Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984

A New Countermeasure to Combat the Embedding-Based Attacks on the Goldreich-Goldwasser-Halevi Lattice-Based Cryptosystem

Arif Mandangan[1,*], Nazreen Syazwina Nazaruddin[2], Muhammad Asyraf Asbullah[3,4], Hailiza Kamarulhaili[5], Che Haziqah Che Hussin[6], Babarinsa Olayiwola[7]

[1] Mathematics Visualization Research Group (MathVis), Faculty of Sciences and Natural Resources, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia
[2] Computational and Theoretical Sciences, Kulliyyah of Science, International Islamic University Malaysia, 25200 Kuantan, Pahang, Malaysia
[3] Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Sciences, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
[4] Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
[5] School of Mathematical Sciences, Universiti Sains Malaysia, 11800 USM Penang, Pulau Pinang, Malaysia
[6] Preparatory Centre for Science and Technology, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia
[7] Department of Mathematics, Federal University Lokoja, P.M.B 1154, Kogi State, Nigeria

ARTICLE INFO

Article history:
Received 2 March 2024
Received in revised form 8 October 2024
Accepted 11 November 2024
Available online 30 November 2024

Keywords:
GGH cryptosystem; lattice-based cryptography; post-quantum cryptography; embedding-based attacks

ABSTRACT

Despite being considered the first practical lattice-based cryptosystem, interest from the post-quantum cryptography society in the Goldreich-Goldwasser-Halevi (GGH) lattice-based cryptosystem drastically drop due to the embedding-based attacks. The attacks successfully simplified the underlying Closest-Vector Problem (CVP) and made the security of the scheme broken. The attacks become noxious to the GGH cryptosystem due to its ability to simplify the underlying CVP which triggered the enlargement of lattice gaps. Consequently, the simplified CVP can be reduced to a Shortest-Vector Problem (SVP) variant which can be solved by using lattice-reduction algorithms such as the LLL algorithm in a shorter amount of time. The simpler way to evade from these attacks is by implementing larger lattice dimensions which immediately reduce the efficiency of this scheme. Recently, an improved version of the GGH cryptosystem, namely the GGH-MKA cryptosystem, has been proven immune to the embedding-based attacks. The improvement is made by preventing the simplification of the underlying CVP. For that purpose, an error vector $\vec{e}'$ is introduced. The error vector is non-eliminable and at the same time maintains the lattice gap. Consequently, the underlying CVP remains in its original form without being simplified. In this study, we showed that the error vector $\vec{e}'$ is not unique. We proposed another error vector $\vec{e}^*$ to combat the embedding-based attacks. We proved that the new error vector $\vec{e}^*$ has similar capabilities in terms of preventing the simplification of the underlying CVP and maintaining the lattice gap. By improving the security of the GGH cryptosystem, more interest from the mainstream post-quantum discussion could be redirected to the scheme to make it competent and relevant again.

* *Corresponding author.*
E-mail address: arifman@ums.edu.my

https://doi.org/10.37934/ard.122.1.173183

1. Introduction

Cryptography becomes crucial in our today's lifestyle since most of our data are currently created, stored, managed, and communicated digitally. That is why security goals are demanded to provide confidentiality, integrity, and availability to our data [1,2]. To accomplish all these goals, cryptography face numerous challenges, obstacles, and threats in the form of cryptanalysis. The situation become more difficult due to the emergence of new computing technology. The term 'quantum' received overwhelming attention in various aspects of discussion including computing technology. This is due to the current development of quantum computing technology that works based on qubits rather than binary bits as deployed by our widely used computers today. This technology offers computational power with extreme efficiency. Once a fully functional quantum computers available to public, then most of the currently deployed cryptosystems underneath our devices might be in fatal danger. This is due to the ability to of Shor's quantum algorithm [3] for solving hard-mathematical problems underlying these cryptosystems in much shorter amounts of time. Consequently, all cryptosystems that lie their security on these problems are considered broken [4].

That is why mainstream discussion in cryptography is currently diverting towards new arena called post-quantum cryptography. The mission is to find cryptographic alternatives which are immune towards the quantum attacks with hope that these alternatives could be deployed whenever a fully functional quantum computers are ready to operate. The mission is still in progress. Various schemes have been proposed [5-10]. To build confidence and trust on these schemes, exhaustive security measures are demanded. Other than security, the aspects of efficiency and practicality also equivalently vital and become the foremost concerns in this mission [11-13].

In the early of its emergence, the Goldreich-Goldwasser-Halevi cryptosystem [14] or simply referred to as GGH cryptosystem once being considered the first practical lattice-based scheme. Unfortunately, Nguyen [15] discovered a significant flaw on the GGH cryptosystem and launched embedding-based attacks which allowed simplification of the underlying Closest-Vector Problem (CVP), defined as GGH-CVP [16]. The simplified version is then being reduced to an easier Closest-Vector Problem (CVP), defined as GGH-SVP [17]. It becomes easier due to the enlargement of lattice gap which allows lattice-reduction algorithms work much efficient for solving the derived GGH-SVP even in lattice dimensions up to 400. Increasing the lattice dimensions could avoid the attacks but the trade-off is the efficiency and practicality of the scheme. Since the devastating attack by Nguyen, interest on the GGH cryptosystem drastically dropped. Other lattice-based scheme received overwhelming attention and leave the GGH cryptosystem far away behind.

