Karlsruhe Institute of Technology

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

Straightline extraction for succinct proof systems

Master's Thesis

Succinct proof systems (for NP languages) produce proofs which are shorter than the witness size. In many settings, one requires not just soundness—the guarantee that no false statement can be proven—but the stronger property of **knowledge soundness**. Intuitively, knowledge soundness asserts that any party that can produce a valid proof must "know" a witness. This is formalized through the existence of an extractor algorithm Ext, which given the code of an adversarial malicious prover and a statement with valid proof produced by the adversary, can efficiently output a witness for the statement. However, even knowledge soundness can be insufficient: If a party runs in an interactive protocol, it might not know the code (which includes any randomness and *secrets* of a party) of other parties it is interacting with. This motivates an even stronger property, called **straightline extractability (SLE)**, which roughly asserts that Ext can produce a witness given a valid proof and the interactions (i.e. messages sent and received) of a party (but not its code). Crucially, we can count evaluation of a random oracle as interaction (in the random oracle model (ROM)), and most succinct non-interactive argument of knowledge (SNARK) are constructed and analysed in the ROM anyway.

Straightline extractability is an important feature and required in many security reductions. For that reason, it has gathered more attention recently, e.g. [Kat21; Ks22; Gan+23; Chi+24; RT24; Che+24]. The recent work [Gan+23] presents a compiler which transforms any SNARK, not necessarily straightline extractable, into a straightline-extractable SNARK. Importantly, their compiler preserves the communication complexity. In particular, if the SNARK was $O_\lambda(\mathsf{poly}(\lambda, \log(n)))$, for security parameter λ and statement/witness size n, then the transformation preserves that.

Scope of this work

The topic of this thesis to revisit [Gan+23] and consider several aspects of it:

(1) As a warm-up, reconsider the setting:
   a) In the rough asymptotic sense that [Gan+23] considers, a simpler Merkle-tree-based approach seems feasible. Namely, $O_\lambda(1) = O_\lambda(\mathsf{poly}(\lambda))$ by definition of O_λ. Investigate whether or not this is true and what potential obstructions there are.
   b) Reconsider the transformations in a less coarse setting, i.e., consider the usual O-notation.

(2) The transformations considered in [Gan+23] assume a generic SNARK. The main goal of the thesis is to improve this by assuming additional properties of the SNARK. For example, can a more efficient transformation be constructed based on a commit-and-prove SNARKs?

(3) A further question is to understand the requirements on the baseline SNARK: Does it have to be knowledge sound, or is soundness already sufficient (for a modified transformation)?

(4) Optional: Investigate other approaches/own ideas for achieving efficient straightline extractability, or investigate extensions to straightline *simulation extractability*, an even security stronger requirement.

To simplify and streamline the setting, everything should be considered in the random oracle model.

Requirements

- Probability theory and analysis of algorithms is a core technical tool.
- Familiarity with SNARKs, basic construction paradigms, and their properties is helpful.[1]
- Familiarity with the random oracle model and cut-and-choose techniques is helpful. See e.g. [Fis05] for a well-known efficient transformation to achieve straightline extractability.

Contact

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

[1] Some books/notes focused on succinct arguments are [CY; Tah]. An outdated source of papers and links [ZKP].

References

[Che+24] Megan Chen, Pousali Dey, Chaya Ganesh, Pratyay Mukherjee, Pratik Sarkar, and Swagata Sasmal. *Universally Composable Non-Interactive Zero-Knowledge from Sigma Protocols via a New Straight-line Compiler.* Cryptology ePrint Archive, Paper 2024/1713. 2024. URL: `https://eprint.iacr.org/2024/1713`.

[Chi+24] Alessandro Chiesa, Ziyi Guan, Shahar Samocha, and Eylon Yogev. "Security Bounds for Proof-Carrying Data from Straightline Extractors". In: 2024, pp. 464–496. DOI: `10.1007/978-3-031-78017-2_16`.

[CY] Alessandro Chiesa and Eylon Yogev. *Building Cryptographic Proofs from Hash Functions.* URL: `https://snargsbook.org/`.

[Fis05] Marc Fischlin. "Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors". In: 2005, pp. 152–168. DOI: `10.1007/11535218_10`.

[Gan+23] Chaya Ganesh, Yashvanth Kondi, Claudio Orlandi, Mahak Pancholi, Akira Takahashi, and Daniel Tschudi. "Witness-Succinct Universally-Composable SNARKs". In: 2023, pp. 315–346. DOI: `10.1007/978-3-031-30617-4_11`.

[Kat21] Shuichi Katsumata. "A New Simple Technique to Bootstrap Various Lattice Zero-Knowledge Proofs to QROM Secure NIZKs". In: 2021, pp. 580–610. DOI: `10.1007/978-3-030-84245-1_20`.

[Ks22] Yashvanth Kondi and abhi shelat. "Improved Straight-Line Extraction in the Random Oracle Model with Applications to Signature Aggregation". In: 2022, pp. 279–309. DOI: `10.1007/978-3-031-22966-4_10`.

[RT24] Lior Rotem and Stefano Tessaro. *Straight-Line Knowledge Extraction for Multi-Round Protocols.* Cryptology ePrint Archive, Paper 2024/1724. 2024. URL: `https://eprint.iacr.org/2024/1724`.

[Tah] Justin Tahler. *Proofs, Arguments, and Zero-Knowledge.* URL: `https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.html`.

[ZKP] ZKP. *Zero-Knowledge Proofs [Outdated resource].* URL: `https://zkp.science/`.