Efficient Zero-Knowledge Proofs

Jens Groth

UCL, London, UK

Abstract. A zero-knowledge proof is a two-party protocol that enables a prover to convince a verifier of the truth of a statement without revealing anything else. Zero-knowledge proofs are widely used in cryptography to guarantee that parties are acting correctly without revealing their private information.

Interestingly, it is possible to make highly efficient zero-knowledge proofs where the amount of communication is much smaller than the size of the statement. We will in this talk discuss practical communication-efficient zero-knowledge proofs.

A. Nitaj and D. Pointcheval (Eds.): AFRICACRYPT 2011, LNCS 6737, p. 379, 2011.