

Cryptology ePrint Archive: Report 2011/328

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

Gu Chunsheng

Abstract: For the fully homomorphic encryption schemes in [SV10, GH11], this paper presents attacks to solve equivalent secret key and directly recover plaintext from ciphertext for lattice dimensions $n=2048$ by using lattice reduction algorithm. According to the average-case behavior of LLL in [NS06], their schemes are also not secure for $n=8192$.

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

Date: received 14 Jun 2011, last revised 8 Jan 2012

Contact author: guchunsheng at gmail com

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

Version: 20120108:211650 ([All versions of this report](#))

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

[[Cryptology ePrint archive](#)]