Verifiable Computing

Advisor(s): Sebastian Ramacher

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Verifiable computing has seen significant interest with the advent of cloud computing and outsourcing of resources. The basic idea is that a client outsources the computation of a particular function to an untrusted worker. Then, the client obtains the result and a proof from the worker that allows to privately/publicly verify the correctness of the result. Clearly, these concepts find broad application in the field of cloud computing.

The goal of this project is to get an overview of the sate-of-the-art in this field and to then use one of the existing frameworks to implement a use-case relevant for practical applications.

Goals and Tasks

- Get familiar with the required background
- Review the state-of-the-art
- Implement a use-case

March 8, 2004

Literature

- M. Walfish and A. J. Blumberg
  Verifying Computations without Reexecuting Them
  Commun. ACM 2015

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW ☒ TM

Prerequisites

- Java programming
- Interest in public key crypto

Advisor / Contact

sebastian.ramacher@iaik.tugraz.at