Cryptology ePrint Archive: Report 2011/567

On the sparse subset sum problem from Gentry-Halevi's implementation of fully homomorphic encryption

Moon Sung Lee

Abstract: In Gentry's fully homoomrphic cryptosystem, a sparse subset sum problem is used and a big set is included in the public key. In the implementation of a variant of Gentry's scheme, to reduce the size of the public key, Gentry and Halevi used a specific form of a sparse subset sum problem with geometric progressions. In this note, we show that their sparse subset sum challenges are rather easy given the aggressive choice of parameters. Our experiment shows that even their large instance of a sparse subset sum problem could be solved within two days with probability of about 44%. A more conservative parameter choice can easily avoid our attack.

Category / Keywords: public-key cryptography / sparse subset sum, lattice reduction, dimension reduction method, geometric progression, homomorphic encryption

Date: received 20 Oct 2011

Contact author: mslee at nims re kr