Department of Informatics
Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

Feasibility Study of Threshold BLS Signature Scheme for Tamper-Resistance Signature Service

Motivation

Threshold signature schemes require only t-of-n active signers to generate a signature. This brings robustness and unforgeability properties to the system. Robustness means that t honest peers are sufficient to produce a valid signature. Unforgeability says that $t-1$ malicious peers *cannot* create a valid signature. To use these benefits, we need to modify traditional signature scheme steps: (1) Regarding the private-public key generation, we need to distribute the private key into n shares. (2) For signing, we collect at least t partial signatures to create a signature.

In this thesis, we want to focus on threshold signature schemes based on elliptic curves (EC). Namely, we talk about Boneh-Lynn-Schacham(BLS) [1], [2]. This is a follow-up work to previous work focused on assessment of other threshold signature schemes. We want to extend the deployments by additional experiments, evaluate recent progress. Overall EC solutions offer better performance, less memory overhead, and are therefore more suitable for applications on constrained devices.

However, as robustness and tamper-resistance are achieved by distributing the private key to various shares physically stored on different peers, the protocol used to generate a signature causes some overhead. As this scheme shall be used in a scenario of autonomous driving security, where performance is essential, we are especially interested how well the signing protocol scales.

Your Tasks

- Familiarize yourself with the topic (scenario, BLS/EC based cryptography protocols, threshold schemes, key generation etc.)
- Research on available implementations of suitable threshold cryptography protocols
- Work out a concept how the signing mechanism could be integrated into the above explained scenario
- Implement the concept
- Evaluate performance of the system

References

[1] https://link.springer.com/article/10.1007%2Fs00145-004-0314-9
[2] https://tools.ietf.org/html/draft-boneh-bls-signature-00

Contact

Filip Rezabek	rezabek@net.in.tum.de
Richard von Seck	seck@net.in.tum.de
Dr. Holger Kinkelin	kinkelin@net.in.tum.de