Malaysian Journal of Mathematical Sciences 13(S) August: 1–11 (2019)
Special Issue: The 6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

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

On the Smallest-Basis Problem underlying the GGH Lattice-based Cryptosystem

Mandangan, A.[1,2], Kamarulhaili, H.[1], and Asbullah, M.A.*[3,4]

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

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

ABSTRACT

The security of the Goldreich-Goldwasser-Halevi (GGH) cryptosystem is relying on the Smallest-Basis Problem (SBP) and the Closest-Vector Problem (CVP) instances. Previously, these instances were just implicitly mentioned and discussed without any proper definition. In this paper, we explicitly defined the underlying SBP instance that arose from the GGH cryptosystem. From that, we showed how the solution to these problems could be obtained and how the obtained solutions could lead to the security breach in the GGH cryptosystem. Finally, we proposed some possible strategies for strengthening the security of the GGH cryptosystem.

Keywords: GGH cryptosystem, Smallest-Basis Problem, Closest-Vector Problem, Shortest-Vector Problem.

1. Introduction

Lattice-based cryptography emerges as one of the high potential alternatives in the post-quantum cryptography era. The construction of cryptographic schemes based on lattice-based problems instead of the number of theoretical-based problems makes the lattice-based cryptosystems conjectured to be unaffected by the Shor's quantum attack, see Shor (1999). In Goldreich et al. (1997) proposed a trapdoor one-way function, addressed as the GGH trapdoor one-way function (Mandangan et al., 2018). The security of this function is inspired by two lattice-based problems, namely the Smallest-Basis Problem (SBP) and the Closest-Vector Problem (SVP). From the GGH trapdoor one-way function, Goldreich et al. (1997) proposed an encryption scheme known as the GGH cryptosystem.

The GGH cryptosystem was recognized as the first lattice-based cryptosystem with a competent level of efficiency and practicality. With low-cost mathematical operations involving matrices and vectors, the GGH cryptosystem offers a better efficiency level compared to the famous RSA and ElGamal cryptosystems. In the security aspect, the underlying lattice-problems that arose from the GGH cryptosystem was conjectured as invulnerable once the cryptosystem is implemented in a lattice dimension of 300 and above (Goldreich et al., 1997). Although the GGH cryptosystem is broken due to the Nguyen's attack (Nguyen, 1999), some attempts for improving the security of the GGH cryptosystem can be found in literature, for instance, de Barros and Schechter (2015), Micciancio (2001), Paeng et al. (2003), Sipasseuth et al. (2019), Yoshino and Kunihiro (2012).

Since the proposal of the GGH cryptosystem, the underlying lattice-based problems that arose from the GGH cryptosystem were just implicitly mentioned and discussed. In (Mandangan et al., 2018), we defined the underlying CVP instance as the GGH-CVP instance together with the simplified versions of this instance that are derived by the Nguyen's attack (Nguyen, 1999) and the Lee-Hahn's attack Lee and Hahn (2010) on it. As a continuity, we proposed the definition for another lattice-based problem that arose from the GGH cryptosystem.

In this paper, we explicitly defined the underlying SBP instance of the GGH cryptosystem. From that, we investigated some features of this instance related to the solution and the method for solving this instance. Finally, we proposed some strategies for strengthening the security of the GGH cryptosystem. This paper is arranged in the following flow.

We provide some related mathematical background in Section 2 then followed by a brief yet necessary introduction to the GGH cryptosystem in Section 3. Furthermore, we defined the underlying lattice-based problems of the GGH cryptosystem in Section 4. Further discussion is presented in Section 5 and conclusion remark is given in Section 6.

2. Mathematical Background

Along this paper, we standardize some mathematical notations. Firstly, we denote $m, n \in \mathbb{N}$. Then, all vectors are considered as column vectors and denoted using standard vector notation. For instance, $\vec{b} \in \mathbb{R}^m$ is a column vector with m real entries $b_i \in \vec{b}$, for all $i = 1, \ldots, m.$. A set of vectors $\vec{b}_i \in \mathbb{R}^m$, denoted as $B = \left\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\right\}$ is representable in matrix form as $B \in \mathbb{R}^{n \times n}$ where the vectors $\vec{b}_i$ be the columns of the matrix B for all $i = 1, \ldots, n$. If the set B is linearly independent, then it can be used to span a lattice.

