Transparency Systems with Succinct Proofs of Correctness

Advisor: **Edona Fasllija**

Motivation

Transparency systems are essential for ensuring account-ability, integrity, and trust in digital infrastructures. However, as these systems grow in complexity and scale, generating and verifying traditional proofs of correctness can become computationally expensive. This thesis focuses on the design and development of transparency systems that employ succinct proofs of correctness—cryptographic proofs that are short, easy to verify, and efficient to generate, even for large datasets or complex operations.

We explore cutting-edge techniques such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), STARKs, and polynomial commitments, integrating them into transparency systems to ensure that users can verify data correctness without needing to re-process the entire dataset. By leveraging these succinct proof systems, we demonstrate significant improvements in performance, scalability, and user verification efficiency. Through rigorous analysis and practical implementation, this thesis shows how succinct proofs can make transparency systems more efficient while preserving strong guarantees of security and correctness, enabling their application in areas like blockchain, digital certificates, and public auditing.

Goals and Tasks

- Get familiar with related literature and open-source implementations of Verifiable Data Structures (Google' Trillian, Meta's AKD)

- Design and implement succinct proofs of membership, consistency

- Evaluate the compatibility and accuracy of your solution

- Write down your findings

Literature

> I. Tzialla et al.
  Transparency dictionaries with succinct proofs of correct operation
  Cryptology ePrint Archive 2021

Courses & Deliverables

☑ **Master Project**
  Project code
  Report
  Presentation

– OR –

☑ **Master's Thesis**
  + DiplomandInnenseminar (CS)
  Initial presentation
  Project code
  Thesis (60+ pages)
  Final presentation

Recommended if you're studying

☑ CS   ☑ ICE   ☑ SEM

Prerequisites

> Interest in zkp

> Programming skills (Rust, Go)

Advisor Contact

edona.fasllija@tugraz.at