Technical University of Munich

Thesis M.Sc.

Threshold Signatures for Digital Currency Payment Protocols

Motivation

Central banks around the world are investigating the introduction of Central Bank Digital Currencies (CBDC) as a digital complement to cash. This will likely create a whole ecosystem of products and services. While CBDC share some characteristics with cryptocurrencies, they serve different purposes. For that various solutions are being discussed and G+D develops a CBDC platform relying on the latest research and available technology.
In this context, threshold cryptography is a field of research that is particularly interesting. Its goal is to decentralize cryptographic operations and carry them out with distributed key material. In the emerging technology of token-based digital currency, some of its protocols and algorithms might be beneficial in order to improve the security of asset storage, token validation, and transaction authorization. Ideally, the findings of this thesis can be generalized towards other digital currencies solutions as well.
We are seeking a motivated student who wants to join our research efforts for a degree project/thesis. In your work, you would analyze how a threshold signature scheme could be integrated into a digital payment protocol, compare different algorithms and possibly implement a proof of concept.

Your Task

- Familiarize yourself with the topics of threshold cryptography
- Research on the existing solutions
- Design a fitting protocol to Filia payment protocol
- Build a proof-of-concept (PoC) implementation
- Evaluate the performance of the system

Qualifications

- Master's program in computer science, computer security, mathematics, or a related field
- Strong interest in cryptography
- Basic skills in programming and software engineering
- Strong communication and collaboration abilities

Sources

- [1] https://www.gi-de.com/en/payment/central-bank-digital-currencies
- [2] Aumasson, J. P. et al. (2020). A survey of ECDSA threshold signing.
- [3] Tillem, G., et al. Threshold Signatures using Secure Multiparty Computation.

Contact

Filip Rezabek	frezabek@net.tum.de
Kilian Glas	glas@net.in.tum.de
Franziska Kreitmair (G+D)	franziska.kreitmair@gi-de.com