Definition 2.1: (Hoffstein et al., 2008) *For $m \leq n$, let $B = \left\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\right\}$ be the set of linearly independent vectors. The lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$ generated by the basis B is defined as the set of all linear combinations of the basis vectors $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ with integer scalars, i.e.,*

$$L(B) = \left\{a_1\vec{b}_1 + a_2\vec{b}_2 + \cdots + a_n\vec{b}_n : a_i \in \mathbb{Z}, \forall i = 1, \ldots, n\right\} \tag{1}$$

Based on Definition 2.1, the dimension of the lattice $L(B)$ is $dim(L(B)) = n$ and the rank of the lattice $L(B)$ is $rank(L(B)) = m$. If $m = n$, then the lattice $L(B)$ is referred to as a full-rank lattice. This paper is dealing only with this kind of lattice.

Theorem 2.1: (Goodaire, 2013). *A square matrix is invertible if and only if its columns are linearly independent.*

Thus, the bases for the full-rank lattices are representable as non-singular matrices. A lattice can be spanned by a more than one basis. Two different bases are mathematically related by a unimodular matrix. The matrix $U \in \mathbb{Z}^{n \times n}$ is called a unimodular matrix if $det(U) = \pm 1$.

Proposition 2.1: (Galbraith, 2012). *Let $G, B \in \mathbb{R}^{n \times n}$ be two non-singular matrices. The matrices G and B span the same lattice $\mathcal{L} \subset \mathbb{R}^n$, i.e., $L(G) = L(B) = \mathcal{L}$, if and only if $G = BU$ where the matrix $U \in \mathbb{Z}^{n \times n}$ is a unimodular matrix.*

When $n \geq 2$, there are infinitely many unimodular matrices. This implies that the lattice in $n \geq 2$ can be spanned by infinitely many bases. Normally, these bases are classified as a good basis and a bad basis. A good basis is a lattice basis consisting of reasonably short and slightly non-orthogonal basis vectors. On the contrary, a lattice basis with long and highly non-orthogonal basis vectors is classified as a bad basis. The non-orthogonality of a lattice basis can be measured by computing the dual-orthogonality defect of the basis.

Definition 2.2: (Goldreich et al., 1997). *Let $G \in \mathbb{R}^{n\times n}$ with columns $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ be a basis for the lattice $\mathcal{L} \subset \mathbb{R}^n$. The dual-orthogonal defect of the basis G is computed as follow,*

$$dual_{OD}(G) = \frac{\prod_{i=1}^{n} \|\vec{g}_i'\|}{|\det G^{-1}|} \tag{2}$$

where $\|\vec{g}_i'\|$ is the Euclidean norm of the i-th row vector in G^{-1}.

To be classified as a good basis, the dual-orthogonality defect of the basis G is required to be small, i.e, $dual_{OD}(G)$ is close to 1. If $dual_{OD}(G)$ is large and far from 1, then the basis G is classified as a bad basis. Consider the following definition related to successive minima of a lattice.

Definition 2.3: (Nguyen, 1999). *Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. The i-th minimum of the lattice $\mathcal{L}$, denoted as $\lambda_i(\mathcal{L})$, is the radius of the smallest sphere centered in the origin containing i linearly independent lattice vectors.*

Basically, the first minimum of the lattice $\mathcal{L}$ is $\lambda_1(\mathcal{L}) = \|\vec{v}_1\|$, where $\vec{v}_1 \in \mathcal{L}$ is shortest non-zero vector in the lattice $\mathcal{L}$ such that $\|\vec{v}_1\| < \|\vec{v}_i\|$ for all $i = 2, \ldots$. Most of the lattice-based problems are related to norm or distance minimization. The most established lattice-based problems are the Smallest-Basis Problem (SBP), Closest-Vector Problem (CVP) and the Shortest-Vector Problem (SVP). Any variant derived from these problems are referred to as instance.

