Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

An Upgrade on the Key Generation Algorithm of the GGH-MKA Lattice-Based Encryption Scheme

Mandangan, A.[1], Kamarulhaili, H.[2], and Asbullah, M. A. *[3]

[1]*Mathematics, Real-Time Graphics and Visualization Laboratory, Faculty of Sciences and Natural Resources, Universiti Malaysia Sabah, Malaysia*
[2]*School of Mathematical Sciences, Universiti Sains Malaysia, Malaysia*
[3]*Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia*
[3]*Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, Malaysia*

E-mail: ma_asyraf@upm.edu.my
* *Corresponding author*

Received: 30 June 2021
Accepted: 8 October 2021

Abstract

This paper presents an upgrade on the key generation algorithm of a current variant of the Goldreich-Goldwasser-Halevi lattice-based encryption scheme, referred to as the GGH-MKA cryptosystem. The keys for this cryptosystem consisting of lattice bases where the private key is required to be a 'good' basis while the public key is required to be a 'bad' basis to ensure the cryptosystem works effectively. In the key generation algorithm of the GGH cryptosystem, the good and bad features of the lattice bases are measured by computing orthogonality-defect value. If the value is 'close to 1', the basis is considered as a good basis. On the contrary, the basis is considered as a bad basis if its orthogonality-defect value is 'far from 1'. Clearly, the consideration on various subjective terms could potentially trigger technical error during the key generation processes. In this paper, we proposed new conditions on the private and public bases of the GGH-MKA cryptosystem. Instead of depending solely on the orthogonality-defect values, the proposed conditions could make the measurement of good and bad bases in the key generation algorithm of the GGH-MKA cryptosystem becomes clearer and deterministic.

Keywords: closest-vector problem; smallest-basis problem; lattice; good basis; bad basis; GGH cryptosystem; lattice-based cryptography.