Cryptology ePrint Archive: Report 2011/404

A constant-round resettably-sound resettable zero-knowledge argument in the BPK model

Seiko Arita

Abstract: In resetting attacks against a proof system, a prover or a verifier is reset and enforced to use the same random tape on various inputs as many times as an adversary may want. Recent deployment of cloud computing gives these attacks a new importance. This paper shows that argument systems for any NP language that are both resettably-sound and resettable zero-knowledge are possible by a constant-round protocol in the BPK model. For that sake, we define and construct a resettably-extractable {\em conditional} commitment scheme.

Category / Keywords: foundations / Resettable zero-knowlege, Resettable sound

Date: received 28 Jul 2011

Contact author: arita at iisec ac jp

Available formats: PDF | BibTeX Citation

Version: 20110730:024628 (All versions of this report)

Discussion forum: Show discussion | Start new discussion