Karlsruhe Institute of Technology

Institut für Theoretische Informatik
Lehrstuhl Prof. Dr. J. Müller-Quade
crypto.iti.kit.edu

Efficient extraction for argument systems

Master's Thesis

Bulletproofs [Bün+17] (and variations) are a popular proof system in the DLOG setting. It can prove so-called rank 1 constraint systems (R1CS), which easily encode arithmetic circuits. Roughly, one multiplication gate in a circuit translates to one constraint in R1CS.

The soundness of Bulletproofs is shown by proving extraction of a witness from any sufficiently successful (malicious) prover. Extraction process is a two step process, and follows [Boo+16]: First, a tree of accepting transcripts is generated. Second, an extraction algorithm can produce from an **valid** tree a witness.

The extraction procedure incurs a (large) computational overhead. The security reduction therefore significantly degrades the provable security. In a recent work of Jaeger und Tessaro [JT20], a precise analysis of the extraction technique is made. It shows that in the generic group model, only a small soundness guarantee remains even for moderately sized statements, where moderate size is $M = 2^{20} \approx 10^6$ multiplication gates. One main problem is that a tree of size M^2 is required to extract a core component, the **inner product argument**.

Such a degradation of security was previously observed in [HKR19], where a variation of Bulletproofs is presented. This variation relies on a different extraction strategy, called **short-circuit extraction**. The basic idea is, that only two cases can happen in **valid** tree of size M^2:

- Either, a subtree of size M suffices for successful extraction,
- or the DLOG assumption must be broken.

While [HKR19] cast their results in this context, a precise analysis of the soundness guarantees is left as an open problem. With the recent work of [JT20], this problem can be resolved.

Scope of this work

The student should apply and extend the techniques from [JT20] to [HKR19] and the short-circuit extraction presented there. After familiarising with the context,[1] the goals of the thesis are as follows.

(1) **Analyse** the **short-circuit** extraction technique in [HKR19] in the same setting as [JT20]. That is, compute a soundness guarantee in the generic group model for expected polynomial time extraction (against strict PPT provers).
(2) **Extend** the security proof to **expected** polynomial time (EPT) provers.
(3) Develop a **general formal model** (building on [JT20]) which captures short-circuit extraction, and prove suitably generalised theorems. Test the generality against similar extraction strategies, such as [Boo+20].
(4) Give an **improved tree-finding** algorithm. (Refer to [Wik18] and [Boo+20] for two constructions.)

The thesis starts with goal 1 and continues with 2. Then, it can move on with 3 and/or 4. The order is roughly in difficulty. Compared to a good answer for point 4, all others are warm-ups.

Requirements

- Probability theory and analysis of algorithms is a core technical tool.
- Familiarity with cryptography (e.g. suitable seminars) or willingness (and time) to review it. It will most likely be essential for non-trivial instantiations.

[1] Argument systems, HVZK, public coin, Sigma-protocols, special soundness, argument of knowledge, knowledge error, black-box extraction, witness-extended emulation, …

Contact

In case of interest or for further information, please contact Michael Klooß, `michael.klooss@kit.edu`. After an initial discussion, but before starting the thesis, interested students are required to write an exposé, detailing their course of action. This includes and serves for acquiring initial familiarity with the topic.

Literatur

[Boo+16] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth und Christophe Petit. “Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting”. In: *IACR Cryptol. ePrint Arch.* 2016 (2016), S. 263. URL: `http://eprint.iacr.org/2016/263`.

[Boo+20] Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen und Gregor Seiler. “A non-PCP Approach to Succinct Quantum-Safe Zero-Knowledge”. In: *IACR Cryptol. ePrint Arch.* 2020 (2020), S. 737. URL: `https://eprint.iacr.org/2020/737`.

[Bün+17] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille und Gregory Maxwell. “Bulletproofs: Short Proofs for Confidential Transactions and More”. In: *IACR Cryptol. ePrint Arch.* 2017 (2017), S. 1066. URL: `http://eprint.iacr.org/2017/1066`.

[HKR19] Max Hoffmann, Michael Klooß und Andy Rupp. “Efficient zero-knowledge arguments in the discrete log setting, revisited”. In: *IACR Cryptol. ePrint Arch.* 2019 (2019), S. 944. URL: `https://eprint.iacr.org/2019/944`.

[JT20] Joseph Jaeger und Stefano Tessaro. “Expected-Time Cryptography: Generic Techniques and Applications to Concrete Soundness”. In: *IACR Cryptol. ePrint Arch.* 2020 (2020), S. 258. URL: `https://eprint.iacr.org/2020/1213`.

[Wik18] Douglas Wikström. “Special Soundness Revisited”. In: *IACR Cryptol. ePrint Arch.* 2018 (2018), S. 1157. URL: `https://eprint.iacr.org/2018/1157`.