In 2020, Mandangan *et al.,* [18] invented the cure which make the GGH cryptosystem to survive against the embedding-based attacks. The upgraded version is called GGH-MKA cryptosystem. The countermeasure is done by introducing a new error vector $\vec{e}'$ and its elements distribution rule to replace the original error vector $\vec{e}$. Simplification of the underlying GGH-CVP was possible since the original error vector $\vec{e}$ is replaceable by a smaller error vector $\vec{\varepsilon}$. Consequently, the lattice gap becomes larger, and this allows efficient performance by lattice reduction algorithm to solve the derived GGH-SVP. On contrast, the newly introduced error vector $\vec{e}'$ is non eliminable and non-replaceable by the smaller error vector $\vec{\varepsilon}$. That means, the underlying GGH-CVP remain in its original form and the enlargement of lattice gap also has been prevented.

In this study, we demonstrate that the error vector $\vec{e}'$ and its elements distribution rule as introduced by the GGH-MKA cryptosystem are not unique. We discovered a new error vector $\vec{e}^*$ together with its elements' distribution rule. We prove that the simplification of the GGH-CVP as well as the lattice gap enlargement also could be prevented. Therefore, the proposed set and its

distribution rule could be deployed as a new countermeasure to combat the Nguyen's embedding attacks, as done in the GGH-MKA cryptosystem.

The rest of this paper is organized as follows. In Section 2, we provide some mathematical foundation related to lattices. Then, few works related to the security of GGH cryptosystem are discussed in the next section. The proposed countermeasure is discussed and justified in Section 4. Finally, discussion and conclusion remark are provided in Section 5.

2. Lattices

Lattice $\mathcal{L}$ is a set of vectors. These vectors could be generated by different bases. When it is generated by basis B, the lattice $\mathcal{L}$ is denoted as $L(B)$, i.e. $L(B) = \mathcal{L}$. The lattice $\mathcal{L}$ is defined as follows.

Definition 1: For $m \geq n$, *let* $B = \{\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n\}$ be a set of linearly independent vectors $\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n \in \mathbb{R}^m$. The lattice $\mathcal{L} \subset \mathbb{R}^m$ that is generated by the set B is the set of all linear combinations of the vectors $\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n$ with integer scalars, i.e. (Figure 1) [19].

$$\mathcal{L} = L(B) = \left\{ \sum_{i=1}^{n} a_i \vec{b}_i \middle| \, \vec{b}_i \in B \; and \; a_i \in \mathbb{Z}, \forall \; i = 1, \dots, n \right\} \tag{1}$$

The set B is called a lattice basis or simply basis. It is a set of linearly independent vectors that spans the entire vectors in the lattice $\mathcal{L}$. For the lattice $L(B)$ as defined in the Definition 1, the dimension is $\dim\big(L(B)\big) = n$ and the rank is $\mathrm{rank}\big(L(B)\big) = m$. If $\dim(\mathcal{L}) = \mathrm{rank}(\mathcal{L})$, then the lattice $\mathcal{L}$ is referred to as a full-rank lattice.

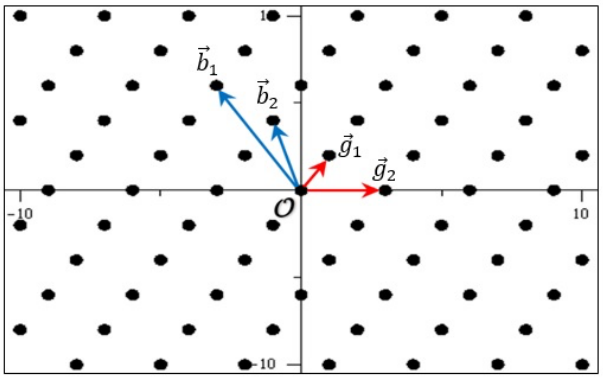

Fig. 1. The lattice $\mathcal{L} \subset \mathbb{R}^2$ with bases $B = \{\vec{b}_1, \vec{b}_2\}$ and $G = \{\vec{g}_1, \vec{g}_2\}$

Consider a full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ that is spanned by the basis $B = \{\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n\}$ where $\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n \in \mathbb{R}^n$. Since $B \in \mathbb{R}^{n \times n}$, then the lattice $\mathcal{L}$ is representable in the following simpler form, $\mathcal{L} = L(B) = \{B\vec{a} \mid \vec{a} \in \mathbb{Z}^n\}$. For $n \geq 2$, the n-dimensional lattice $\mathcal{L}$ has more than a single basis. Any two different bases for the lattice $\mathcal{L}$ are mathematically related by a unimodular matrix $U \in \mathbb{Z}^{n \times n}$.

Definition 2: Let $U \in \mathbb{Z}^{n \times n}$. If $\det(U) = \pm 1$, then U is a unimodular matrix. Since $\det(U) \neq 0$, this implies that the inverse U^{-1} exists and it is a unimodular matrix as well, where $U^{-1} \in \mathbb{Z}^{n \times n}$ and $\det(U^{-1}) = \pm 1$ [20].

