

Thesis
M.Sc.

IDP,
Guided
Research

Securing co-SNARK Proof Generation Offloading

Motivation

Zero-knowledge proofs like zk-SNARKs are cryptographic mechanisms that enable proofs on secrets without revealing any secret data. Especially verification of these proofs is fast and can often be completed within milliseconds. This makes zk-SNARKs popular for various privacy-preserving applications like identity verification, confidential transactions or private voting. However, this fast verification comes at the price of a resource-consuming proof generation. Especially on resource-constrained devices, proof generation is often impossible. Co-SNARKs have been proposed to overcome this limitation. Contrary to classical zk-SNARKs, co-SNARKs allow multiple provers to collaborate on creating a proof without sharing their secrets. This is achieved by combining Multi-Party Computation (MPC) with zk-SNARKs. By offloading the proof generation to a group of co-SNARK provers, these provers can generate a proof without learning the user's secret. This allows users with limited computing power to utilize zk-SNARKs. Your task will be to implement a system in which the user securely secret-shares the information with multiple provers and gets one zk-SNARK proof in return without revealing any secret data.

Your tasks

- Familiarize yourself with co-SNARKs and previous work on zk-SNARKs and MPC
- Implement a protocol allowing secure proof offloading to multiple proving parties
- Conduct a security analysis of the proposed solution
- Perform an experimental performance evaluation by collecting benchmarks

Prerequisites

- For this work, the TACEO co-SNARK implementation will be used. Large parts of this implementation are written in Rust. Therefore, proficiency in Rust is beneficial.
- Background in cryptography is recommended
- Prior knowledge about zk-SNARK and/or MPC is beneficial but not a must
- Strong analytical and problem-solving skills, with a keen attention to detail
- Ability to work independently and conduct scientific experiments

References

- <https://eprint.iacr.org/2021/1530.pdf>
- <https://cs.stanford.edu/~aozdemir/docs/cozkSNARKs.pdf>
- <https://github.com/TaceoLabs/co-snarks>

Interested?

Then we look forward hearing from you!
Contact us via email including your CV and a transcript of records:

Veronika Bauer
Nina Schwanke

bav@net.in.tum.de
schwanke@net.in.tum.de