The Efficiency of Embedding-Based Attacks on the GGH Lattice-Based Cryptosystem

ABSTRACT

The Goldreich-Goldwasser-Halevi (GGH) cryptosystem is declared broken due to the modified versions of the embedding attacks, known as Nguyen's σ, Nguyen's 2σ and Lee-Hahn's attacks. Despite using the same approach as the original embedding attack, these attacks deployed different strategies and resulted in different performances for breaking the GGH cryptosystem. In this paper, we described those strategies in detail. Moreover, we investigated the mathematical factors behind these attacks' ability and performance discrepancies. Mathematical proof examines and discusses the factors that triggered those variances. As a result, the expected lattice gap and implemented lattice dimensions are mathematically proven as the factors that significantly influenced these attacks' performance. By demonstrating how the attacks manipulated these factors, any lattice-based cryptosystem that relies on the hardness of the CVP could avoid repeating the same slipup as the GGH. Hence, precautionary action could be proactively taken to prevent it from being threatened by embedding-based attacks.