KASTEL: Cryptography and Security Group
Chair Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

1-out-of-2 equivocal commitments from generic assumptions

Bachelor's (or Master's) Thesis

A normal commitment scheme allows the committer to commit to a value v in such a way that the receiver (of the commitment) does not learn the value before it is unveiled (the **hiding** property), and yet, the committer is bound to a single value v and cannot unveil two different values $v' \neq v$ (the **binding** property). Commitments are an important building block in many cryptographic protocols, in particular for zero-knowledge proof systems. Oftentimes, commitments with special properties are required for advanced constructions. Namely, for constructions of so-called "stackable Σ-protocols", [Goe+22] one needs 1-out-of-2 equivocal commitments (or a different approach [BS24]).[1, 2] In a 1-out-of-2 equivocal commitment, the committer chooses a bit b and value v_b simultaneously. It opens the commitment to (v_0, v_1) where it is bound for v_b but can open v_{1-b} to any value (called **equivocation** of v_{1-b}).

Scope of the work

There are some generic ways to construct (1-out-of-2) commitment schemes, and the goal of this thesis is to find existing constructions in the literature, and devise new and improved constructions from generic assumptions. After researching the literature, the next goals of the thesis could be some of the following, assuming the questions are not fully answered in the literature already:

- Construct 1-out-of-2 equivocal commitment schemes from *one-way functions*.
- Construct *more efficient* 1-out-of-2 equivocal commitment schemes from assumption still in minicrypt (e.g. collision resistant hashes) or in the random oracle model.
- Investigate 1-out-of-n constructions, devise new applications, and so on...

Requirements

Following prior knowledge is helpful for the bachelor's thesis.

- Theoretical foundations of cryptography, provable security and security reductions is required or must be acquired.
- Good proficiency with basic probability theory will be helpful.

This topic might serve as a master's thesis, but additional material/depth will be required.

Contact

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

References

[Avi+24] Gennaro Avitabile, Vincenzo Botta, Daniele Friolo, Daniele Venturi, and Ivan Visconti. *Compact Proofs of Partial Knowledge for Overlapping CNF Formulae*. Cryptology ePrint Archive, Paper 2024/1488. 2024. DOI: 10.1007/s00145-024-09532-3. URL: https://eprint.iacr.org/2024/1488.

[BS24] Katharina Boudgoust and Mark Simkin. "The Power of NAPs: - Compressing OR-Proofs via Collision-Resistant Hashing". In: 2024, pp. 35–66. DOI: 10.1007/978-3-031-78011-0_2.

[Goe+22] Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and Gabriel Kaptchuk. "Stacking Sigmas: A Framework to Compose Σ-Protocols for Disjunctions". In: 2022, pp. 458–487. DOI: 10.1007/978-3-031-07085-3_16.

[1] In [Avi+24], a good overview of stackable Σ-protocols is given in the introduction.
[2] To find open access and full versions of the cited papers, use dblp or academic search engines.