Security Threats and Upgrades on The Ggh Lattice-Based Encrption Scheme

Arif Mandangan
Universiti Malaysia Sabah, Malaysia

Abstract:

Current interest in cryptography is moving towards new arena known as Post-Quantum Cryptography to find alternatives for replacing number theoretical-based cryptosystems. One of the highly potential alternatives is lattice-based cryptography. In this talk, the first practical lattice-based encryption scheme known as the Goldreich-Goldwasser-Halevi (GGH) cryptosystem is discussed. This talk is divided into three parts. The first part covers some foundation aspects such as the trapdoor one-way function, key generation, encryption and decryption algorithms of the GGH cryptosystem. After rigorous security analysis on the scheme, its inventors conjectured that the Closest-Vector Problem underlying the GGH cryptosystem (GGH-CVP) is invulnerable once the cryptosystem is implemented in lattice dimensions beyond 300. However, major flaw in its design has made the simplification of the GGH-CVP possible. Thus, the second part of this talk emphasises the security aspect of the GGH cryptosystem where the exploited flaw as well as the powerful attacks on the scheme are discussed. Nguyen's embedding attack is considered as fatal attack on the GGH cryptosystem. By making the GGH cryptosystem survives against this attack, there is hope for the cryptosystem to make remarkable return into mainstream discussion in lattice-based cryptography. Therefore, two strategies for upgrading the security of the GGH cryptosystem are proposed and discussed in the final part of this talk. By deploying the strategies, the underlying GGH-CVP could be maintained in its original form so that the Nguyen's embedding attacks could be prevented and the GGH cryptosystem could potentially survive.