Definition 2.4: (Goldreich et al., 1997). *Let $B \in \mathbb{R}^{n\times n}$ be a basis for the full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$. Given the basis B, the Smallest Basis Problem (SBP)is to find the smallest basis B' for the same lattice $\mathcal{L}$ where the basis B' has a small orthogonal defect.*

Definition 2.5: (Hoffstein et al., 2008). *Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. Given a basis of 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 $\vec{v} \in \mathcal{L}$ such that the Euclidean norm $\|\vec{t} - \vec{v}\|$ is minimum.*

Definition 2.6: (Galbraith, 2012). *Let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. Given a basis for the lattice $\mathcal{L}$, the Shortest-Vector Problem (SVP) is to find a non-zero vector $\vec{v} \in \mathcal{L}$ such that the Euclidean norm $\|\vec{v}\|$ is minimal, i.e., $\|\vec{v}\| = \lambda_1(\mathcal{L})$.*

3. GGH Cryptosystem

Consider a communications scenario where Bob wants to send a secret message to Alice and they agree to use the GGH cryptosystem. The key generation, encryption and decryption algorithms of the GGH cryptosystem are given in the following tables:

Table 1: Key Generation Algorithm done by Alice

Input	Security parameter n.
Output	Public key (B, σ, n) and private key (G, U).
Steps	Generate the private basis $G \in \mathbb{R}^{n \times n}$. Generate the unimodular matrix $U \in \mathbb{Z}^{n \times n}$. Compute the public basis $B \in \mathbb{R}^{n \times n}$ as $B = GU^{-1}$. Determine the threshold parameter $\sigma \in \mathbb{N}$.

Table 2: Encryption Algorithm done by Bob

Input	Alice's public key (B, σ, n) and plaintext $\vec{m} \in \mathbb{Z}^n$.
Output	Ciphertext $\vec{c} \in \mathbb{R}^n$.
Steps	Generate the error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$. Generate the plaintext vector $\vec{m} \in \mathbb{Z}^n$. Encrypt the plaintext as $\vec{c} = B\vec{m} + \vec{e}$.

Table 3: Decryption Algorithm done by Alice

Input	Bob's ciphertext $\vec{c} \in \mathbb{R}^n$ and private key (G, U).
Output	Bob's plaintext $\vec{m} \in \mathbb{Z}^n$.
Steps	Compute $\vec{x} = G^{-1}\vec{c}$. Round each entry $x_i \in \vec{x}$ to the nearest integer $\lfloor x_i \rceil \in \mathbb{Z}$ such that $\lvert x_i - \lfloor x_i \rceil \rvert < \frac{1}{2}$ for all $i = 1, \ldots, n$. Decrypt the ciphertext as $\vec{m} = U\lfloor \vec{x} \rceil$.

Consider following computation in the decryption algorithm,

$$\begin{aligned}
U\lfloor \vec{x}\rceil &= U\lfloor G^{-1}\vec{c}\rceil, since\ \vec{x}=G^{-1}\vec{c}\\
&= U\lfloor G^{-1}(B\vec{m}+\vec{e})\rceil, since\ \vec{c}=B\vec{m}+\vec{e}\\
&= U\lfloor G^{-1}B\vec{m}+G^{-1}\vec{e}\rceil\\
&= \lfloor UG^{-1}B\vec{m}\rceil + U\lfloor G^{-1}\vec{e}\rceil\\
&= \lfloor B^{-1}GG^{-1}B\vec{m}\rceil + U\lfloor G^{-1}\vec{e}\rceil, since\ U=B^{-1}G\\
&= \lfloor \vec{m}\rceil + U\lfloor G^{-1}\vec{e}\rceil\\
&= \vec{m} + U\lfloor G^{-1}\vec{e}\rceil, since\ \vec{m}\in\mathbb{Z}^n
\end{aligned}$$

