Malaysian Journal of Mathematical Sciences 17(4): 673–690 (2023)
https://doi.org/10.47836/mjms.17.4.09

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

# The Efficiency of Embedding-Based Attacks on the GGH Lattice-Based Cryptosystem

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

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

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

*Received: 19 July 2022*
*Accepted: 5 October 2022*

## Abstract

The Goldreich-Goldwasser-Halevi (GGH) cryptosystem is declared broken due to the modified versions of the embedding attacks, known as Nguyen's $\sigma$, Nguyen's $2\sigma$ and Lee-Hahn's attacks. Despite using the same approach as the original embedding attack, these attacks deployed different strategies and resulted in different performances for breaking the GGH cryptosystem. In this paper, we described those strategies in detail. Moreover, we investigated the mathematical factors behind these attacks' ability and performance discrepancies. Mathematical proof examines and discusses the factors that triggered those variances. As a result, the expected lattice gap and implemented lattice dimensions are mathematically proven as the factors that significantly influenced these attacks' performance. By demonstrating how the attacks manipulated these factors, any lattice-based cryptosystem that relies on the hardness of the CVP could avoid repeating the same slipup as the GGH. Hence, precautionary action could be proactively taken to prevent it from being threatened by embedding-based attacks.

**Keywords:** lattice-based cryptosystem; post-quantum cryptography; embedding-based attacks; lattices; embedded lattices; GGH cryptosystem.

## 1 Introduction

Lattice-based cryptography appears as one of the most promising alternatives in post-quantum cryptography. Security of lattice-based cryptosystems relies on the hardness of lattice-based computational problems such as the Closest-Vector Problem (CVP), Shortest-Vector Problem (SVP) and Smallest-Basis Problem (SBP). Since the CVP is NP-hard while the SVP is NP-hard for polynomial random reductions [8], these problems are potential candidates for creating one-way functions. The lattice problems required minor modifications to create a trapdoor feature and practical implementation as a cryptosystem. Some variants of these problems become the security backbone of lattice-based cryptosystems. One of the earliest lattice-based cryptosystems is the Goldreich-Goldwasser-Halevi cryptosystem, known as the GGH cryptosystem. The security of this cryptosystem relies on the hardness of the CVP-variant, defined as GGH-CVP [10]. Keeping this problem in its original form, various attacks launched toward the GGH cryptosystem certainly failed. Among all these attacks, the most promising attack was the embedding attack. Instead of solving the GGH-CVP, this attack solves the easier version of this problem defined as GGH-SVP, a variant of the Shortest-Vector Problem (SVP). Although both problems are hard, the SVP is considered easier than the CVP [6]. By reducing the underlying GGH-CVP to its corresponding GGH-SVP, the embedding attack worked better than other attacks on the GGH cryptosystem [5]. However, this embedding attack can be avoided by increasing the implemented lattice dimension to $250$ and beyond.

In 1999, [13] discovered a strategy that unleashed the embedding attack's full potential for breaking the GGH cryptosystem. Using this strategy, the derived GGH-CVP can be simplified to a new variant, defined as the Nguyen$_{GGH}$-CVP. Like the original embedding attack, Nguyen's embedding attack also works by reducing the Nguyen$_{GGH}$-CVP to its corresponding Nguyen$_{GGH}$-SVP. Solving the Nguyen$_{GGH}$-SVP would immediately solve the corresponding Nguyen$_{GGH}$-CVP, making the GGH cryptosystem broken. Nguyen's embedding attack performed more efficiently for breaking the GGH cryptosystem in the lattice dimensions up to $350$. This attack can only be avoided by increasing the implemented lattice dimension to $400$ and beyond. About 10 years later, another embedding-based attack was proposed by [9], known as Lee-Hahn's embedding attack. This attack simplifies the underlying Nguyen$_{GGH}$-CVP to a simpler form, defined as the Lee-Hahn$_{GGH}$-CVP, which later is reduced to its corresponding Lee-Hahn$_{GGH}$-SVP. Solving the Lee-Hahn$_{GGH}$-SVP would immediately solve the Lee-Hahn$_{GGH}$-CVP and consequently break the GGH cryptosystem in the lattice dimensions of $400$ and beyond [9].

Despite using the same approach, Nguyen's and Lee-Hahn's embedding attacks performed differently compared to the original embedding attacks. One of the main factors is the value of the threshold parameter $\sigma \in \mathbb{N}$. Nguyen's embedding attacks consist of two types, known as Nguyen's $\sigma$ and Nguyen's $2\sigma$ embedding attacks which performed differently for breaking the GGH cryptosystem. Therefore, this study is conducted to investigate the reasons behind these occurrences. The outcome of this study could be beneficial to any lattice-based cryptosystems, especially those that rely on the CVP-based variant as a security backbone to hinder any possible threat by the embedding-based attacks. Due to its simplicity, the GGH cryptosystem was considered the most practical lattice-based cryptosystem [12]. Unfortunately, it receives less attention than other lattice-based cryptosystems since the successful attacks by the Nguyen's and Lee-Hahn's embedding attacks. If the security of the GGH cryptosystem can be upgraded to make it immune to those attacks, there is hope for the GGH cryptosystem to survive. As stated by [14], the general idea behind the GGH cryptosystem is still worthwhile. The simplicity of the GGH cryptosystem also should be appreciated. Therefore, the remedy to upgrade its security is worth exploring and discovering. Recently, there is current interest in this cryptosystem to combat the embedding-based attacks and bring the GGH cryptosystem back to the mainstream arena [11, 15, 1].

This paper is organised as follows. The next section provides a light introduction to the GGH cryptosystem, including the lattice-based computational problems underlying this cryptosystem. Then, we explain the details of the embedding attacks and their improved version in Section 3. The investigation is done in Section 4. This paper is concluded in Section 5, with suggestions for future research that could be derived from this study.

## 2 GGH Lattice-based Cryptosystem

GGH cryptosystem is one of the earliest cryptosystems developed based on the lattice. Lattice is defined as follows:

**Definition 2.1.** [2] *For $m, n \in \mathbb{N}$ and $m \geq n$, let $B = \left\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\right\}$ be a set of linearly independent vectors $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^m$. 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 $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ with integer scalars, i.e.,*

$$\mathcal{L} = L(B) = \left\{ \sum_{i=1}^{n} a_i \vec{b}_i \;\middle|\; \vec{b}_i \in B \text{ and } a_i \in \mathbb{Z}, \forall i = 1, 2, \ldots, n \right\}. \tag{1}$$

The matrix $B$ is called a basis of lattice $\mathcal{L}$ if its' columns are linearly independent and it spans the lattice $\mathcal{L}$. If $m = n$, then the set $B$ can be represented as a square matrix $B \in \mathbb{R}^{n \times n}$ with vectors $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$ as its columns. With a square matrix $B$ as the basis, then the lattice $L(B)$ is referred to as a full-rank lattice.