Lemma 1: Let $G, B \in \mathbb{R}^{n \times n}$ be non-singular matrices and $U \in \mathbb{Z}^{n \times n}$ be a unimodular matrix. The matrices G and B span the same lattice $\mathcal{L} \subset \mathbb{R}^n$, i.e., $L(G) = L(B) = \mathcal{L} \subset \mathbb{R}^n$, if and only if these matrices are related as $G = BU$ [19]. For $n \geq 2$, there are infinitely many unimodular matrix U. This

implies that, there are infinitely many bases for the lattice $\mathcal{L}$. These bases have different quality in terms of the norms and orthogonality of their basis vectors. A basis with shorter and more orthogonal vectors is referred to as a 'good' basis while a 'bad' basis is a basis with longer and less orthogonal vectors. Both good and bad bases are essential in cryptography where a bad basis is normally used as public key while the good basis is used as private key. Lattice bases are used to define lattice-based problems.

Definition 3: Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice. Given a basis for the lattice $\mathcal{L}$ and a target vector $\vec{t} \in \mathbb{R}^n$, the Closest-Vector Problem *(CVP)* is to find a non-zero vector $\vec{v} \in \mathcal{L}$ that minimizes the distance $\left\|\vec{t} - \vec{v}\right\|$ [19].

Definition 4: Let $\mathcal{L} \subset \mathbb{R}^n$ *be a lattice. Given a basis for the lattice* $\mathcal{L}$*, the Shortest-Vector Problem (SVP) is to find a non-zero vector* $\vec{x} \in \mathcal{L}$ *such that* $\|\vec{x}\|$ *is minimal, i.e.,* $\|\vec{x}\| = \lambda_1(\mathcal{L})$ [19]. The CVP is proven to be NP-hard while the SVP is NP-hard under randomized reduction [19]. In [21], the CVP is proven to be a little bit harder than the SVP. The hardness of these problems is significantly influenced by various factors. One of the factors is lattice gap as defined below.

Definition 5: Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice and $\lambda_1(\mathcal{L}), \lambda_2(\mathcal{L}) \in \mathbb{R}^+$ denote the first and second minima of the lattice $\mathcal{L}$ respectively. The lattice gap of the lattice $\mathcal{L}$ is the ratio between the $\lambda_2(\mathcal{L})$ and the $\lambda_1(\mathcal{L})$, i.e. [15].

$$gap(\mathcal{L}) = \frac{\lambda_2(\mathcal{L})}{\lambda_1(\mathcal{L})} \in \mathbb{R}^+ \tag{2}$$

Experimentally, the larger the lattice gap is, the more efficient lattice-reduction algorithm could perform to solve the lattice problems [15]. For congruence relation between vectors, consider the following definition.

Definition 6: For $n, \sigma \in \mathbb{N}$, let $\vec{a}, \vec{b} \in \mathbb{Z}^n$. Then $\vec{a} \equiv \vec{b}(mod\ \sigma)$ holds if:

$$\frac{\vec{a}-\vec{b}}{\sigma} = \vec{k} \in \mathbb{Z}^n \tag{3}$$

3. Security of the GGH Cryptosystem

3.1 Embedding-Based Attacks

Through extensive security measures, inventors of the GGH cryptosystem conjectured that the underlying GGH-CVP of the GGH scheme are intractable in lattice dimensions of more than 300. The GGH-CVP can be solved or approximated using embedding-based attacks. The attack works by reducing the underlying GGH-CVP to the GGH-SVP. The derived GGH-SVP is then solved by using lattice-reduction algorithm and the obtained solution is containing the demanded solution of the GGH-CVP which immediately break the GGH cryptosystem.

Security threat by the embedding-based attacks already being realised by the inventors of the GGH cryptosystem. That is why they launch the attack to the GGH cryptosystem in their security measures [14]. By using LLL algorithm for solving the derived GGH-SVP, the attack only managed to break the GGH cryptosystem in 120 lattice dimensions. Later, Schnorr et al replaced the LLL algorithm by the BKZ algorithm [22] and the attack managed to break the GGH cryptosystem in 150 lattice dimensions. Using the same strategy, Nguyen launched another embedding-based attack [15]. This time the underlying GGH-SVP is solved by using pruning algorithm and the attack managed to reach 200 lattice dimensions after being executed in few days. Note that, all these attacks used the same strategy. The only difference was the lattice-reduction algorithm being deployed to solve the derived GGH-SVP.

3.2 Improved Embedding-Based Attacks

Nguyen discovered that the underlying GGH-CVP as well as the derived GGH-SVP are hard to solved in their original form. That is why GGH cryptosystem in practical lattice dimensions up to 400 dimensions remain secure at those time. The breakthrough happened when Nguyen discovered a major flaw regarding the error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$, where $n, \sigma \in \mathbb{N}$. The vector can be eliminated from the encryption equation and this allowed the simplification of the underlying GGH-CVP as well the GGH-SVP.

The simplification occurred due a major flaw in the design of the GGH cryptosystem. The encryption equation is as follows.

$$\vec{c} = B\vec{m} + \vec{e} \tag{4}$$

where $\vec{c} \in \mathbb{R}^n$ is a ciphertext, $B \in \mathbb{R}^{n\times n}$ is a lattice basis, $\vec{m} \in \mathbb{Z}^n$ is a plaintext and $\vec{e} \in \{-\sigma, +\sigma\}^n$ is an error vector. Since B is a basis for the lattice $\mathcal{L}$ and $\vec{m} \in \mathbb{Z}^n$, then $B\vec{m} = \vec{v} \in \mathcal{L}$ is a lattice vector. Thus, Eq. (4) can be rewritten as follows.

$$\vec{c} = \vec{v} + \vec{e} \tag{5}$$

The error vector $\vec{e}$ is added to the lattice vector $\vec{v}$ and yields a non-lattice vector $\vec{c}$. The GGH cryptosystem is constructed in such a way that $\vec{v}$ is the lattice vector that is located closest to the ciphertext $\vec{c}$. This implies that, the distance $\|\vec{c} - \vec{v}\|$ as well as the norm $\|\vec{e}\|$ are considered minimum.

