Cryptology ePrint Archive: Report 2011/457

Resettable Statistical Zero Knowledge

Sanjam Garg, Rafail Ostrovsky, Ivan Visconti, Akshay Wadia

Abstract: Two central notions of Zero Knowledge that provide very strong, yet seemingly incomparable security guarantees against malicious verifiers are those of Statistical Zero Knowledge and Resettable Zero Knowledge. The current state of the art includes several feasibility and impossibility results about the two notions separately. However, the challenging question of achieving Resettable Statistical Zero Knowledge (i.e., Resettable Zero Knowledge and Statistical Zero Knowledge simultaneously) for non-trivial languages is still open. In this paper, we show:

- Resettable Statistical Zero Knowledge with efficient provers: Efficient-prover Resettable Sta-tistical Zero-Knowledge proof systems exist for all languages that admit hash proof systems (e.g., QNR, QR, DDH, DCR). Furthermore, for these languages, as an application of our technique, we also construct a two-round resettable statistical witness-indistinguishable argument system.

- Resettable Statistical Zero Knowledge with unbounded provers: Under the assumption that sub-exponentially hard one-way functions exist, rSZK = SZK. In other words, every language that admits a Statistical Zero-Knowledge (SZK) proof system also admits a Resettable Statistical Zero-Knowledge (rSZK) proof system. (Further, the result can be re-stated unconditionally provided there exists a sub-exponentially hard language in SZK). Moreover, under the assumption that (standard) one-way functions exist, all languages L such that the complement of L is random self reducible, admit a rSZK, in other words: co-RSR \subseteq rSZK. The round complexity of all our proof systems is O(log n), where n is the security parameter, and all our simulators are black-box.

Category / Keywords: Resettable zero-knowledge, statistical zero-knowledge, instance dependent primitives.

Date: received 21 Aug 2011, last revised 21 Aug 2011

Contact author: awadia at cs ucla edu