To avoid the decryption error, the selection of the threshold parameter σ, which is the entry of the error vector $\vec{e}$, must be properly done based on the following theorem:

Theorem 3.1: (Mandangan et al., 2018). *Let $G \in \mathbb{R}^{n\times n}$ be the private basis for the lattice $\mathcal{L} \subset \mathbb{R}^n$ and $\rho \in \mathbb{R}$ denotes the maximum l_1-norm of the rows of G^{-1}. As long as the threshold parameter $\sigma \in \mathbb{R}$ satisfies $\sigma < \frac{1}{2\rho}$, then no decryption error can occur.*

By determining the threshold parameter σ as required by Theorem 3.1, then the condition $\lfloor G^{-1}\vec{e}\rceil = \vec{0}$ can be fulfilled (Mandangan et al., 2018). Thus,

$$U\lfloor \vec{x}\rceil = \vec{m} + U\lfloor \vec{0}\rceil = \vec{m}$$

which indicates that the decryption is done without error.

4. The Smallest-Basis Problem Instance

In this section, consider Eve as an unauthorized third party between the communication of Alice and Bob. Suppose that Eve has Alice's public key (B, σ, n) and Bob's ciphertext $\vec{c}$. To break the GGH cryptosystem, Eve aims to recover Bob's plaintext $\vec{m}$ using the available information. The security of the GGH cryptosystem is relying on several lattice-based problems. Thus, the most obvious way to break the security of the GGH cryptosystem is by solving the underlying lattice-based problem instances that arose from the GGH cryptosystem. For that purpose, Eve launches the Babai's round-off attack and the embedding attack. Since Eve does not has Alice's private basis G, then she could not perform the effective decryption as done by Alice. The only available information to her is the public basis of B, which is a bad basis. Suppose that, Eve proceeds to perform the decryption using the public basis B. Before that, consider the following proposition:

Proposition 4.1: *For $\sigma \in \mathbb{N}$, let $\vec{\sigma} = \{+\sigma\}^n$, $\vec{e} \in \{-\sigma, +\sigma\}^n$ and $M \in \mathbb{R}^{n\times n}$. If $\lfloor M\vec{\sigma} \rceil = \vec{0}$, then $\lfloor M\vec{e} \rceil = \vec{0}$.*

Proof:
Consider the vector $M\vec{\sigma}$ as follows,

$$M\vec{\sigma} = \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \cdots & m_{n,n} \end{pmatrix} \begin{bmatrix} \sigma \\ \sigma \\ \vdots \\ \sigma \end{bmatrix} = \begin{bmatrix} \sigma\left(m_{1,1} + m_{1,2} + \cdots + m_{1,n}\right) \\ \sigma\left(m_{2,1} + m_{2,2} + \cdots + m_{2,n}\right) \\ \vdots \\ \sigma\left(m_{n,1} + m_{n,2} + \cdots + m_{n,n}\right) \end{bmatrix}$$

Suppose that $\lfloor M\vec{\sigma} \rceil = \vec{0}$. This implies that

$$\left|\sigma\left(m_{i,1} + m_{i,2} + \cdots + m_{i,n}\right)\right| < \frac{1}{2}$$

for all $i = 1, \ldots, n$. Now, consider the vector $M\vec{e}$ as follows,

$$M\vec{e} = \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \cdots & m_{n,n} \end{pmatrix} \begin{bmatrix} \pm\sigma \\ \pm\sigma \\ \vdots \\ \pm\sigma \end{bmatrix} = \begin{bmatrix} (\pm\sigma)\left(m_{1,1} + m_{1,2} + \cdots + m_{1,n}\right) \\ (\pm\sigma)\left(m_{2,1} + m_{2,2} + \cdots + m_{2,n}\right) \\ \vdots \\ (\pm\sigma)\left(m_{n,1} + m_{n,2} + \cdots + m_{n,n}\right) \end{bmatrix}$$

