

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

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: A preliminary version of this work was published in Asiacrypt 2010. This version is different in many ways -- the notation has been cleaned up to make the exposition more readable, we give a much better analysis of the parameters involved in the scheme, and we fixed a small mistake in the main construction of Section 3.2.

Version: 20110208:170219 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]