Cryptology ePrint Archive: Report 2013/064

Lightweight Zero-Knowledge Proofs for Crypto-Computing Protocols

Sven Laur and Bingsheng Zhang

Abstract: Crypto-computing is a set of well-known techniques for computing with encrypted data. The security of the corresponding protocols are usually proven in the semi-honest model. In this work, we propose a new class of zero-knowledge proofs, which are tailored for crypto-computing protocols. First, these proofs directly employ properties of the underlying crypto systems and thus many facts have more concise proofs compared to generic solutions. Second, we show how to achieve universal composability in the trusted set-up model where all zero-knowledge proofs share the same system-wide parameters. Third, we de- rive a new protocol for multiplicative relations and show how to combine it with several crypto-computing frameworks to get security in the malicious model.

Category / Keywords: public-key cryptography / Universal composability, conditional disclosure of secrets, zero-knowledge proof, homomorphic encryption scheme, crypto-computing

Date: received 7 Feb 2013

Contact author: swen at math ut ee

Available formats: PDF | BibTeX Citation

Version: 20130212:094503 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]