Cryptology ePrint Archive: Report 2011/114

Fully Homomorphic Encryption, Approximate Lattice Problem and LWE

Gu Chunsheng

Abstract: In this paper, we first introduce a new concept of approximate lattice problem (ALP), which is an extension of learning with errors (LWE). Next, we propose two ALP-based public key encryption schemes. Then, we construct two new fully homomorphic encryption scheme (FHE) based on respectively approximate principal ideal lattice problem with related modulus (APIP-RM) and approximate lattice problem with related modulus (ALP-RM). Moreover, we also extend our ALP-RM-based FHE to the ALP problem with unrelated modulus (ALP-UM). Our work is different from previous works in three aspects: (1) We extend the LWE problem to the ALP problem. This ALP problem is similar to the closest vector problem in lattice. We believe that this problem is independent of interest. (2) We construct a new FHE by using a re-randomizing method, which is different from the squashing decryption in previous works. (3) The expansion rate is merely O(k) with k a security parameter in Our FHE, which can be improved to O(logk) by using dimension reduction [BV11], whereas all previous schemes are at least O (k*logk) [BV11, Gen11, LNV11]. Our method can also decrease a factor k of the expansion rate in their schemes.

Category / Keywords: Fully Homomorphic Encryption, Approximate Lattice Problem, Approximate Principal Ideal Lattice Problem, LWE, Approximate GCD, Integer Factoring

Date: received 7 Mar 2011, last revised 4 Jul 2011

Contact author: guchunsheng at gmail com