Cryptology ePrint Archive: Report 2011/507

Relatively-Sound NIZKs and Password-Based Key-Exchange

Charanjit Jutla and Arnab Roy

Abstract: We define a new notion of relatively-sound non-interactive zero-knowledge (NIZK) proofs, where a private verifier with access to a trapdoor continues to be sound even when the Adversary has access to simulated proofs and common reference strings. It is likely that this weaker notion of relative-soundness suffices in most applications which need simulation-soundness. We show that for certain languages which are diverse groups, and hence allow smooth projective hash functions, one can obtain more efficient single-theorem relatively-sound NIZKs as opposed to simulation-sound NIZKs. We also show that such relatively-sound NIZKs can be used to build rather efficient publicly-verifiable CCA2-encryption schemes.

By employing this new publicly-verifiable encryption scheme along with an associated smooth projective-hash, we show that a recent PAK-model single-round password-based key exchange protocol of Katz and Vaikuntanathan, Proc. TCC 2011, can be made much more efficient. We also show a new single round UC-secure password-based key exchange protocol with only a constant number of group elements as communication cost, whereas the previous single round UC-protocol required $\Omega(k) $ group elements, where k is the security parameter.

Category / Keywords:

Date: received 15 Sep 2011, last revised 3 Nov 2011

Contact author: csjutla at us ibm com

Note: 1. Alternate (weaker) Definition of Relatively-Sound NIZKs. 2. A stand-alone complete proof of the PAK protocol. 3. A reference to Groth, Asiacrypt 06.