Scalable computational integrity and privacy, with applications to Bitcoin and Zerocash

Eli Ben Sasson, Technion

Abstract

It has been known since the late 1980's that multi-prover interactive proofs (MIPs) and probabilistically checkable proofs (PCPs) can be used to construct asymptotically efficient zero knowledge arguments of membership for any language in NEXP, with minimal communication complexity. Reducing this marvelous (asymptotic) theory to practice requires new models and techniques to deal with concrete, non-asymptotic, efficiency. This talk surveys our efforts over the past six years to analyze theoretically, and build practically, zero-knowledge proof systems that are concretely efficient, succinctly verifiable and which require only a short public random string for their setup. Applications to Bitcoin and Zerocash will be discussed as well.

Based on joint works with Iddo Ben-Tov, Alessandro Chiesa, Michael Forbes, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Ynon Horesh, Evgenya Pergament, Michael Riabzev, Mark Siberstein, Nicholas Spooner, Eran Tromer and Madars Virza.