**Theorem 2.1.** [7] *For $n \in \mathbb{N}$, a square matrix $G \in \mathbb{R}^{n \times n}$ is invertible if and only if its columns $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_n \in \mathbb{R}^n$ are linearly independent. The lattice $\mathcal{L}$ could be spanned by infinitely many lattice bases and these bases are mathematically related by unimodular matrix.*

**Definition 2.2.** [8] *For $n \in \mathbb{N}$, $U \in \mathbb{Z}^{n \times n}$ is called a unimodular matrix if $\det(U) = \pm 1$.*

**Lemma 2.1.** [5] *For $n \in \mathbb{N}$, 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 $G = BU$.*

**Proposition 2.1.** [5] *For $n \in \mathbb{N}$, suppose that $G, B \in \mathbb{R}^{n \times n}$ be bases of the lattice $\mathcal{L}$ where $L(G) = L(B) = \mathcal{L}$. The value of the $\det(\mathcal{L})$ is an invariant, i.e., $\det(\mathcal{L}) = \det(L(G)) = \det(L(B))$ where $\det(L(G)) = |\det(G)|$ and $\det(L(B)) = |\det(B)|$.*

**Definition 2.3.** [13] *For $n \in \mathbb{N}$, let $\mathcal{L} \subset \mathbb{R}^n$ be a full-rank lattice. The $i$-th minimum of the lattice $\mathcal{L}$, denoted as $\lambda_i(\mathcal{L}) \in \mathbb{R}^+$, is the radius of the smallest sphere centred at the origin that is containing $i$ linearly independent lattice vectors.*

From the successive minima $\lambda_1(\mathcal{L})$ and $\lambda_2(\mathcal{L})$, the lattice gap of the lattice $\mathcal{L}$, denoted as $gap(\mathcal{L}) \in \mathbb{R}^+$, can be computed as follows:

**Definition 2.4.** [13] *For $n \in \mathbb{N}$, 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., $gap(\mathcal{L}) = \dfrac{\lambda_2(\mathcal{L})}{\lambda_1(\mathcal{L})} \in \mathbb{R}^+$.*

The GGH cryptosystem is described in the following algorithms [5]:

**Algorithm 1** Key generation algorithm of the GGH cryptosystem is done by the recipient.

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

**Algorithm 2** Encryption algorithm of the GGH cryptosystem is done by the sender.

**Input:** Public key $(B, n, \sigma)$.
**Output:** Ciphertext $\vec{c} \in \mathbb{R}^n$.
1: Generate an error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$.
2: Generate a plaintext vector $\vec{m} \in \mathbb{Z}^n$.
3: Encrypt the plaintext as

$$\vec{c} = B\vec{m} + \vec{e}. \tag{2}$$

**Algorithm 3** Decryption algorithm of the GGH cryptosystem is done by the recipient.

**Input:** Ciphertext $\vec{c} \in \mathbb{R}^n$ from the sender and private key $(G, U)$.
**Output:** Plaintext $\vec{m} \in \mathbb{Z}^n$.
1: Compute $\vec{x} \in \mathbb{R}^n$ as $\vec{x} = G^{-1}\vec{c}$.
2: For all $i = 1, \ldots, n$, round each entry $x_i \in \vec{x}$ to the nearest integer $\lfloor x_i \rceil \in \mathbb{Z}$ such that $|x_i - \lfloor x_i \rceil| \leq \frac{1}{2}$ and form an integer vector $\lfloor \vec{x} \rceil \in \mathbb{Z}^n$.
3: Decrypt the ciphertext as

$$\vec{m} = U \lfloor \vec{x} \rceil \ . \tag{3}$$

## 3 Embedding-Based Attacks on The GGH Cryptosystem

The GGH cryptosystem is developed with security dependency on the variant of the CVP, defined as the GGH-CVP. The CVP is defined as follows:

**Definition 3.1.** [5] *For $n \in \mathbb{N}$, let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice. Given a basis for the lattice $\mathcal{L}$ and a target vector $\vec{w} \in \mathbb{R}^n$, the Closest-Vector Problem (CVP) is to find a non-zero vector $\vec{x} \in \mathcal{L}$ such that $\|\vec{x} - \vec{w}\|$ is minimal.*

We explicitly define the GGH-CVP as follows:

**Definition 3.2.** *(GGH-CVP) For $n, \sigma \in \mathbb{N}$, let $B \in \mathbb{R}^{n\times n}$ be a basis for the 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 $\sigma$, find the lattice vector $\vec{v}$ such that $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$.*

One of the alternatives to breaking the security of lattice-based cryptosystems is solving the underlying lattice-based computational problems. Embedding attacks work based on this approach. Instead of directly solving the underlying GGH-CVP, the embedding attacks reduce this problem to its corresponding SVP variant, defined as the GGH-SVP. The SVP is defined as follows:

**Definition 3.3.** [5] *For $n \in \mathbb{N}$, 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 $x$ is minimal, i.e., $\|\vec{x}\| = \lambda_1(\mathcal{L})$.*

We explicitly define the GGH-SVP as follows:

**Definition 3.4.** *(GGH-SVP) For $n \in \mathbb{N}$, let $B \in \mathbb{R}^{n\times n}$ with columns $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$ be a basis for the lattice $L(B) \subset \mathbb{R}^n, \vec{c} \in \mathbb{R}^n$ be a ciphertext an $X = \begin{bmatrix} \vec{c} & \vec{b_1} & \vec{b_2} & \ldots & \vec{b_n} \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}$ be a basis for the lattice $L'(X) \subset \mathbb{R}^{n+1}$. Given $B$ and $\vec{c}$, find a non-zero vector in the lattice $L'(X)$, denoted as $\vec{\delta}_1 \in L'(X)$, such that $\lambda_1(L'(X)) = \|\vec{\delta_1}\|$ where $\lambda_1(L'(X))$ is the first minimum of the lattice $L'(X)$.*

The SVP and its variants can be solved or approximated using lattice-reduction algorithms such as the LLL and BKZ algorithms. The lattice gap is one of the factors that could influence the performance of the lattice-reduction algorithm. Experimentally, the larger the lattice gap is, the more efficient the lattice-reduction algorithm could perform for solving the underlying SVP [3].

### 3.1 Original embedding attacks

The original embedding attacks consists of a sequence of two stages, namely the reduction and solution stages. In the reduction stage, the underlying GGH-CVP in n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$ is reduced to its corresponding GGH-SVP in an $(n+1)$-dimensional lattice $\mathcal{L}' \subset \mathbb{R}^{n+1}$. Finally, the solution stage works to solve the derived GGH-SVP using lattice-reduction algorithms. Consider the public basis $B \in \mathbb{R}^{n\times n}$ and the ciphertext $\vec{c} \in \mathbb{R}^n$. In the reduction stage, the vector $\begin{bmatrix} \vec{e} \\ 1 \end{bmatrix} \in \mathbb{R}^{n+1}$ is embedded into the basis $B$ to form a new basis $X = \begin{bmatrix} \vec{c} & \vec{b_1} & \vec{b_2} & \ldots & \vec{b_n} \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}$ for an $(n+1)$-dimensional lattice $L'(X) \subset \mathbb{R}^{n+1}$. The lattice $L'(X)$ is referred to as embedded lattice. [2] stated that, the new lattice $\mathcal{L}'$ is expected to contain a shortest vector $\vec{e}' = \begin{bmatrix} \vec{e} \\ \eta \end{bmatrix} \in L'$ where $\|\vec{e}\| \leq \frac{\lambda_1(\mathcal{L})}{2}$ and $\eta = \|\vec{e}\|$. Thus, a short vector in the lattice $\mathcal{L}'$ can be defined as follows:

**Definition 3.5.** *For $n \in \mathbb{N}$, let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice, $\vec{c}, \vec{e} \in \mathbb{R}^n$ and $\vec{v} \in \mathcal{L}$ such that $\vec{c} = \vec{v} + \vec{e}$. Suppose that $\mathcal{L}' \subset \mathbb{R}^{n+1}$ be an embedded lattice that is derived from the lattice $\mathcal{L}$ and $\vec{e}' \in \mathcal{L}'$ be a non-zero vector. Then, $\vec{e}'$ is considered as a short vector in the lattice $\mathcal{L}'$ if $\|\vec{e}'\| < \|\vec{e}\| + \eta$ where $\eta \in \mathbb{N}$ and $\eta < \|\vec{e}\|$.*

**Lemma 3.1.** *For $n,\ \sigma \in \mathbb{N}$, let $B \in \mathbb{R}^{n\times n}$ with columns $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$ be a basis for the lattice $L(B) \subset \mathbb{R}^n, \vec{c} \in \mathbb{R}^n, \vec{e} \in \{-\sigma, +\sigma\}^n$ and $\vec{v} \in L(B)$ such that $\vec{c} = \vec{v} + \vec{e}$. If $X = \begin{bmatrix} \vec{c} & \vec{b_1} & \vec{b_2} & \ldots & \vec{b_n} \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}$ is a basis for the embedded lattice $L'(X) \subset \mathbb{R}^{n+1}$, then $\begin{bmatrix} \vec{e} \\ 1 \end{bmatrix}$ is a short vector in the lattice $L'(X)$.*

The original embedding attacks consider the vector $\begin{bmatrix} \vec{e} \\ 1 \end{bmatrix}$ as the shortest non-zero vector in the embedded lattice $L'(X)$. Finding such vector is the GGH-SVP. Thus, the solution stage is executed to solve the derived GGH-SVP by reducing the basis $X$ using lattice-reduction algorithm.

**Lemma 3.2.** *For $n \in \mathbb{N}$, let $L'(X) \subset \mathbb{R}^{n+1}$ be a lattice, $\lambda_1(L'(X))$ denotes the first minimum of the lattice $L'(X), \vec{\delta}_1 \in L'(X)$ and $\vec{e} \in \mathbb{R}^n$ be an error vector of the GGH-CVP. Suppose that the solution of*

*the GGH-SVP is obtained as* $\vec{\delta}_1 \in L'(X)$ *such that* $\lambda_1(L'(X)) = \|\vec{\delta}_1\|$. *If* $\vec{\delta}_1 = \begin{bmatrix} \vec{e} \\ 1 \end{bmatrix}$, *then the solution for the GGH-CVP can be obtained.*

**Lemma 3.3.** *For* $n, \sigma \in \mathbb{N}$, *let* $B \in \mathbb{Z}^{n \times n}$ *be a basis for the lattice* $\mathcal{L} \subset \mathbb{R}^n$, $\vec{c} \in \mathbb{Z}^n$ *be a ciphertext vector,* $\vec{m} \in \mathbb{Z}^n$ *be a plaintext vector and* $\vec{e} \in \{-\sigma, +\sigma\}^n$ *be an error vector such that* $\vec{c} = B\vec{m} + \vec{e}$. *The vector* $\vec{v} = B\vec{m} \in \mathcal{L}$ *is the solution of the GGH-CVP. If the GGH-CVP is solved, then the GGH cryptosystem is broken.*

### 3.2 Nguyen's embedding attacks

The Nguyen's embedding attack has two additional stages prior to its reduction and solution stages, named as elimination and simplification stages respectively. The elimination stage works to eliminate the error vector $\vec{e}$ from the encryption Equation (2). Using public parameters $n, \sigma \in \mathbb{N}$, a vector $\vec{s} \in \{\sigma\}^n$ is formed and inserted into the encryption Equation (2) as $\vec{c} + \vec{s} = B\vec{m} + \vec{e} + \vec{s}$. Note that, the following equations hold,

$$\frac{\vec{c} + \vec{s} - B\vec{m}}{\sigma} = \frac{\vec{e} + \vec{s}}{\sigma}, \tag{4}$$

$$\frac{\vec{c} + \vec{s} - B\vec{m}}{2\sigma} = \frac{\vec{e} + \vec{s}}{2\sigma}. \tag{5}$$

Since $\vec{e} \in \{-\sigma, +\sigma\}^n$ and $\vec{s} \in \{\sigma\}^n$, then $\vec{e} + \vec{s} \in \{0,\ 2\sigma\}^n$. Thus, $\dfrac{\vec{e} + \vec{s}}{\sigma} \in \{0,\ 2\}^n$ and $\dfrac{\vec{e} + \vec{s}}{2\sigma} \in \{0,\ 1\}^n$. Since,

$$\frac{\vec{e} + \vec{s}}{\sigma}, \frac{\vec{e} + \vec{s}}{2\sigma} \in \mathbb{Z}^n,$$

then,

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

as well. Consequently, the following congruences hold,

$$\vec{c} + \vec{s} \equiv B\vec{m} \pmod{\sigma}, \tag{6}$$

$$\vec{c} + \vec{s} \equiv B\vec{m} \pmod{2\sigma}. \tag{7}$$

Clearly, the elimination stage had successfully eliminated the error vector $\vec{e}$ from the encryption equation. The encryption Equation (2) which originally has two unknown vectors $\vec{m}$ and $\vec{e}$ has been transformed to the congruences (6) and (7) which contain only a single unknown vector $\vec{m}$ respectively. Based on the congruences (6) and (7), the Nguyen's embedding attack is launched using two different moduli namely $\sigma$ and $2\sigma$. [13] proved that the congruences (6) and (7) are solvable with very few solutions. 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 congruences (6) and (7) respectively are obtained as the following,

$$\vec{m} \equiv B^{-1}(\vec{c} + \vec{s}) \pmod{\sigma}, \tag{8}$$

$$\vec{m} \equiv B^{-1}(\vec{c} + \vec{s}) \pmod{2\sigma}. \tag{9}$$

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

$$\vec{m} \equiv \vec{m}_\sigma \pmod{\sigma}, \tag{10}$$
$$\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}. \tag{11}$$

Once the vectors $\vec{m}_\sigma$ and $\vec{m}_{2\sigma}$ are obtained, the Nguyen's embedding attack moves to its simplification stage. The vectors $\vec{m}_\sigma$ and $\vec{m}_{2\sigma}$ are multiplied with the public basis $B$ respectively. Then, the vectors $B\vec{m}_\sigma, B\vec{m}_{2\sigma} \in \mathbb{R}^n$ are respectively inserted into the encryption Equation (2) as follows,

$$\vec{c} - B\vec{m}_\sigma = B(\vec{m} - \vec{m}_\sigma) + \vec{e}, \tag{12}$$
$$\vec{c} - B\vec{m}_{2\sigma} = B(\vec{m} - \vec{m}_{2\sigma}) + \vec{e}. \tag{13}$$

