Chair of Network Architectures and Services
School of Computation, Information, and Technology
Technical University of Munich

Thesis M.Sc.

Assessment of Post-Quantum Threshold Signing Systems

Motivation

Threshold signing (TS) is a cryptographic technique that allows a group of nodes to collaboratively generate a digital signature without any single node holding the complete private key. This approach enhances security and fault tolerance by requiring a minimum number of nodes to cooperate in producing a valid signature, thereby mitigating the risk of key compromise.
Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to withstand the potential threats posed by quantum computers. These quantum systems can efficiently solve mathematical problems that classical cryptography relies upon. In contrast, PQC employs novel mathematical challenges that are believed to remain difficult even for quantum computers, ensuring the continued security of sensitive data in a future influenced by quantum computing.
The primary objective of this research is to investigate the current state of PQC TS systems, deepen our understanding of their functionality and properties, and evaluate the available implementations.

Your Tasks

- Conduct a comprehensive literature review to assess the current state of PQC TS systems.
- Identify and evaluate available implementations, selecting the most promising one.
- If necessary, implement the networking aspect to make the PQC TS system network-ready, as many TS implementations do not address this component.
- Develop an experimental setup to evaluate the performance of the networked PQC TS system under varying conditions, such as different node counts and thresholds.

If a suitable implementation cannot be identified, this thesis may continue previous work on a TS emulator. This emulator was designed to replicate the behavior of actual TS systems by exchanging realistic dummy payloads through various transport protocols between emulator nodes, simulating processing times, and more. Your task would be to leverage the knowledge gained from the analysis of PQC TS to enhance the emulator's capabilities.

Prerequisites

- A background in cryptography, networking, and distributed systems is highly recommended.

Contact

Filip Rezabek rezabek@net.in.tum.de
Holger Kinkelin kinkelin@net.in.tum.de
Dominik Marchsreitner dominik.marchsreiter@tum.de