a function f to anyone, dubbed a verifier, and convince the verifier that it knows the solution x to $Y = f(x)$ without having to reveal x (on the right picture, $f(x) = g^x$). Lattice-based ZKs are now well documented and implemented ([LNP22, ESLR23, BS23, CMS+24, LSS24], as well as clear M2 reports of previous internships). Nevertheless there is room, if the candidate likes, to shift the goal of the internship to optimize the ZKs needed in the constructions. Indeed, the specific needs of thresholds signatures and DKG call for optimizations (some possibly based on advanced arithmetics, e.g., [KLNO24, DK22]).

Location Ideally at Telecom Paris (neighboring Inria Saclay), but with possibility to potentially also go to Montpellier.

References

[BC25] Katharina Boudgoust and Anamaria Costache. Improved rényi arguments for lattice-based threshold encryption. *IACR Cryptol. ePrint Arch.*, 2025.

[BS23] Ward Beullens and Gregor Seiler. Labrador: Compact proofs for R1CS from module-sis. In *CRYPTO*, 2023.

[CdPE+26a] Sofía Celi, Rafaël del Pino, Thomas Espitau, Guilhem Niot, and Thomas Prest. Efficient threshold ML-DSA. In *Usenix Security*, 2026.

[CdPE+26b] Sofía Celi, Rafaël del Pino, Thomas Espitau, Guilhem Niot, Thomas Prest, and Kaoru Takemure. Hermine: An efficient raccoon-style non-interactive threshold signature with advanced properties, 2026. https://csrc.nist.gov/presentations/2026/mpts2026-3b3.

[CMS+24] Sylvain Chatel, Christian Mouchet, Ali Utkan Sahin, Apostolos Pyrgelis, Carmela Troncoso, and Jean-Pierre Hubaux. PELTA – shielding multiparty-FHE against malicious adversaries. In *CCS*, 2024.

[Coi23] Coinbase. Building user-focused web3 wallets at coinbase, 2023. link.

[DK22] Samed Düzlü and Juliane Krämer. Application of automorphic forms to lattice problems. *J. Math. Cryptol.*, 2022.

[ESLR23] Muhammed F. Esgin, Ron Steinfeld, Dongxi Liu, and Sushmita Ruj. Efficient hybrid exact/relaxed lattice proofs and applications to rounding and vrfs. In *CRYPTO*, 2023.

[Fir21] Fireblocks. Mpc and key refresh. link, 2021.

[GHL22] Craig Gentry, Shai Halevi, and Vadim Lyubashevsky. Practical non-interactive pvss with thousands of parties. In *EUROCRYPT*, 2022.

[Gra25] Grand View Research. Digital asset custody market (2025–2033), 2025. Report ID: GVR-4-68040-770-2.

[HLW+26] Zhenkai Hu, Haofei Liang, Xiao Wang, Xiang Xie, Kang Yang, Yu Yu, and Wenhao Zhang. Ajax: Fast threshold fully homomorphic encryption without noise flooding. In *Usenix*, 2026.

[Inc24] Circle & Inco. Confidential ERC20 Framework using Fully Homomorphic Encryption (FHE), 2024. file:///home/matthieu/T%C3%A9l%C3%A9chargements/whitepaper.pdf.

[Kin24] Zama & JP Morgan Kinexys. Project EPIC, 2024. https://www.zama.org/post/kinexys-by-jpmorgan-releases-a-proof-of-concept-leveraging-zama-fhevm and https://www.jpmorgan.com/kinexys/documents/JPMC-Kinexys-Project-Epic-Whitepaper-2024.pdf.

[KLNO24] Michael Klooß, Russell W. F. Lai, Ngoc Khanh Nguyen, and Michał Osadnik. RoK, paper, SISsors – toolkit for lattice-based succinct arguments. In *Asiacrypt*, 2024.

[KMM+24] Aniket Kate, Easwar Vivek Mangipudi, Pratyay Mukherjee, Hamza Saleem, and Sri Aravinda Krishnan Thyagarajan. Non-interactive VSS using class groups and application to DKG. In *CCS*, 2024.

[LNP22] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plancon. Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. In *CRYPTO*, 2022.

[LSS24] Vadim Lyubashevsky, Gregor Seiler, and Patrick Steuer. The lazer library: Lattice-based zero knowledge and succinct proofs for quantum-safe privacy. In *CCS*, 2024.

[NIS26] NIST. First call for multi-party threshold schemes, 2026. https://csrc.nist.gov/pubs/ir/8214/c/final.

[QSL+25] Wenjie Qu, Yijun Sun, Xuanming Liu, Tao Lu, Yanpei Guo, Kai Chen, and Jiaheng Zhang. zkgpt: an efficient non-interactive zero-knowledge proof framework for llm inference. In *USENIX Security Symposium*, 2025.