Cryptology ePrint Archive: Report 2013/008

Non-Black-Box Simulation from One-Way Functions And Applications to Resettable Security

Kai-Min Chung and Rafael Pass and Karn Seth

Abstract: The simulation paradigm, introduced by Goldwasser, Micali and Rackoff, is of fundamental importance to modern cryptography. In a breakthrough work from 2001, Barak (FOCS'01) introduced a novel non-black-box simulation technique. This technique enabled the construction of new cryptographic primitives, such as resettably-sound zero-knowledge arguments, that cannot be proven secure using just black-box simulation techniques.

The work of Barak and its follow-ups, however, all require stronger cryptographic hardness assumptions than the minimal assumption of one-way functions: the work of Barak requires the existence of collision-resistant hash functions, and a very recent result by Bitansky and Paneth (FOCS'12) instead requires the existence of an Oblivious Transfer protocol.

In this work, we show how to perform non-black-box simulation assuming just the existence of one-way functions. In particular, we demonstrate the existence of a constant-round resettably-sound zero-knowledge argument based only on the existence of one-way functions. Using this technique, we determine necessary and sufficient assumptions for several other notions of resettable security of zero-knowledge proofs. An additional benefit of our approach is that it seemingly makes practical implementations of non-black-box zero-knowledge viable.

Category / Keywords: foundations / non-black-box simulations, resettable security, one-way functions, zero-knowledges

Date: received 6 Jan 2013, last revised 5 Feb 2013

Contact author: chung at cs cornell edu