Assume that the k-th row of the matrix M has the maximum l_1-norm, i.e.,

$$\sum_{j=1}^{n} |m_{k,j}| > \sum_{j=1}^{n} |m_{i,j}|$$

where $1 \leq k \leq n$ for all $i = 1, \ldots, n$ and $k \neq i$. Consider the absolute value of the k-th row of the vector $M\vec{e}$ as follows,

$$\begin{aligned} \left|(\pm\sigma)\left(m_{k,1} + m_{k,2} + \cdots + m_{k,n}\right)\right| &= |\pm\sigma|\left|m_{k,1} + m_{k,2} + \cdots + m_{k,n}\right| \\ &= \left|\sigma\left(m_{k,1} + m_{k,2} + \cdots + m_{k,n}\right)\right|. \end{aligned}$$

Since

$$\left|\sigma\left(m_{i,1} + m_{i,2} + \cdots + m_{i,n}\right)\right| < \frac{1}{2}$$

for all $i = 1, \ldots, n$, then

$$\left|\sigma\left(m_{k,1} + m_{k,2} + \cdots + m_{k,n}\right)\right| < \frac{1}{2}$$

as well. Since $\sigma\left(m_{k,1} + m_{k,2} + \cdots + m_{k,n}\right)$ is the largest entry in the vector $M\vec{e}$, then the absolute value of each entry of the vector $M\vec{e}$ is less than $\frac{1}{2}$ as well. Consequently, $\lfloor M\vec{e} \rceil = \vec{0}$ and this ends the proof.

Now, consider the following attack by Eve on the GGH cryptosystem:

Lemma 4.1: *Let $B \in \mathbb{R}^{n\times n}$ be a basis for the lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$, $\sigma \in \mathbb{N}$ be a threshold parameter, $\vec{e} \in \{-\sigma, +\sigma\}^n$ be an error vector and $\vec{\sigma} = \{+\sigma\}^n$. Suppose that $\vec{y} \in \mathbb{R}^n$ such that $\vec{y} = B^{-1}\vec{c}$. If $\lfloor B^{-1}\vec{\sigma}\rceil = \vec{0}$, then $\lfloor \vec{y}\rceil = \vec{m} \in \mathbb{Z}^n$.*

Proof:
Note that,

$$\begin{aligned}
\lfloor \vec{y}\rceil &= \lfloor B^{-1}\vec{c}\rceil \\
&= \lfloor B^{-1}\left(B\vec{m} + \vec{e}\right)\rceil \\
&= \lfloor B^{-1}B\vec{m} + B^{-1}\vec{e}\rceil \\
&= \lfloor \vec{m}\rceil + \lfloor B^{-1}\vec{e}\rceil \\
&= \vec{m} + \lfloor B^{-1}\vec{e}\rceil
\end{aligned}$$

since $\vec{m} \in \mathbb{Z}^n$. Suppose that, $\lfloor B^{-1}\vec{\sigma}\rceil = \vec{0}$. According to Proposition 4.1, we have $\lfloor B^{-1}\vec{e}\rceil = \vec{0}$ as well. Therefore,

$$\lfloor \vec{y}\rceil = \vec{m} + \lfloor \vec{0}\rceil = \vec{m}$$

which indicates that decryption by Eve succeeds.This ends the proof.

Instead of performing decryption using the bad basis B, alternatively, Eve could use the reduced-form of the basis B. By reducing the basis B using a lattice-reduction algorithm, the orthogonality of the bad basis B can be improved. Suppose that, Eve uses the LLL-algorithm as the lattice-reduction tool. Then, denote the LLL-reduced form of the basis B as B_{LLL} where $dual_{OD}(B_{LLL}) < dual_{OD}(B)$.