The congruences (10) and (11) imply the existence of $\vec{k}_1, \vec{k}_2 \in \mathbb{Z}^n$ such that,

$$\vec{m} - \vec{m}_\sigma = \sigma\vec{k}_1, \tag{14}$$
$$\vec{m} - \vec{m}_{2\sigma} = 2\sigma\vec{k}_2. \tag{15}$$

Substituting Equation (14) into congruence (15) and Equation (12) into congruence (13) respectively yield,

$$\frac{\vec{c} - B\vec{m}_\sigma}{\sigma} = B\vec{k}_1 + \frac{\vec{e}}{\sigma}, \tag{16}$$
$$\frac{\vec{c} - B\vec{m}_{2\sigma}}{2\sigma} = B\vec{k}_2 + \frac{\vec{e}}{2\sigma}. \tag{17}$$

For simplicity, denote $\dfrac{\vec{c} - B\vec{m}_\sigma}{\sigma} = \vec{p}_1 \in \mathbb{R}^n$ and $\dfrac{\vec{c} - B\vec{m}_{2\sigma}}{2\sigma} = \vec{p}_2 \in \mathbb{R}^n$. Since $\vec{c}, B, \vec{m}_\sigma, \vec{m}_{2\sigma}$ and $\sigma$ are known information, then $\vec{p}_1$ and $\vec{p}_2$ are known vectors. Note that, $B$ is a basis for the lattice $L(B) \subset \mathbb{R}^n$ and $\vec{k}_1, \vec{k}_2 \in \mathbb{Z}^n$, then $B\vec{k}_1 = \vec{q}_1 \in L(B)$ and $B\vec{k}_2 = \vec{q}_2 \in L(B)$. Since $\vec{k}_1$ and $\vec{k}_2$ are unknown vectors, then $\vec{q}_1$ and $\vec{q}_2$ are also unknown lattice vectors. Although the value of the parameter $\sigma$ is known, the arrangement of the entries $-\sigma$ and $+\sigma$ in the error vector $\vec{e} \in \{-\sigma, +\sigma\}^n$ is privately determined by Bob. Thus, the following vectors are unknown vectors,

$$\vec{\varepsilon}_1 = \frac{\vec{e}}{\sigma} \in \left\{-\frac{\sigma}{\sigma}, +\frac{\sigma}{\sigma}\right\}^n = \{-1, 1\}^n,$$
$$\vec{\varepsilon}_2 = \frac{\vec{e}}{2\sigma} \in \left\{-\frac{\sigma}{2\sigma}, +\frac{\sigma}{2\sigma}\right\}^n = \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n.$$

Now, Equations (16) and (17) can be simply rewritten as follows,

$$\vec{p}_1 = \vec{q}_1 + \vec{\varepsilon}_1, \tag{18}$$
$$\vec{p}_2 = \vec{q}_2 + \vec{\varepsilon}_2, \tag{19}$$

where $\vec{p}_1, \vec{p}_2 \in \mathbb{R}^n$, $\vec{q}_1, \vec{q}_2 \in L(B)$, $\vec{\varepsilon}_1 \in \{-1, 1\}^n$ and $\vec{\varepsilon}_2 \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$.

**Proposition 3.1.** *For $n, \sigma \in \mathbb{N}$ where $n, \sigma > 1$, let $B \in \mathbb{R}^{n\times n}$ be a basis for the lattice $L(B) \subset \mathbb{R}^n$, $\vec{p}_1, \vec{p}_2 \in \mathbb{R}^n$ such that $\vec{p}_1 = \vec{q}_1 + \vec{\varepsilon}_1$ and $\vec{p}_2 = \vec{q}_2 + \vec{\varepsilon}_2$ where $\vec{q}_1, \vec{q}_2 \in L(B)$, $\vec{\varepsilon}_1 = \{-1, 1\}^n$ and $\vec{\varepsilon}_2 \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$. If the GGH-CVP distance is $\|\vec{c} - \vec{v}\| = \sigma\sqrt{n}$, then $\|\vec{p}_2 - \vec{q}_2\| < \|\vec{p}_1 - \vec{q}_1\| < \|\vec{c} - \vec{v}\|$ where $\vec{c}, \vec{v} \in \mathbb{Z}^n$.*

*Proof.* Given that $\vec{p}_1 = \vec{q}_1 + \vec{\varepsilon}_1$ and $\vec{p}_2 = \vec{q}_2 + \vec{\varepsilon}_2$. These imply that $\vec{p}_1 - \vec{q}_1 = \vec{\varepsilon}_1$ and $\vec{p}_2 - \vec{q}_2 = \vec{\varepsilon}_2$. Hence,

$$\|\vec{p}_1 - \vec{q}_1\| = \|\vec{\epsilon}_1\| = \sqrt{\underbrace{(\pm 1)^2 + (\pm 1)^2 + \ldots + (\pm 1)^2}_{\text{added } n \text{ times}}} = \sqrt{n},$$

and

$$\|\vec{p}_2 - \vec{q}_2\| = \|\vec{\epsilon}_2\| = \sqrt{\underbrace{\left(\pm\frac{1}{2}\right)^2 + \left(\pm\frac{1}{2}\right)^2 + \ldots + \left(\pm\frac{1}{2}\right)^2}_{\text{added } n \text{ times}}} = \frac{\sqrt{n}}{2}.$$

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

$$\frac{\sqrt{n}}{2} < \sqrt{n} < \sigma\sqrt{n}.$$

This implies that,

$$\|\vec{p}_2 - \vec{q}_2\| < \|\vec{p}_1 - \vec{q}_1\| < \|\vec{c} - \vec{v}\|.$$

□

Observe that, Equations (18) and (19) are similar to equation $\vec{c} = \vec{v} + \vec{e}$ which is the GGH-CVP with $\vec{c} \in \mathbb{R}^n$, $\vec{v} \in L(B)$ and $\vec{e} \in \{-\sigma, +\sigma\}^n$. That means, new CVP variants could be derived from Equations (18) and (19). With shorter distances $\|\vec{p}_1 - \vec{q}_1\|$ and $\|\vec{p}_2 - \vec{q}_2\|$, the derived CVP variants by the Nguyen's embedding attacks are considered simpler than the GGH-CVP. These variants are addressed as the Nguyen$_{GGH}$-CVP1 and Nguyen$_{GGH}$-CVP2 respectively. We define these variants as follows:

**Definition 3.6.** *For $n \in \mathbb{N}$, let $B \in \mathbb{R}^{n\times n}$ be a basis for the lattice $L(B) \subset \mathbb{R}^n, \vec{p}_1, \vec{p}_2 \in \mathbb{R}^n$ such that $\vec{p}_1 = \vec{q}_1 + \vec{\varepsilon}_1$ and $\vec{p}_2 = \vec{q}_2 + \vec{\varepsilon}_2$, where $\vec{q}_1, \vec{q}_2 \in L(B), \vec{\varepsilon}_1 \in \{-1, 1\}^n$ and $\vec{\varepsilon}_2 \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$,*

