Cryptology ePrint Archive: Report 2013/010

Simultaneous Resettable WI from One-way Functions

Kai-Min Chung and Rafael Pass

Abstract: In this short note, we demonstrate that the existence of one-way functions implies the existence of an $\omega(1)$-round simultaneously resettable witness indistinguishable argument.

Category / Keywords: foundations / resettable security, witness indistinguishability, one-way functions, concurrent zero-knowledge

Date: received 7 Jan 2013, last revised 5 Feb 2013

Contact author: chung at cs cornell edu

Available formats: PDF | BibTeX Citation

Version: 20130205:205333 (All versions of this report)