# A security upgrade on the GGH lattice-based cryptosystem


## ABSTRACT

Due to the Nguyen's attack, the Goldreich-Goldwasser-Halevi (GGH) encryption scheme, simply referred to as GGH cryptosystem, is considered broken. The GGH cryptosystem was initially addressed as the first practical latticebased cryptosystem. Once the cryptosystem is implemented in a lattice dimension of 300 and above, its inventors was conjectured that the cryptosystem is intractable. This conjecture was based on thorough security analyses on the cryptosystem against some powerful attacks. This conjecture became more concrete when all initial efforts for decrypting the published GGH Internet Challenges were failed. However, a novel strategy by the Nguyen's attack for simplifying the underlying Closest-Vector Problem (CVP) instance that arose from the cryptosystem, had successfully decrypted almost all the challenges and eventually made the cryptosystem being considered broken. Therefore, the Nguyen's attack is considered as a fatal attack on the GGH cryptosystem. In this paper, we proposed a countermeasure to combat the Nguyen's attack. By implementing the proposed countermeasure, we proved that the simplification of the underlying CVP instance could be prevented. We also proved that, the upgraded GGH cryptosystem remains practical where the decryption could be done without error. We are optimistic that, the upgraded GGH cryptosystem could make a remarkable return into the mainstream discussion of the lattice-based cryptography.