Now, consider the following lemma:

Lemma 4.2: *Let $B \in \mathbb{R}^{n\times n}$ be a basis for the lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$, $B_{LLL} \in \mathbb{R}^{n\times n}$ be the LLL-reduced form of the basis B such that $B_{LLL} = BT$ where $T \in \mathbb{Z}^{n\times n}$ is a unimodular matrix, $\sigma \in \mathbb{N}$ be the threshold parameter, $\vec{e} \in \{-\sigma, +\sigma\}^n$ be the error vector, $\vec{\sigma} = \{+\sigma\}^n$ and $\vec{c} \in \mathbb{R}^n$ be the ciphertext vector such that $\vec{c} = B\vec{m} + \vec{e}$ where $\vec{m} \in \mathbb{Z}^n$ is the plaintext vector. Suppose that $\vec{z} \in \mathbb{R}^n$ such that $\vec{z} = B_{LLL}^{-1}\vec{c}$. If $\lfloor B_{LLL}^{-1}\vec{\sigma}\rceil = \vec{0}$, then $T\lfloor \vec{z}\rceil = \vec{m}$.*

Proof:

Note that,

$$\begin{aligned} T\lfloor \vec{z} \rceil &= T\lfloor B_{LLL}^{-1}\vec{c} \rceil \\ &= T\lfloor B_{LLL}^{-1}\left(B\vec{m} + \vec{e}\right) \rceil \\ &= T\lfloor B_{LLL}^{-1}B\vec{m} + B_{LLL}^{-1}\vec{e} \rceil \\ &= \lfloor TB_{LLL}^{-1}B\vec{m} \rceil + T\lfloor B_{LLL}^{-1}\vec{e} \rceil \\ &= \lfloor B^{-1}B_{LLL}B_{LLL}^{-1}B\vec{m} \rceil + T\lfloor B_{LLL}^{-1}\vec{e} \rceil \\ &= \lfloor \vec{m} \rceil + T\lfloor B_{LLL}^{-1}\vec{e} \rceil \\ &= \vec{m} + T\lfloor B_{LLL}^{-1}\vec{e} \rceil \end{aligned}$$

since $T = B^{-1}B_{LLL}$ and $\vec{m} \in \mathbb{Z}^n$. Suppose that, $\lfloor B_{LLL}^{-1}\vec{\sigma} \rceil = \vec{0}$. According to Proposition 4.1, we have $\lfloor B_{LLL}^{-1}\vec{e} \rceil = \vec{0}$ as well. Therefore,

$$T\lfloor \vec{z} \rceil = \lfloor \vec{m} + \vec{0} \rceil = \vec{m}$$

which indicates that decryption by Eve succeeds.This ends the proof.

From Lemma 4.2, it can be observed that the attempt by Eve to perform decryption using the reduced basis B_{LLL} succeeds once the reduced basis B_{LLL} satisfies the condition $\lfloor B_{LLL}^{-1}\vec{\sigma} \rceil = \vec{0}$. This condition can be met if the reduced basis B_{LLL} has much shorter and more orthogonal basis vectors compared to the original basis of B.

In other words, the reduced basis B_{LLL} must have a small dual-orthogonality defect. Finding such a lattice basis is an SBP instance. Thus, we propose the following definition for the underlying SBP instance that arose from the GGH cryptosystem, addressed as the GGH-SBP instance.

Definition 4.1: *Let $B \in \mathbb{R}^{n\times n}$ be the basis for the lattice $L(B) = \mathcal{L} \subset \mathbb{R}^n$, $\sigma \in \mathbb{N}$ be the threshold parameter and $\vec{\sigma} = \{+\sigma\}^n$. Suppose that the reduced form of the basis B is denoted as $B_{reduced}$ such that $B_{reduced} = BT$ where $T \in \mathbb{Z}^{n\times n}$ is a unimodular matrix. The GGH-SBP instance is to find the reduced basis $B_{reduced}$ such that $dual_{OD}(B_{reduced}) < dual_{OD}(B)$ and $\lfloor B_{reduced}^{-1}\vec{\sigma} \rceil = \vec{0}$.*

In Definition 4.1, we generalize the lattice-reduction algorithm to be used for reducing the public basis of B. Eve may use any latice-reduction algorithm such as the LLL-algorithm or any of its variants. By solving the GGH-SBP instance, then Eve could perform effective decryption as done by Alice to obtain the plaintext $\vec{m} \in \mathbb{Z}^n$ exactly as sent by Bob to Alice.