Definition 7: For $n \in \mathbb{N}$, let $\vec{c} = \vec{v} + \vec{e}$ *where* $\vec{c} \in \mathbb{R}^n$ is a ciphertext, $\vec{v} \in \mathcal{L}$ is a lattice vector and $\vec{e} \in \mathbb{R}^n$ is an error vector. The Euclidean distance $\|\vec{c} - \vec{v}\|$ is defined as the *GGH-CVP* distance. As proved in [15], the GGH-CVP distance $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$. A task to find the lattice vector $\vec{v}$ in Eq. [5] is a variant of the CVP, defined as the GGH-CVP.

Definition 8: *(GGH-C*VP) For $n, \sigma \in \mathbb{N}$, *let* $B \in \mathbb{R}^{n\times n}$ be a basis for a lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$ and $\vec{c} = \vec{v} + \vec{e}$ be a ciphertext vector where $\vec{v} \in \mathcal{L}$ is a lattice vector and $\vec{e} \in \{-\sigma, +\sigma\}^n$ is an error vector. Given $B, \vec{c}$ *and* σ, find the lattice vector $\vec{v}$ such that $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$ [17]. Once the GGH-CVP distance is shorter than $\sigma\sqrt{n}$, the lattice gap in the embedded lattice $\mathcal{L}' \subset \mathbb{R}^{n+1}$ becomes larger. Consequently, the Nguyen's embedding attacks could perform better for solving the GGH-SVP which immediately solve the GGH-CVP as well. Details of the embedding based attack are explained in [17]. The distance become shorter since the error vector $\vec{e}$ is eliminable from the encryption Eq. (4) To do so, Nguyen used public parameters $n, \sigma \in \mathbb{N}$ to form an integer vector $\vec{s} \in \{\sigma\}^n$ and then inserted it into the encryption Eq. (4) as follows.

$$\vec{c} + \vec{s} = B\vec{m} + \vec{e} + \vec{s} \tag{6}$$

Note that, the following equation hold.

$$\frac{\vec{c}+\vec{s}-B\vec{m}}{2\sigma} = \frac{\vec{e}+\vec{s}}{2\sigma} \tag{7}$$

Since $\vec{e} \in \{-\sigma, +\sigma\}^n$ and $\vec{s} \in \{\sigma\}^n$, then $\vec{e} + \vec{s} \in \{0, 2\sigma\}^n$. Thus,

$$\frac{\vec{e}+\vec{s}}{2\sigma} \in \{0, 1\}^n \tag{8}$$

is an integer vector. Eq. (7) implies that,

$$\frac{\vec{c}+\vec{s}-B\vec{m}}{2\sigma} \in \mathbb{Z}^n \tag{9}$$

as well and this allows the following congruence holds.

$$\vec{c}+\vec{s} \equiv B\vec{m}\ (mod\ 2\sigma) \tag{10}$$

Clearly, the error vector $\vec{e}$ has been successfully eliminated from the encryption Eq. (4). The encryption Eq. (4) which originally has two unknown vectors $\vec{m}$ and $\vec{e}$ has been transformed to the congruence Eq. (10) which contain only a single unknown vector $\vec{m}$. Nguyen proved that the congruences Eq. (10) is solvable with very few solutions [15]. With non-negligible probability, these congruences has a single solution when $\gcd(|\det(B)|, \sigma) = 1$ and $\gcd(|\det(B)|, 2\sigma) = 1$. Thus, assume that the solutions of the congruence Eq. (10) are obtained as the following.

$$\vec{m} \equiv B^{-1}(\vec{c}+\vec{s})(mod\ 2\sigma) \tag{11}$$

Denote the solution as $B^{-1}(\vec{c}+\vec{s})\ mod\ 2\sigma = \vec{m}_{2\sigma}$ where $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^n$. Although $\vec{m} \neq \vec{m}_{2\sigma}$, the vector $\vec{m}_{2\sigma}$ is considered as partially decrypted plaintext since,

$$\vec{m} \equiv \vec{m}_{2\sigma}(mod\ 2\sigma). \tag{12}$$

Once the vector $\vec{m}_{2\sigma}$ is obtained, the GGH-CVP can be simplified. The vectors $\vec{m}_{2\sigma}$ is multiplied with the public basis B. The product vector $B\vec{m}_{2\sigma} \in \mathbb{R}^n$ is inserted into both sides of encryption Eq. (4) as follows.

$$\vec{c} - B\vec{m}_{2\sigma} = B(\vec{m} - \vec{m}_{2\sigma}) + \vec{e} \tag{13}$$

By Definition 6, the congruences is representable as follows.

$$\vec{m} - \vec{m}_{2\sigma} = 2\sigma\vec{k} \tag{14}$$

for $\vec{k} \in \mathbb{Z}^n$. Substituting Eq. (14) into Eq. (13) yields the following equation.

