Compressed Σ-protocol theory

Attema, T.

Propositions

accompanying the dissertation

Compressed Σ-Protocol Theory

by Thomas Attema — Leiden, June 1, 2023

(i) At the cost of a logarithmic number of rounds, the communication complexity of many Σ-protocols can be compressed from linear down to logarithmic. However, already with a constant number of rounds a sublinear communication complexity can be achieved (Chapter 3).

(ii) Parallel repetition does not necessarily reduce the knowledge error in an argument of knowledge. However, for multi-round special-sound interactive arguments parallel repetition reduces the knowledge error at an exponential rate, which is optimal (Section 6.5).

(iii) The security loss incurred by applying the Fiat-Shamir transformation to multi-round special-sound interactive proofs and arguments does not depend on the number of rounds (Section 6.6).

(iv) The practical deployment of (zero-knowledge) proof systems, in a wide variety of application scenarios, has incentivized more fine-grained performance analyses. Not surprisingly, there is no single proof system (yet) that outperforms all others across the board (Chapter 1).

(v) Due to a generic reduction from NP statements to circuit satisfiability, a (zero-knowledge) proof system for arithmetic circuit satisfiability immediately implies a proof system for any NP language. However, even given the recent efficiency improvements, there often exist more efficient approaches, avoiding generic circuit techniques ([ACF21] and [ACR21] as referred to in Section 1.3).

(vi) For any prime-power cyclotomic number field, any integral basis that contains elements that are not roots of unity is suboptimal in that there exists an integral basis that is shorter and/or more orthogonal with respect to the canonical geometry ([ACX21] as referred to in Section 1.3).

(vii) The general design principle behind Pedersen's vector commitment scheme applies to many other homomorphic commitment schemes, turning them into vector commitment schemes as well, for which the size of a commitment is independent of the size of the committed vector ([ACC+22] as referred to in Section 1.3).

(viii) Certain approaches for detecting fraudulent monetary transactions can be captured efficiently by restricted multiplication straight-line (RMS) programs. Further, when restricting to RMS programs, secure multiparty computation based on (additively) homomorphic encryption can be significantly more efficient than secret-sharing based multiparty computation ([SHA+19] as referred to in Section 1.3).

(ix) An elegant technique allows a judoka to tackle strong opponents, demonstrating that elegance can outperform brute-force strategies. Likewise, in mathematics, elegance not only provides an aesthetic appeal, it is also a means for providing a deep understanding of mathematical problems and their solutions.

(x) Some of the most revolutionary technologies have emerged from fundamental research without concern for immediate applications. To safeguard the continuation of technological advancement, it is important that research institutes, even those focusing on applications, encourage curiosity driven research.