Cryptology ePrint Archive: Report 2011/060

A Group Signature Scheme from Lattice Assumptions

S. Dov Gordon and Jonathan Katz and Vinod Vaikuntanathan

Abstract: Group signature schemes allow users to sign messages on behalf of a group while (1) maintaining anonymity (within that group) with respect to an observer, yet (2) ensuring traceability of a signer (by the group manager) when needed. In this work we give the first construction of a group signature scheme based on lattices (more precisely, the learning with errors assumption), in the random oracle model. Toward our goal, we construct a new algorithm for sampling a random superlattice of a given modular lattice together with a short basis, that may be of independent interest.

Category / Keywords: public-key cryptography /

Date: received 1 Feb 2011, last revised 8 Feb 2011

Contact author: gordon at cs columbia edu