$$\vec{c} - B\vec{m}_{2\sigma} = B2\sigma\vec{k} + \vec{e} \tag{15}$$

$$\frac{\vec{c}-B\vec{m}_{2\sigma}}{2\sigma} = B\vec{k} + \frac{\vec{e}}{2\sigma} \tag{16}$$

For simplicity, denote $\frac{\vec{c}-B\vec{m}_{2\sigma}}{2\sigma} = \vec{p} \in \mathbb{R}^n$. Since $\vec{c}, B, \vec{m}_{2\sigma}$ and σ are known information, then $\vec{p}$ is known vectors. Note that, B is a basis for the lattice $L(B) \subset \mathbb{R}^n$ and $\vec{k} \in \mathbb{Z}^n$. By Definition 1, $B\vec{k} = \vec{q} \in L(B)$ which means that $\vec{q} \in \mathcal{L}$. Since $\vec{k}$ is an unknown vector, then $\vec{q}$ is also an unknown lattice vector. Although the value of the parameter σ is known, the arrangement of the entries $-\sigma$ and $+\sigma$ in the error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$ is privately determined. Thus, the following is an unknown vector.

$$\vec{\varepsilon} = \frac{\vec{e}}{2\sigma} \in \left\{-\frac{\sigma}{2\sigma}, +\frac{\sigma}{2\sigma}\right\}^n = \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n \tag{17}$$

Now, Eq. (16) can be simply rewritten as:

$$\vec{p} = \vec{q} + \vec{\varepsilon} \tag{18}$$

where $\vec{p} \in \mathbb{R}^n, \vec{q} \in L(B)$, and $\vec{\varepsilon} \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$. Note that, Eq. (18) is similar to Eq. (4) where the distance $\|\vec{p} - \vec{q}\|$ is analogue to the distance of $\|\vec{c} - \vec{v}\|$ in GGH-CVP. Recall that $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$. But the Nguyen's attack made $\|\vec{p} - \vec{q}\| < \|\vec{c} - \vec{v}\|$ as proven below.

Proposition 1: For $n, \sigma \in \mathbb{N}$ where $\mathrm{n}, \sigma > 1$, *let* $B \in \mathbb{R}^{n \times n}$ be a basis for the lattice $L(B) \subset \mathbb{R}^n$, $\vec{p} \in \mathbb{R}^n$ such that $\vec{p} = \vec{q} + \vec{\varepsilon}$ where $\vec{q} \in L(B)$. *If* $\vec{\varepsilon} \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$, then $\|\vec{p} - \vec{q}\| < \sigma\sqrt{n}$. Proof, since $\vec{p} = \vec{q} + \vec{\varepsilon}$, then $\|\vec{p} - \vec{q}\| = \|\vec{\varepsilon}\|$. Note that,

$$\|\vec{\varepsilon}\| = \sqrt{\underbrace{\left(\pm\frac{1}{2}\right)^2 + \left(\pm\frac{1}{2}\right)^2 + \cdots + \left(\pm\frac{1}{2}\right)^2}_{\text{added } n \text{ times}}} = \sqrt{n\left(\frac{1}{4}\right)} = \frac{\sqrt{n}}{2}. \tag{19}$$

Suppose that $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$. Since $n, \sigma \in \mathbb{N}$ and $n, \sigma > 1$, thus,

$$\sigma\sqrt{n} - \frac{\sqrt{n}}{2} = \frac{2\sigma\sqrt{n} - \sqrt{n}}{2} = \frac{\sqrt{n}(2\sigma - 1)}{2} > 0 \tag{20}$$

This implies that, $\|\vec{p} - \vec{q}\| < \sigma\sqrt{n}$.

3.3 GGH-MKA Cryptosystem

Recently, Mandangan *et al.,* [18] proposed a new variant of the GGH cryptosystem, referred to as the GGH-MKA cryptosystem. Through minor modification on the GGH cryptosystem's design, the flaw that being exploited by the Nguyen's embedding attacks is repaired. Consequently, the simplification of the GGH-CVP is completely prevented, and the GGH-CVP distance is maintained as $\sigma\sqrt{n}$. These improvements are achieved by introducing a new error vector $\vec{e}' \in \mathbb{Z}^n$ the together with its elements' distribution rule to ensure that the distance $\sigma\sqrt{n}$ could be preserved.

The error vector $\vec{e}'$ consisting the entries$e_i \in \{(2-\sigma), (1-\sigma), \sigma, (\sigma+1)\}$ for all $i = 1, \ldots, n$. By distributing the entries $(2-\sigma), (1-\sigma), \sigma$ and $(\sigma+1)$ randomly in the vector $\vec{e}'$ according to the provided distribution rule, then it is proven that the error vector $\vec{e}'$ is non-eliminable from the encryption equation and the distance $\|\vec{p} - \vec{q}\| = \sigma\sqrt{n}$.