1. *(Nguyen$_{GGH}$-CVP1) Given $B$ and $\vec{p}_1$, find $\vec{q}_1 \in L(B)$ such that $\|\vec{p}_1 - \vec{q}_1\| = \sqrt{n}$.*
2. *(Nguyen$_{GGH}$-CVP2) Given $B$ and $\vec{p}_2$, find $\vec{q}_2 \in L(B)$ such that $\|\vec{p}_2 - \vec{q}_2\| = \frac{\sqrt{n}}{2}$.*

Now, the attacks move to the reduction stage. Consider the vectors $\vec{p}_1, \vec{p}_2 \in \mathbb{R}^n$ and the basis $B \in \mathbb{R}^{n\times n}$ as defined in Definition 3.6. The vector $\begin{bmatrix}\vec{p_1}\\ 1\end{bmatrix} \in \mathbb{R}^{n+1}$ is embedded into the basis $B$ to form a basis $Y_1 = \begin{bmatrix}\vec{p_1} & \vec{b_1} & \vec{b_2} & \ldots & \vec{b_n}\\ 1 & 0 & 0 & \ldots & 0\end{bmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}$ for the lattice $L'(Y_1) \subset \mathbb{R}^{n+1}$. On the other hand, the vector $\begin{bmatrix}\vec{p_2}\\ 1\end{bmatrix} \in \mathbb{R}^{n+1}$ is embedded into the basis $B$ to form a basis $Y_2 = \begin{bmatrix}\vec{p_2} & \vec{b_1} & \vec{b_2} & \ldots & \vec{b_n}\\ 1 & 0 & 0 & \ldots & 0\end{bmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}$ for the other lattice $L'(Y_2) \subset \mathbb{R}^{n+1}$. The following lemma describes the expected short vectors in the embedded lattices $L'(Y_1)$ and $L'(Y_2)$.

**Lemma 3.4.** *For $n \in \mathbb{N}$, let $B \in \mathbb{R}^{n\times n}$ with columns $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$ be a basis for the lattice $L(B) \subset \mathbb{R}^n, \vec{p}_1, \vec{p}_2 \in \mathbb{R}^n$ such that $\vec{p}_1 = \vec{q}_1 + \vec{\varepsilon}_1$ and $\vec{p}_2 = \vec{q}_2 + \vec{\varepsilon}_2$ where $\vec{q}_1, \vec{q}_2 \in L(B), \vec{\varepsilon}_1 \in \{-1, 1\}^n$*

*and* $\vec{\varepsilon}_2 \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$. *If* $Y_1 = \begin{bmatrix} \vec{p_1} & \vec{b_1} & \vec{b_2} & \dots & \vec{b_n} \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}$ *and* $Y_2 = \begin{bmatrix} \vec{p_2} & \vec{b_1} & \vec{b_2} & \dots & \vec{b_n} \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}$ *are bases for the lattices* $L'(Y_1)$ *and* $L'(Y_2)$ *respectively, then* $\begin{bmatrix} \vec{\epsilon_1} \\ 1 \end{bmatrix}$ *and* $\begin{bmatrix} \vec{\epsilon_2} \\ 1 \end{bmatrix}$ *are short vectors in the lattices* $L'(Y_1)$ *and* $L'(Y_2)$ *respectively.*

Searching for the short vectors $\begin{bmatrix} \vec{\epsilon_1} \\ 1 \end{bmatrix} \in L'(Y_1)$ and $\begin{bmatrix} \vec{\epsilon_2} \\ 1 \end{bmatrix} \in L'(Y_2)$ are SVP variants. These variants are defined as the Nguyen$_{GGH}$-SVP1 and Nguyen$_{GGH}$-SVP2 respectively as follows:

**Definition 3.7.** *For* $n \in \mathbb{N}$, *let* $B \in \mathbb{R}^{n \times n}$ *with columns* $\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n \in \mathbb{R}^n$ *be a basis for the lattice* $L(B) \subset \mathbb{R}^n$, *while* $Y_1 = \begin{bmatrix} \vec{p_1} & \vec{b_1} & \vec{b_2} & \dots & \vec{b_n} \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}$ *and* $Y_2 = \begin{bmatrix} \vec{p_2} & \vec{b_1} & \vec{b_2} & \dots & \vec{b_n} \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}$ *be bases for the lattices* $L'(Y_1)$ *and* $L'(Y_2)$ *respectively,* $\vec{p}_1, \vec{p}_2 \in \mathbb{R}^n$ *such that* $\vec{p}_1 = \vec{q}_1 + \vec{\varepsilon}_1$ *and* $\vec{p}_2 = \vec{q}_2 + \vec{\varepsilon}_2$ *where* $\vec{q}_1, \vec{q}_2 \in L(B), \vec{\varepsilon}_1 \in \{-1, 1\}^n$ *and* $\vec{\varepsilon}_2 \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$,

1. (*Nguyen$_{GGH}$-SVP1*) *Given* $B$ *and* $\vec{p}_1$, *find a non-zero vector* $\vec{\delta}_2 \in L'(Y_1)$ *such that* $\lambda_1(L'(Y_1)) = \delta_2$, *and*
2. (*Nguyen$_{GGH}$-SVP2*) *Given* $B$ *and* $\vec{p}_2$, *find a non-zero vector*$\vec{\delta}_3 \in L'(Y_2)$ *such that* $\lambda_1(L'(Y_2)) = \delta_3$,

*where* $\lambda_1(L'(Y_1)), \lambda_1(L'(Y_2)) \in \mathbb{R}^+$ *denote the first minimum of the embedded lattices* $L'(Y_1)$ *and* $\lambda_1(L'(Y_2))$ *respectively.*

Finally, Nguyen's embedding attacks move to the solution stage that works to solve the derived Nguyen$_{GGH}$-SVP1 and Nguyen$_{GGH}$-SVP2. BKZ and pruning algorithms reduce the bases $Y_1$ and $Y_2$. The following lemma states that the Nguyen$_{GGH}$-CVP1 and Nguyen$_{GGH}$-CVP2 are solvable once the solution for the derived Nguyen$_{GGH}$-SVP1 and Nguyen$_{GGH}$-SVP2 are respectively obtained:

**Lemma 3.5.** *For* $n \in \mathbb{N}$, *let* $L'(Y_1), L'(Y_2) \subset \mathbb{R}^{n+1}$ *be lattices,* $\vec{\varepsilon}_1, \vec{\varepsilon}_2 \in \mathbb{R}^n$ *be the error vectors in the Nguyen$_{GGH}$-CVP1 and Nguyen$_{GGH}$-CVP2 respectively and* $\lambda_1(L'(Y_1)), \lambda_1(L'(Y_2)) \in \mathbb{R}^+$ *denote the first minimum of the lattices* $L'(Y_1)$ *and* $L'(Y_2)$ *respectively. Suppose that, the solutions of the Nguyen$_{GGH}$-SVP1 and Nguyen$_{GGH}$-SVP2 are obtained as* $\vec{\delta}_2 \in L'(Y_1)$ *and* $\vec{\delta}_3 \in L'(Y_2)$ *respectively such that* $\lambda_1(L'(Y_1)) = \|\vec{\delta}_2\|$ *and* $\lambda_1(L'(Y_2)) = \|\vec{\delta}_3\|$. *If* $\vec{\delta}_2 = \begin{bmatrix} \vec{\epsilon_1} \\ 1 \end{bmatrix}$ *and* $\vec{\delta}_3 = \begin{bmatrix} \vec{\epsilon_2} \\ 1 \end{bmatrix}$, *then the solution for the Nguyen$_{GGH}$-CVP1 and Nguyen$_{GGH}$-CVP2 can be obtained.*

