Survey on Lookup Arguments
Bachelor’s Thesis

Given a vector $v$ of elements, a lookup argument allows to efficiently prove that a hidden pair $(i, a)$ of index and element, e.g. an encrypted or committed element, corresponds to the vector component, i.e. that $a = v[i]$. Such arguments can be used in subprotocols and are especially useful for privacy-preserving protocols.

Scope of the work

The student is expected to write a survey on the state of the art in lookup argument and closely related primitives. The goals of the thesis are to

1. research the literature for lookup arguments;
2. classify and compare lookup arguments by security guarantees, hardness assumptions, model assumptions and use cases, efficiency, etc.;
3. compare and relate lookup proofs to related primitives, such as membership proofs.
4. New lookup arguments may be devised as part of thesis. However this is a strictly optional goal.

As a starting point and for some references for lookup arguments and related works, refer to [Zap+22]. To find open access and/or full versions of the cited papers, use [dblp] or some (academic) search engine.

Requirements

Following prior knowledge is helpful for, but can also be acquired while working on, the bachelor’s thesis:

- Basic knowledge of cryptography, in particular (non-interactive) commitment schemes and (non-interactive) zero-knowledge is helpful.
- Basic familiarity with group-based and pairing-based cryptography is advantageous.

Contact

In case of interest or for further information, please contact Michael Klooß, michael.klooss@kit.edu.

References