Cryptology ePrint Archive: Report 2011/328

Cryptanalysis of the Smart-Vercauteren and Gentry-Halevi's Fully Homomorphic Encryption

Gu Chunsheng

Abstract: In this paper, we first analyze the security of the fully homomorphic encryption schemes based on principal ideal lattice in [SV10, GH11] by using block lattice reduction algorithm. Our result implies that their schemes are insecure for lattice dimensions n=2048, and even for n=8192 if we suppose the random assumption and the geometric series assumption of [Sch03] for a lattice basis. If we suppose the average-case behavior of LLL in [NS06], then their schemes are also insecure for lattice dimension n less than 6000. Moreover, we further analyze how to find the small generator of a principal ideal lattice for the practical parameters in their schemes.

Category / Keywords: Fully Homomorphic Encryption, Cryptanalysis, Principal Ideal Lattice, Lattice Reduction

Date: received 14 Jun 2011, last revised 20 Jun 2011

Contact author: guchunsheng at gmail com