Cryptology ePrint Archive: Report 2011/118

New Fully Homomorphic Encryption over the Integers

Gu Chunsheng

Abstract: We first present a fully homomorphic encryption scheme over the integers, which modifies the fully homomorphic encryption scheme in [vDGHV10]. The security of our scheme is merely based on the hardness of finding an approximate-GCD problem over the integers, which is given a list of integers perturbed by the small error noises, removing the assumption of the sparse subset sum problem in the origin scheme [vDGHV10]. Then, we construct a new fully homomorphic encryption scheme, which extends the above scheme from approximate GCD over the ring of integers to approximate principal ideal lattice over the polynomial integer ring. The security of our scheme depends on the hardness of the decisional approximate principle ideal lattice polynomial (APIP), given a list of approximate multiples of a principal ideal lattice. At the same time, we also provide APIP-based fully homomorphic encryption by introducing the sparse subset sum problem. Finally, we design a new fully homomorphic encryption scheme, whose security is based on the hardness assumption of approximate lattice problem and the decisional SSSP.

Category / Keywords: Fully Homomorphic Encryption, Approximate Lattice Problem, Approximate Principal Ideal Lattice, Approximate GCD, BDDP, SSSP

Date: received 9 Mar 2011, last revised 8 Jul 2011

Contact author: guchunsheng at gmail com