Cryptology ePrint Archive: Report 2013/133

New Lattice Based Signature Using The Jordan Normal Form

Hemlata Nagesh and Birendra Kumar Sharma

Abstract: In this paper it is shown that the use of Jordan normal form instead of Hermite normal form would improve substantially the efficiency and the security of the lattice based signature scheme. In this scheme we also use a new hash function in such a way that the efficiency improved is obtain without decreasing the security of the function.

Category / Keywords: applications / Lattices; Jordan Normal Form;Digital Signature Scheme

Publication Info: the paper has not been published elsewhere.

Date: received 6 Mar 2013

Contact author: 5HEMLATA5 at gmail com