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

1-out-of-2 equivocal commitments and stackable Σ-protocols

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

The goal of this thesis is to instantiate the framework of [Goe+22] more generically, more efficiently and/or from weaker assumptions. 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 goals of the thesis are the following, assuming the questions are not fully answered in the literature already:

- Understand the approach of [Goe+22] and the requirements on the 1-out-of-2 commitment schemes. In particular: Does it still work for *interactive* commitments? What flexibility can we afford at what cost?
- There are generic commitment scheme constructions, e.g. based on Σ-protocols [Lin15]. Investigate if these generalize to 1-out-of-2 commitments, and if constructions from one-way functions or collision resistance are possible.
- Investigate *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.
- Optional (and hard) question: Understanding (im)possibilities within minicrypt.

Requirements

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

- Theoretical foundations of cryptography, provable security and security reductions are essential.
- Good proficiency with basic probability theory will be helpful.
- Knowledge of Σ-protocols is very helpful, see [Dam10] or [BS23, Ch. 19].[1]
- Knowledge of cut-and-choose techniques and their analysis is 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.

[1] In [Avi+24], a good overview of stackable Σ-protocols is given in the introduction.
[2] Searching via dblp helps to find open access and full versions of published papers or vice versa.

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, Report 2024/1488. 2024. URL: https://eprint.iacr.org/2024/1488.

[BS23] Dan Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography*. 2023. URL: https://toc.cryptobook.us/.

[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.

[Dam10] Ivan Damgård. *On Σ-protocols*. 2010. URL: https://cs.au.dk/~ivan/Sigma.pdf.

[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.

[Lin15] Yehuda Lindell. "An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle". In: 2015, pp. 93–109. DOI: 10.1007/978-3-662-46494-6_5.