Theorem 1: For $n, \sigma \in \mathbb{N}$, *let* $\vec{c} = B\vec{m} + \vec{e}$ be a ciphertext vector where $B \in \mathbb{R}^{n \times n}$ is a public basis for the lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$, $\vec{m} \in \mathbb{Z}^n$ is a plaintext vector and $\vec{e} \in \mathbb{Z}^n$ is an error vector. Suppose that $n = (4\sigma - 2)k$, where $\sigma > 2$ and $k \in \mathbb{N}$. If $e_i \in \vec{e}$ for all $i = 1, \ldots, n$ are randomly selected from the set $E = \{(2-\sigma), (1-\sigma), \sigma, (\sigma+1)\}$ based on the following distributions. Then, the GGH cryptosystem is invulnerable to Nguyen's embedding attacks [18].

$$e_i = \begin{cases} (2-\sigma), for\ \frac{n}{4\sigma-2}\ number\ of\ entries \\ (1-\sigma), for\ \frac{\sigma n-n}{2\sigma-1}\ number\ of\ entries \\ \sigma, \qquad for\ \frac{n}{4\sigma-2}\ number\ of\ entries \\ (\sigma+1), for\ \frac{\sigma n-n}{2\sigma-1}\ number\ of\ entries \end{cases} \tag{21}$$

4. The Proposed Countermeasure

The Nguyen's embedding-based attacks succeed due to its ability to simplify the underlying GGH-CVP and make the GGH-SVP distance shorter than $\sigma\sqrt{n}$. Thus, stopping the simplification and maintain the distance could win the combat against the Nguyen's embedding-based attacks.

4.1 Preventing Simplification of GGH-CVP

Nguyen's embedding attacks work by inserting vector $\vec{s} \in \{\sigma\}^n$ into the encryption equation $\vec{c} = B\vec{m} + \vec{e}$, where $\vec{c} \in \mathbb{R}^n$ is a ciphertext vector, $B \in \mathbb{R}^{n\times n}$ is a basis for the lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$, $\vec{m} \in \mathbb{Z}^n$ is a plaintext vector and $\vec{e} \in \mathbb{Z}^n$ is an error vector. In the GGH cryptosystem, the vector $\vec{e} \in \{-\sigma, +\sigma\}^n$ is eliminable through the formation of the congruences $\vec{c} + \vec{s} \equiv B\vec{m}\ (mod\ 2\sigma)$. Consequently, the GGH-CVP can be simplified. To prevent the simplification, consider the following lemma.

Lemma 2.1: For $n, \sigma \in \mathbb{N}$, let $\vec{s} \in \{\sigma\}^n$ and $\vec{c} = B\vec{m} + \vec{e}$ where $\vec{c} \in \mathbb{R}^n$ is a ciphertext vector, $B \in \mathbb{R}^{n\times n}$ is a basis for the lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$, $\vec{m} \in \mathbb{Z}^n$ is a plaintext vector and $\vec{e}^* \in \mathbb{Z}^n$ is an error vector. If $\sigma > 1$ and $e_i^* \in \vec{e}^*$ are randomly selected from $F = \{(2+\sigma), (2-\sigma), (1+\sigma), (-\sigma-1)\}$ for all $i = 1, \dots, n$ and all entries of F appear at least once in $\vec{e}^*$, then $\vec{c} + \vec{s} \not\equiv B\vec{m}\ (mod\ \sigma)$ and $\vec{c} + \vec{s} \not\equiv B\vec{m}\ (mod\ 2\sigma)$. Proof, given that $\vec{c} = B\vec{m} + \vec{e}^*$ and $\vec{s} \in \{\sigma\}^n$. Thus,

$$\vec{c} + \vec{s} = B\vec{m} + \vec{e}^* + \vec{s} \tag{22}$$

$$\vec{c} + \vec{s} - B\vec{m} = \vec{e}^* + \vec{s} \tag{23}$$

Suppose that $e_1^* = 2+\sigma, e_2^* = 2-\sigma, e_3^* = 1+\sigma, e_4^* = -\sigma-1$ and $e_n^* = -\sigma-1$. Thus,

$$\frac{\vec{e}^*+\vec{s}}{2\sigma} = \frac{1}{2\sigma}\begin{bmatrix} 2+\sigma+\sigma \\ 2-\sigma+\sigma \\ 1+\sigma+\sigma \\ -\sigma-1+\sigma \\ \vdots \\ -\sigma-1+\sigma \end{bmatrix} = \frac{1}{2\sigma}\begin{bmatrix} 2+2\sigma \\ 2 \\ 1+2\sigma \\ -1 \\ \vdots \\ -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sigma}+1 \\ \frac{1}{\sigma} \\ \frac{1}{2\sigma}+1 \\ -\frac{1}{2\sigma} \\ \vdots \\ -\frac{1}{2\sigma} \end{bmatrix} \notin \mathbb{Z}^n \tag{24}$$

These imply that,

$$\frac{\vec{c}+\vec{s}-B\vec{m}}{2\sigma} \notin \mathbb{Z}^n \tag{25}$$

By Definition 6, therefore $\vec{c} + \vec{s} \not\equiv B\vec{m}\ (mod\ 2\sigma)$. By implementing the proposed error vector $\vec{e}^*$, the simplification of the underlying GGH-CVP can be totally prevented. The encryption equation is maintained as $\vec{c} = B\vec{m} + \vec{e}^*$ and the underlying GGH-CVP remain in its original form.

