Ron Rothblum\textemdash\textit{The Technion}

Proving as Fast as Computing: Succinct Arguments with Constant Prover Overhead

Abstract:

Succinct arguments are proof systems that allow a powerful, but untrusted, prover to convince a weak verifier that an input $x$ belongs to a language $L \in \text{NP}$, with communication that is much shorter than the NP witness. Such arguments, which grew out of the theory literature, are now drawing immense interest also in practice, where a key bottleneck that has arisen is the high computational cost of proving correctness. In this work we address this problem by constructing succinct arguments for general computations, expressed as Boolean circuits (of bounded fan-in), with a strictly linear size prover. The soundness error of the protocol is an arbitrarily small constant. Prior to this work, succinct arguments were known with a quasi-linear size prover for general Boolean circuits or with linear-size only for arithmetic circuits, defined over large finite fields. Joint work Noga Ron-Zewi.