Cryptology ePrint Archive: Report 2011/513

Non-Malleable Zero Knowledge: Black-Box Constructions and Definitional Relationships

Abhishek Jain and Omkant Pandey

Abstract: This paper deals with efficient non-malleable zero-knowledge proofs for NP, based on general assumptions. We construct a simulation-sound zero-knowledge protocol for NP, based only on the black-box use of one-way functions. Constructing such a proof system has been an open question ever since the original work of Dolev, Dwork, and Naor [DDN'91]. In addition to the feasibility result, our protocol has a constant number of rounds, which is asymptotically optimal.

Traditionally, the term non-malleable zero-knowledge (NMZK) refers to the original definition of Dolev et al. Today, it is used loosely to also refer to simulation-soundness (SIM-SOUND) [Sahai'99], and simulation-extractability (SIM-EXT) [PR'05]. While the common perception is that SIM-EXT is the strongest of the three notions (e.g., SIM-EXT is known to imply NMZK), a formal study of the definitional relationship between these notions has never been done.

In the second part of this work, we try to correct this situation by initiating such a study. We show that in the "static" case, if an NMZK protocol is also an argument-of-knowledge, then it is in fact SIM-EXT. Furthermore, in the most strict sense of the definition, SIM-SOUND does not necessarily follow from SIM-EXT. These results are somewhat surprising because they are opposite to the common perception that SIM-EXT is the strongest of the three notions.

Category / Keywords: foundations / Non-malleability, zero knowledge, commitments, black-box constructions

Date: received 17 Sep 2011

Contact author: abhishek at cs ucla edu

Available formats: PDF | BibTeX Citation

Version: 20110918:025745 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]