5. Discussion

As stated in Lemma 4.1, the computed public basis B needs to satisfy the condition $\lfloor B^{-1}\vec{\sigma}\rceil \neq \vec{0}$ to avoid unauthorized decryption by Eve using the public basis B succeeds. In the GGH key generation algorithm, Alice need to check this condition other than ensuring that the public basis B is a bad basis. Although Alice does not know the exact entries of the error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$ generated by Bob, but Alice could check the condition since it only involves the vector $\vec{\sigma}$ rather than the error vector $\vec{e}$.

On the other hand, another condition that needs to be fulfilled by the public basis B is as stated in Lemma 4.2. The computed public basis B must bad enough with large dual-orthogonality defect and the chosen lattice dimension n also must large enough. This is important for ensuring that any lattice-reduction algorithm could not efficiently reduce the public basis of B in reasonable amount of time. If Eve could efficiently reduce the public basis B and the condition $\lfloor B^{-1}_{reduced}\vec{\sigma}\rceil = \vec{0}$ holds, then Eve could use the reduced basis $B_{reduced}$ as good as Alice's private basis G to perform effective decryption and eventually break the GGH cryptosystem. These strategies can be considered for strengthening the GGH cryptosystem and its variants.

6. Conclusion

In this paper, we explicitly defined the underling GGH-SBP instance of the GGH cryptosystem. By properly and explicitly defining the underlying lattice problem instances that arose from the GGH cryptosystem, more investigation on the features and behaviors of these instances could be done thoroughly. From that, we could discovered more strategies for strengthening the security of the GGH cryptosystem by preventing any potential attacks related to these instances.

Acknowledgements

The present research is partially supported by the Putra Grant with project number GP 2017/9552200. The corresponding author also want to acknowledge the Malaysian Ministry of Education and Universiti Malaysia Sabah for financial support.

References

de Barros, C. F. and Schechter, L. M. (2015). Ggh may not be dead after all. *Proceeding Series of the Brazilian Society of Computational and Applied Mathematics*, 3(1).

Galbraith, S. D. (2012). *Mathematics of public key cryptography.* Cambridge University Press.

Goldreich, O., Goldwasser, S., and Halevi, S. (1997). Public-key cryptosystems from lattice reduction problems. In *Annual International Cryptology Conference*, pages 112–131. Springer.

Goodaire, E. G. (2013). *Linear algebra: pure & applied.* World Scientific Publishing Company.

Hoffstein, J., Pipher, J., Silverman, J. H., and Silverman, J. H. (2008). *An introduction to mathematical cryptography*, volume 1. Springer.

Lee, M. S. and Hahn, S. G. (2010). Cryptanalysis of the ggh cryptosystem. *Mathematics in Computer Science*, 3(2):201–208.

Mandangan, A., Kamarulhaili, H., and Asbullah, M. A. (2018). On the underlying hard lattice problems of ggh encryption scheme. In *Cryptology and Information Security Conference 2018*, page 42.

Micciancio, D. (2001). Improving lattice based cryptosystems using the hermite normal form. In *International Cryptography and Lattices Conference*, pages 126–145. Springer.

Nguyen, P. (1999). Cryptanalysis of the goldreich-goldwasser-halevi cryptosystem from crypto'97. In *Annual International Cryptology Conference*, pages 288–304. Springer.

Paeng, S.-H., Jung, B. E., and Ha, K.-C. (2003). A lattice based public key cryptosystem using polynomial representations. In *International Workshop on Public Key Cryptography*, pages 292–308. Springer.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332.

Sipasseuth, A., Plantard, T., and Susilo, W. (2019). Enhancing goldreich, goldwasser and halevi's scheme with intersecting lattices. *Journal of Mathematical Cryptology*, 13(3-4):169–196.

Yoshino, M. and Kunihiro, N. (2012). Improving ggh cryptosystem for large error vector. In *2012 International Symposium on Information Theory and its Applications*, pages 416–420. IEEE.