SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

A Practical Lattice-Based Threshold Signature

Yi Xu * Yuntao Wang * Eiichiro Fujisaki *

Keywords: threshold signatures, lattice, Fiat-Shamir Signature Scheme

—

Abstract

Threshold cryptography schemes can be applied to many areas, and a well-known example is Bitcoin. Bitcoin was invented in 2008 by "Satoshi Nakamoto" and has gained much intention in recent years. Research produced by the University of Cambridge estimated that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using Bitcoin. To use Bitcoin, everyone should own a wallet that stores the collections of one's public key and private key. If the wallet is compromised, the Bitcoin will be stolen. Correspondently, an alternative countermeasure is to split keys into several shares. Only a threshold set of shares can sign a transaction in this situation. Bitcoin is currently signed with an ECDSA, which is vulnerable to quantum computers, so it prefers to be replaced by signatures with Post-Quantum Cryptography (PQC) properties. The NIST is holding a PQC standardization project [AASA+20], and nine signature schemes are selected for the second round in 2019. It includes three lattice-based signature schemes, and two of them are Fiat-Shamir based, which suggests the lattice-based Fiat-Shamir signatures are promising.

In this paper, we propose a practical (k, n) threshold signature by adapting the $\{0, 1\}$-Linear Secret Sharing Scheme technique [BGG+18] to a without rejection variant of Lyubashevsky's signature scheme [Lyu09, Lyu12, ASY21], so a threshold of parties can produce a valid signature. The security of our scheme is based on the hardness of finding an approximate shortest vector and the Learning With Errors problem in the random oracle model, and its security is not deteriorated compared to the n-out-of-n threshold signatures. When creating a partial signature, since it is a Fiat-Shamir type, a public channel between signers is required. Although it is not round optimal, partial signature generation always ends in three rounds of Multi-Party Communications.

References

[AASA+20] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status report on the second round of the nist post-quantum cryptography standardization process. *US Department of Commerce, NIST*, 2020.

[ASY21] Shweta Agrawal, Damien Stehlé, and Anshu Yadav. Towards practical and round-optimal lattice-based threshold and blind signatures. *IACR Cryptol. ePrint Arch.*, 2021:381, 2021.

[BGG+18] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai. Threshold cryptosystems from threshold fully homomorphic encryption. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 565–596. Springer, Heidelberg, August 2018.

[Lyu09] Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 598–616. Springer, Heidelberg, December 2009.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 738–755. Springer, Heidelberg, April 2012.

* Japan Advanced Institute of Science and Technology (JAIST)