4.2 Maintaining GGH-CVP Distance as $\sigma\sqrt{n}$

We proposed the distribution rule to tabulate the entries of the new set F in the new error vector $\vec{e}^*$. The position of all these entries is randomly distributed but the number of appearances of each entry must follows the proposed distribution rule. By doing so, we proved that the desired GGH-CVP distance can be preserved as $\sigma\sqrt{n}$. Consequently, the lattice gap in the embedded lattice $\mathcal{L}'$ is maintained and this makes the derived GGH-SVP by the embedding-based attacks becomes harder to solve as faced by all attacks prior to Nguyen's embedding-based attack.

Lemma 2.2: For $n, \sigma \in \mathbb{N}$, let $\vec{s} \in \{\sigma\}^n$ and $\vec{c} = \vec{v} + \vec{e}^*$ where $\vec{c} \in \mathbb{R}^n$, $\vec{v} \in \mathcal{L} \subset \mathbb{R}^n$ and $\vec{e}^* \in \mathbb{Z}^n$ is an error vector. If $\sigma > 1$, $n = (10\sigma - 3)k$ and $e_i^* \in \vec{e}^*$ are randomly selected from $F = \{(2+\sigma), (2-\sigma), (1+\sigma), (-\sigma-1)\}$ based on the following distribution rule.

$$e_i^* = \begin{cases} 2+\sigma, \text{for } \frac{n(2\sigma-2)}{10\sigma-3} \text{ entries}, \\ 2-\sigma, \text{for } \frac{n(4\sigma-3)}{10\sigma-3} \text{ entries}, \\ 1+\sigma, \text{for } \frac{n(2\sigma-2)}{10\sigma-3} \text{ entries}, \\ -\sigma-1, \text{for } \frac{n(2\sigma-2)}{10\sigma-3} \text{ entries}, \end{cases} \tag{26}$$

For all $i = 1, \dots, n$, then $\vec{c} - \vec{v} = \sigma\sqrt{n}$. Proof, note that,

$$\begin{aligned} \|\vec{e}\| &= \sqrt{\sum_{i=1}^{\frac{n(2\sigma-2)}{10\sigma-3}} (2+\sigma)^2 + \sum_{i=1}^{\frac{n(4\sigma-3)}{10\sigma-3}} (2-\sigma)^2 + \sum_{i=1}^{\frac{n(2\sigma-2)}{10\sigma-3}} (1+\sigma)^2 + \sum_{i=1}^{\frac{n(2\sigma-2)}{10\sigma-3}} (-\sigma-1)^2} \\ &= \sqrt{\frac{n(2\sigma-2)}{10\sigma-3}(2+\sigma)^2 + \frac{n(4\sigma-3)}{10\sigma-3}(2-\sigma)^2 + \frac{n(2\sigma-2)}{10\sigma-3}(1+\sigma)^2 + \frac{n(2\sigma-2)}{10\sigma-3}(-\sigma-1)^2} \\ &= \sqrt{n\left(\frac{2\sigma-2((2+\sigma)^2+(\sigma+1)^2+(-\sigma-1)^2)+4\sigma+3(2-\sigma)^2}{10\sigma-3}\right)} \\ &= \sqrt{n\sigma^2\left(\frac{10\sigma-3}{10\sigma-3}\right)} \\ &= \sigma\sqrt{n} \end{aligned} \tag{27}$$

Since $\vec{c} = \vec{v} + \vec{e}^*$, then $\vec{c} - \vec{v} = \vec{e}^*$ and $\|\vec{c} - \vec{v}\| = \|\vec{e}\|$. Therefore, $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$.

5. Discussion and Conclusion

Other than security, practicality also should be considered as significant aspect in post-quantum cryptography. The GGH cryptosystem was considered practical prior to the devastating attacks by Nguyen. Upgrading the security of the GGH cryptosystem against the Nguyen's embedding attacks should revive the interest on the GGH cryptosystem. That is why countermeasure to strengthen security of the scheme is worth to be done. Findings from this study justify that the set of entries F as well as the distribution rule for the entries of F in the error vector are not unique. We expect that more sets and distribution rules could be discovered to secure the GGH cryptosystem against Nguyen's embedding attacks. Since the set of entries is not unique, it could be interesting to find the

generalization of the set based on the pre-setup parameters. The strategy is still the same. Prevent the simplification of the GGH-CVP and keep the GGH-CVP distance as $\sigma\sqrt{n}$. This is what we have done in this study.

We proved that the formation of the congruence $\vec{c} + \vec{s} \equiv B\vec{m}\ (mod\ 2\sigma)$ can be prevented by using the newly proposed error vector $\vec{e}^*$. On top of that, the lattice gap enlargement which accelerates the performance of lattice reduction algorithms also totally avoided due to the proposed distribution rules on the entries of the proposed error vector $\vec{e}^*$. More and thorough security analyses on the GGH-MKA cryptosystem are demanded to justify its robustness towards any possible attacks other than the Nguyen's embedding-based attacks to build confident, trust and willingness to consider the scheme as competent alternative in post-quantum cryptography.

Acknowledgement
The authors would like to express their gratitude to the anonymous reviewers for their valuable comments and suggestions for a betterment of this extended abstract. This study is financially supported by the research grant SBK0508-2021 awarded by Universiti Malaysia Sabah.