**Lemma 3.6.** *If the Nguyen$_{GGH}$-CVP1 and Nguyen$_{GGH}$-CVP2 are solved, then the GGH cryptosystem is broken.*

### 3.3 Lee-Hahn's embedding attack

Lee-Hahn's embedding attack consists of a sequence of four stages, namely the guessing, simplification, reduction and solution stages respectively. In the GGH Internet Challenges [4], the plaintext vectors $\vec{m} \in \mathbb{Z}^n$ have entries $m_i \in [-128,\ 127]$ for all $i = 1, \dots, n$ and the used threshold

parameter is $\sigma = 3$. These imply that, the partially decrypted plaintext $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^n$ is $\vec{m}_6 \in \mathbb{Z}_6^n$. Due to the modulo reduction with modulus 6, then $m_i' \in [0,5]$ where $m_i' \in \vec{m}_6$ for all $i = 1, \ldots, n$. The partially decrypted plaintext $\vec{m}_6 \in \mathbb{Z}_6^{400}$ are published in [13]. Using this information, the guessing stage of Lee-Hahn's embedding attack managed to guess the first $k \in \mathbb{N}$ actual plaintext values from $\vec{m} \in \mathbb{Z}^{400}$. From the obtained first $k$-entries of the plaintext $\vec{m} \in \mathbb{Z}^n$, the attack is moving to its simplification stage where the plaintext $\vec{m}$, partially decrypted plaintext $\vec{m}_{2\sigma}$ and public basis $B$ are all divided into two blocks based on the number $k$.

The plaintext $\vec{m} \in \mathbb{Z}^n$ is represented as $\vec{m} = \begin{bmatrix} \vec{m}^1 \\ \vec{m}^2 \end{bmatrix} \in \mathbb{Z}^n$ where $\vec{m}^1 = \begin{bmatrix} m_1 \\ \vdots \\ m_k \end{bmatrix} \in \mathbb{Z}^k$ and $\vec{m}^2 = \begin{bmatrix} m_{k+1} \\ \vdots \\ m_n \end{bmatrix} \in \mathbb{Z}^{n-k}$. The first sub-vector $\vec{m}^1$ contains the known first $k$-entries of the plaintext $\vec{m}$ and the second sub-vector $\vec{m}^2$ contains the remaining unknown entries of the plaintext $\vec{m}$. On the other hand, the partially decrypted plaintext $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^n$ is represented as $\vec{m}_{2\sigma} = \begin{bmatrix} \vec{m_{2\sigma}}^1 \\ \vec{m_{2\sigma}}^2 \end{bmatrix} \in \mathbb{Z}^n$ where $\vec{m_{2\sigma}}^1 = \begin{bmatrix} m_1' \\ \vdots \\ m_k' \end{bmatrix} \in \mathbb{Z}_{2\sigma}^k$ and $\vec{m_{2\sigma}}^2 = \begin{bmatrix} m_{k+1}' \\ \vdots \\ m_n' \end{bmatrix} \in \mathbb{Z}_{2\sigma}^{n-k}$ while the public basis $B \in \mathbb{R}^{n \times n}$ is represented as $B = \begin{bmatrix} B_1 & B_2 \end{bmatrix}$ where $B_1 = \begin{bmatrix} \vec{b}_1 & \cdots & \vec{b}_k \end{bmatrix} \in \mathbb{R}^{n \times k}$ and $B_2 = \begin{bmatrix} \vec{b}_{k+1} & \vec{b}_{k+2} & \cdots & \vec{b}_n \end{bmatrix} \in \mathbb{R}^{n \times (n-k)}$. As described in [9], $B_2$ is a basis for the lattice $L^*(B_2) \subset \mathbb{R}^n$ which is a sub-lattice for the original lattice $L(B) \subset \mathbb{R}^n$. Now, the encryption Equation (2) is rewritten as follows,

$$\vec{c} - B_1 \vec{m}^1 = B_2 \vec{m}^2 + \vec{e}. \tag{20}$$

The sub-basis $B_2$ and the sub-vector $\vec{m}_{2\sigma}^2$ are multiplied as $B_2 \vec{m}_{2\sigma}^2 \in \mathbb{R}^n$ and then inserted into Equation (20) as follows,

$$\vec{c} - B_1 \vec{m}^1 - B_2 \vec{m}_{2\sigma}^2 = B_2 \left( \vec{m}^2 - \vec{m}_{2\sigma}^2 \right) + \vec{e}. \tag{21}$$

Since $\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}$, then $\vec{m}^2 \equiv \vec{m}_{2\sigma}^2 \pmod{2\sigma}$ holds as well for $\vec{m}^2 \in \vec{m}$ and $\vec{m}_{2\sigma}^2 \in \vec{m}_{2\sigma}$. This implies that, there exists $\vec{h} \in \mathbb{Z}^{n-k}$ such that

$$\vec{m}^2 - \vec{m}_{2\sigma}^2 = 2\sigma \vec{h}. \tag{22}$$

Substituting Equation (22) into Equation (21) yields,

$$\frac{\vec{c} - B_1 \vec{m}^1 - B_2 \vec{m}_{2\sigma}^2}{2\sigma} = B_2 \vec{h} + \frac{\vec{e}}{2\sigma}. \tag{23}$$

For simplicity, denote $\dfrac{\vec{c} - B_1 \vec{m}_1 - B_2 \vec{m}_{2\sigma}^2}{2\sigma} = \vec{t} \in \mathbb{R}^n$. Since the vectors $\vec{c}, B_1 \vec{m}_1, B_2 \vec{m}_{2\sigma}^2 \in \mathbb{R}^n$ and parameter $\sigma$ are known, then $\vec{t}$ is a known vector. Since $B_2 \in \mathbb{R}^{n \times (n-k)}$ is a basis for the sub-lattice $L^*(B_2)$ and $\vec{h} \in \mathbb{Z}^{n-k}$ is an unknown integer vector, then $B_2 \vec{h} = \vec{u} \in L^*(B_2)$ is an unknown lattice vector. Finally, the following is an unknown vector,

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

since $\vec{e}$ is an unknown vector. Now, Equation (23) can be rewritten as,

$$\vec{t} = \vec{u} + \vec{\epsilon}, \tag{24}$$

where $\vec{t} \in \mathbb{R}^n$, $\vec{u} \in L^*(B_2)$ and $\vec{\epsilon} \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$. According to Proposition 3.1, $\|\vec{\epsilon}\| = \|\vec{\epsilon_1}\| = \frac{\sqrt{n}}{2}$ since $\vec{\epsilon} = \vec{\varepsilon_2} \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$. From Equation (24), the LeeHahn$_{GGH}$-CVP is defined as follows:

**Definition 3.8.** (*LeeHahn$_{GGH}$-CVP*) *For $n, k \in \mathbb{N}$ with $k < n$, let $B \in \mathbb{R}^{n\times n}$ with columns $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$ be a basis for the lattice $L(B) \subset \mathbb{R}^n$, $B_2 \in \mathbb{R}^{n\times(n-k)}$ with columns $\vec{b}_{k+1}, \vec{b}_{k+2}, \ldots, \vec{b}_n \in B$ be a basis for the sub-lattice $L^*(B_2) \subset \mathbb{R}^n$ and $\vec{t} \in \mathbb{R}^n$ such that $\vec{t} = \vec{u} + \vec{\epsilon}$ where $\vec{u} \in L^*(B_2)$ and $\vec{\epsilon} = \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$. Given $B$ and $\vec{t}$, find the vector $\vec{u} \in L^*(B_2)$ such that $\|\vec{t} - \vec{u}\| = \frac{\sqrt{n}}{2}$.*

Recall that, the GGH-CVP is to find the vector $\vec{v}$ in the $n$-dimensional lattice $L(B) \subset \mathbb{R}^n$ such that $\vec{c} = \vec{v} + \vec{e}$ and $\|\vec{c} - \vec{v}\| = \sigma n$. On the other hand, the LeeHahn$_{GGH}$-CVP is to find the vector $\vec{u}$ in the $(n-k)$-dimensional lattice $L^*(B_2) \subset \mathbb{R}^n$ such that $\vec{t} = \vec{u} + \vec{\epsilon}$ and $\|\vec{t} - \vec{u}\| = \frac{\sqrt{n}}{2}$. With shorter distance and smaller lattice dimension, the LeeHahn$_{GGH}$-CVP is considered simpler than the GGH-CVP. Now, the Lee-Hahn's embedding attack moves to its reduction stage. In this stage, the embedding technique is used to reduce the LeeHahn$_{GGH}$-CVP in the $(n-k)$-dimensional lattice $L^*(B_2) \subset \mathbb{R}^n$ to an SVP variant in the $(n-k+1)$-dimensional lattice $L'(Z) \subset \mathbb{R}^{n+1}$. For that purpose, the vector $\begin{bmatrix}\vec{t}\\ 1\end{bmatrix} \in \mathbb{R}^{n+1}$ is embedded into the basis $B_2 \in \mathbb{R}^{n\times(n-k)}$ to form the basis $Z = \begin{bmatrix}\vec{t} & \vec{b_{k+1}} & \vec{b_{k+2}} & \ldots & \vec{b_n}\\ 1 & 0 & 0 & \ldots & 0\end{bmatrix} \in \mathbb{R}^{(n+1)\times(n-k+1)}$ that spans the embedded lattice $L'(Z)$. The Lee-Hahn's embedding attack also is expecting that the embedded lattice $L'(Z)$ contains a short vector. Consider the following lemma:

**Lemma 3.7.** *For $n, k \in \mathbb{N}$ with $k < n$, let $B \in \mathbb{R}^{n\times n}$ with columns $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$ be a basis for the $n$-dimensional lattice $L(B) \subset \mathbb{R}^n$, $B_2 \in \mathbb{R}^{n\times(n-k)}$ with columns $\vec{b}_{k+1}, \vec{b}_{k+2}, \ldots, \vec{b}_n \in B$ be a basis for the $(n-k)$-dimensional lattice $L^*(B_2) \subset \mathbb{R}^n$ and $\vec{t} \in \mathbb{R}^n$ such that $\vec{t} = \vec{u} + \vec{\epsilon}$ where $\vec{u} \in L^*(B_2)$ and $\vec{\epsilon} \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$. If $Z = \begin{bmatrix}\vec{t} & \vec{b_{k+1}} & \vec{b_{k+2}} & \ldots & \vec{b_n}\\ 1 & 0 & 0 & \ldots & 0\end{bmatrix} \in \mathbb{R}^{(n+1)\times(n-k+1)}$ is a basis for the $(n-k+1)$-dimensional lattice $L'(Z) \subset \mathbb{R}^{n+1}$, then $\begin{bmatrix}\vec{\epsilon}\\ 1\end{bmatrix}$ is a short vector in the lattice $L'(Z)$.*

As stated in Lemma 3.7, $\begin{bmatrix}\vec{\epsilon}\\ 1\end{bmatrix}$ is a short vector in the embedded lattice $L'(Z)$. The Lee-Hahn's embedding attack is expecting that this vector is the shortest non-zero vector in the embedded lattice $L'(Z)$. Finding the shortest non-zero vector in the embedded lattice $L'(Z)$ is an SVP variant. It is specifically addressed as the LeeHahn$_{GGH}$-SVP and it is explicitly defined as the following:

**Definition 3.9.** (*LeeHahn$_{GGH}$-SVP*) *For $n, k \in \mathbb{N}$ with $k < n$, let $B \in \mathbb{R}^{n\times n}$ with columns $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^n$ be a basis for the $n$-dimensional lattice $L(B) \subset \mathbb{R}^n$ and*

$$Z = \begin{bmatrix}\vec{t} & \vec{b_{k+1}} & \vec{b_{k+2}} & \ldots & \vec{b_n}\\ 1 & 0 & 0 & \ldots & 0\end{bmatrix} \in \mathbb{R}^{(n+1)\times(n-k+1)},$$

*where $\vec{b}_{k+1}, \vec{b}_{k+2}, \ldots, \vec{b}_n \in B$ and $\vec{t} \in \mathbb{R}^n$, be a basis for the $(n-k+1)$-dimensional lattice $L'(Z) \subset \mathbb{R}^{n+1}$. Given $B$ and $\vec{t}$, find the vector $\vec{\delta}_4 \in L'(Z)$ such that $\lambda_1(L'(Z)) = \|\vec{\delta}_4\|$ where $\lambda_1(L'(Z)) \in \mathbb{R}^+$ denotes the first minimum of the lattice $L'(Z)$.*

Finally, the Lee-Hahn's embedding attack is moving to its solution stage to solve the derived LeeHahn$_{GGH}$-SVP using lattice-reduction algorithm. The next lemma states that the corresponding LeeHahn$_{GGH}$-CVP is solvable if the solution of the LeeHahn$_{GGH}$-SVP is obtained as $\vec{\delta}_4 = \begin{bmatrix} \vec{\epsilon} \\ 1 \end{bmatrix}$.

