Cryptology ePrint Archive: Report 2011/012

Minimizing Non-interactive Zero-Knowledge Proofs Using Fully Homomorphic Encryption

Jens Groth

Abstract: A non-interactive zero-knowledge proof can be used to demonstrate the truth of a statement without revealing anything else. It has been shown under standard cryptographic assumptions that non-interactive zero-knowledge proofs of membership exist for all languages in NP. However, known non-interactive zero-knowledge proofs of membership of NP-languages yield proofs that are larger than the corresponding membership witnesses.

We investigate the question of minimizing the communication overhead involved in making non-interactive zero-knowledge proofs and show that if fully homomorphic encryption exists then it is possible to minimize the size of non-interactive zero-knowledge proofs and get proofs that are of the same size as the witnesses.

Our technique is applicable to many types of non-interactive zero-knowledge proofs. We apply it to both standard non-interactive zero-knowledge proofs and to universally composable non-interactive zero-knowledge proofs. The technique can also be applied outside the realm of non-interactive zero-knowledge proofs, for instance to get witness-size interactive zero-knowledge proofs in the plain model without any setup.

Category / Keywords: foundations / Non-interactive zero-knowledge proofs, fully homomorphic encryption

Date: received 6 Jan 2011

Contact author: j groth at ucl ac uk

Available formats: PDF | BibTeX Citation

Version: 20110108:014956 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]