References

[1] Muslim, Norliana, Faridah Yunos, Zuren Razali, and Nur Idalisa Norddin. "Enhanced scalar multiplication algorithm over prime field using elliptic net." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 40, no. 2 (2024): 22-35. https://doi.org/10.37934/araset.40.2.2235

[2] Pappa, Chandramohan Kanmani, Dasthegir Nasreen Banu, Kumar Vaishnavi, Susila Nagarajan, Manivannan Karunakaran, and Perisetla Kandaswamy Hemalatha. "A novel approach for block chain technology based cyber security in cloud storage using hash function." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 32, no. 3 (2023): 178-189. https://doi.org/10.37934/araset.32.3.178189

[3] Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134. Ieee, 1994. https://doi.org/10.1109/SFCS.1994.365700

[4] Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." *Nature* 549, no. 7671 (2017): 188-194. https://doi.org/10.1038/nature23461

[5] Asif, Rameez. "Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms." *IoT* 2, no. 1 (2021): 71-91. https://doi.org/10.3390/iot2010005

[6] Kuznetsov, Alexandr, Igor Svatovskij, Nastya Kiyan, and Andriy Pushkar'ov. "Code-based public-key cryptosystems for the post-quantum period." In *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, p. 125-130. IEEE, 2017. https://doi.org/10.1109/INFOCOMMST.2017.8246365

[7] Cheon, Jung Hee, Kyoohyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. "A practical post-quantum public-key cryptosystem based on." In *International Conference on Information Security and Cryptology*, p. 51-74. Cham: Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-53177-9_3

[8] Gaborit, Philippe, and Marc Girault. "Lightweight code-based identification and signature." In *2007 IEEE International Symposium on Information Theory*, p. 191-195. IEEE, 2007. https://doi.org/10.1109/ISIT.2007.4557225

[9] Baldi, Marco, Paolo Santini, and Giovanni Cancellieri. "Post-quantum cryptography based on codes: State of the art and open challenges." In *2017 AEIT International Annual Conference*, p. 1-6. IEEE, 2017. https://doi.org/10.23919/AEIT.2017.8240549

[10] Shrestha, Sujan Raj, and Young-Sik Kim. "New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography." In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, pp. 368-372. IEEE, 2014. https://doi.org/10.1109/ISCIT.2014.7011934

[11] An, SangWoo, and Seog Chung Seo. "Efficient parallel implementations of LWE-based post-quantum cryptosystems on graphics processing units." *Mathematics* 8, no. 10 (2020): 1781. https://doi.org/10.3390/math8101781

[12] Güneysu, Tim, Vadim Lyubashevsky, and Thomas Pöppelmann. "Practical lattice-based cryptography: A signature scheme for embedded systems." In *Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14*, pp. 530-547. Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-33027-8_31

[13] Roma, Crystal Andrea, Chi-En Amy Tai, and M. Anwar Hasan. "Energy efficiency analysis of post-quantum cryptographic algorithms." *IEEE Access* 9 (2021): 71295-71317. https://doi.org/10.1109/ACCESS.2021.3077843
[14] Goldreich, Oded, Shafi Goldwasser, and Shai Halevi. "Public-key cryptosystems from lattice reduction problems." In *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17*, p. 112-131. Springer Berlin Heidelberg, 1997. https://doi.org/10.1007/BFb0052231
[15] Nguyen, Phong. "Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto'97." In *Annual International Cryptology Conference*, p. 288-304. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999. https://doi.org/10.1007/3-540-48405-1_18
[16] Mandangan, Arif, Hailiza Kamarulhaili, and Muhammad Asyraf Asbullah. "On the underlying hard lattice problems of ggh encryption scheme." In *Cryptology and Information Security Conference*, p. 42. 2018.
[17] Mandangan, Arif, Hailiza Kamarulhaili, and Muhammad Asyraf Asbullah. "On the underlying hard lattice problems of ggh encryption scheme." In *Cryptology and Information Security Conference*, p. 42. 2018. Mandangan, A., H. Kamarulhaili, and M. A. Asbullah. "The Efficiency of Embedding-Based Attacks on the GGH Lattice-Based Cryptosystem." *Malaysian Journal of Mathematical Sciences* 17, no. 4 (2023). https://doi.org/10.47836/mjms.17.4.09
[18] mandangan, arif, hailiza kamarulhaili, and Muhammad Asyraf Asbullah. "A security upgrade on the GGH lattice-based cryptosystem." *Sains Malaysiana* 49, no. 6 (2020): 1471-1478. http://dx.doi.org/10.17576/jsm-2020-4906-25
[19] Hoffstein, Jeffrey, Jill Pipher, Joseph H. Silverman, Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. "Lattices and cryptography." *An Introduction to Mathematical Cryptography* (2014): 373-470. https://doi.org/10.1007/978-1-4939-1711-2_7
[20] Banerjee, Utpal, and Utpal Banerjee. "Unimodular Matrices." *Loop Transformations for Restructuring Compilers: The Foundations* (1993): 21-48. https://doi.org/10.1007/978-0-585-28004-2_2
[21] Goldreich, Oded, Daniele Micciancio, Shmuel Safra, and J-P. Seifert. "Approximating shortest lattice vectors is not harder than approximating closest lattice vectors." *Information Processing Letters* 71, no. 2 (1999): 55-61. https://doi.org/10.1016/S0020-0190(99)00083-6
[22] Schnorr, C. P., M. Fischlin, H. Koy, and A. May. "Lattice attacks on GGH-Cryptosystem." *Rump session of Crypto* 97 (1997).