**Lemma 3.8.** *For $n \in \mathbb{N}$, let $L'(Z) \subset \mathbb{R}^{n+1}$ be a lattice, $\vec{\epsilon} \in \mathbb{R}^n$ be the error vectors in the LeeHahn$_{GGH}$-CVP and $\lambda_1(L'(Z)) \in \mathbb{R}^+$ denotes the first minimum of the lattice $L'(Z)$. Suppose that the solution of the LeeHahn$_{GGH}$-SVP is obtained as $\vec{\delta}_4 \in L'(Z)$ such that $\lambda_1(L'(Z)) = \delta_4$. If $\vec{\delta}_4 = \begin{bmatrix} \vec{\epsilon} \\ 1 \end{bmatrix}$, then the solution for the LeeHahn$_{GGH}$-CVP could be obtained.*

**Lemma 3.9.** *If the LeeHahn$_{GGH}$-CVP is solved, then the GGH cryptosystem is broken.*

The implementation of Lee-Hahn's embedding attack completely decrypted the GGH Internet Challenge in the lattice dimension of 400 in just about 18 hours. The attack was also launched toward the GGH cryptosystem in the lattice dimensions of 450, and 500 [9]. The results show that the more actual plaintext values can be guessed, the more powerful the attack could perform.

## 4 Performances Comparison Between the Original, Nguyen's and Lee-Hahn's Embedding Attacks

The best achievement of the original embedding attacks is breaking the GGH cryptosystem in the dimension of 200 [5]. The Nguyen's attacks with modulus $\sigma$ defeated the GGH cryptosystem in the lattice dimension of 350 in about 21 hours[13]. The performance becomes even better when the modulus $2\sigma$ is used where in the same lattice dimension, the GGH cryptosystem is defeated in just about 4 hours [13]. Despite using the same strategy, using two different moduli resulted in two different performances. The performance of Nguyen's embedding attacks using the modulus $2\sigma$ is much better than the modulus $\sigma$. Recall that the reduction stage of the original embedding attacks is launched towards the GGH-CVP. In contrast, the reduction stage of the Nguyen embedding attacks is launched towards the Nguyen$_{GGH}$-CVP1 and Nguyen$_{GGH}$-CVP2. As a result, Nguyen's embedding attacks worked much better than the original embedding attacks. Simplification of the GGH-CVP plays a crucial role in Nguyen's embedding attacks.

In the original embedding attacks, lattice reduction algorithms are deployed to solve the GGH-SVP. In the Nguyen's embedding attacks, these algorithms are deployed to solve the Nguyen$_{GGH}$-SVP1 and Nguyen$_{GGH}$-SVP2. The results indicate that these algorithms performed better in solving the Nguyen $_{GGH}$-SVP1 and Nguyen$_{GGH}$-SVP2 compared to the GGH-SVP. The performance of lattice-reduction algorithms is influenced by various factors including theoretical (mathematical) and practical (computer architecture) factors. In the context of this study, only the mathematical factors will be discussed while the practical factors are beyond the interest of this study. The mathematical factors to be considered are the lattice dimension $n \in \mathbb{N}$ and the expected gap in the embedded lattices $L'(X)$, $L'(Y_1)$ and $L'(Y_2)$. In terms of lattice dimension $n$, the lattice-reduction algorithms are performed on the bases $X,\ Y_1, Y_2 \in \mathbb{R}^{(n+1)\times(n+1)}$ that span the embedded lattices $L'(X)$, $L'(Y_1)$ and $L'(Y_2)$ respectively. Note that, these bases consist of the same number of basis vectors. Each basis consists of $(n+1)$ vectors and each vector have $(n+1)$ entries. This implies that, the embedded lattices $L'(X)$, $L'(Y_1)$ and $L'(Y_2)$ are full-rank lattices with similar dimensions, i.e., $\dim(L'(X)) = \dim(L'(Y_1)) = \dim(L'(Y_2)) = n+1$. This indicates that lattice dimension is not the main factor that caused the original and Nguyen's embedding attacks to perform differently. Nevertheless, there is a similarity that could be observed with regard to the

lattice dimensions. The higher the lattice dimension $n$ is, the longer time is consumed to solve the derived SVP variant.

As defined in Definition 2.4, gap in the lattice $\mathcal{L}$ is measured as $gap(\mathcal{L}) = \dfrac{\lambda_2(\mathcal{L})}{\lambda_1(\mathcal{L})}$ where $\lambda_1(\mathcal{L})$ is the norm of the shortest vector in the lattice $\mathcal{L}$ and $\lambda_2(\mathcal{L})$ is the norm of the second shortest vector in the lattice $\mathcal{L}$. Finding such vectors in the lattice $\mathcal{L}$ is an SVP.

As proven before, the embedded lattices $L'(X)$, $L'(Y_1)$ and $L'(Y_2)$ are expected to contain short vectors $\vec{\delta}_1 = \begin{bmatrix}\vec{e}\\ 1\end{bmatrix} \in L'(X), \vec{\delta}_2 = \begin{bmatrix}\vec{\epsilon_1}\\ 1\end{bmatrix} \in L'(Y_1)$ and $\vec{\delta}_3 = \begin{bmatrix}\vec{\epsilon_2}\\ 1\end{bmatrix} \in L'(Y_2)$ respectively. The derived GGH-SVP, Nguyen$_{GGH}$-SVP1 and Nguyen$_{GGH}$-SVP2 are considered solved once these vectors are obtained by the lattice-reduction algorithms. Thus, the norm of the vectors $\vec{\delta}_1$, $\vec{\delta}_2$ and $\vec{\delta}_3$ are considered as the first minimum of the embedded lattices $L'(X)$, $L'(Y_1)$ and $L'(Y_2)$ respectively, i.e., $\lambda_1(L'(X)) = \|\vec{\delta_1}\|, \lambda_1(L'(Y_1)) = \|\vec{\delta_2}\|$ and $\lambda_1(L'(Y_2)) = \|\vec{\delta_3}\|$.

Note that, the embedded lattices $L'(X)$, $L'(Y_1)$ and $L'(Y_2)$ are spanned by the bases $X, Y_1$ and $Y_2$ respectively. These bases have almost similar structure with the only difference is the embedded vectors $\begin{bmatrix}\vec{c_1}\\ 1\end{bmatrix}, \begin{bmatrix}\vec{p_1}\\ 1\end{bmatrix}, \begin{bmatrix}\vec{p_2}\\ 1\end{bmatrix} \in \mathbb{R}^{n+1}$ in the bases $X, Y_1$ and $Y_2$ respectively. As done in [13] and [9], the shortest vector in the lattice $L(B)$ is considered as the second shortest vector in the embedded lattices $L'(X)$, $L'(Y_1)$ and $L'(Y_2)$ respectively, i.e.,

$$\lambda_2(L'(X)) = \lambda_2(L'(Y_1)) = \lambda_2(L'(Y_2)) = \lambda_1(L(B)).$$

Therefore, the expected gap of the lattices $L'(X), L'(Y_1)$ and $L'(Y_2)$ are obtained as the following:

$$gap(L'(X)) = \frac{\lambda_2(L'(X))}{\lambda_1(L'(X))} = \frac{\lambda_1(L(B))}{\|\vec{\delta_1}\|} \in \mathbb{R}^+, \tag{25}$$

$$gap(L'(Y_1)) = \frac{\lambda_2(L'(Y_1))}{\lambda_1(L'(Y_1))} = \frac{\lambda_1(L(B))}{\|\vec{\delta_2}\|} \in \mathbb{R}^+, \tag{26}$$

$$gap(L'(Y_2)) = \frac{\lambda_2(L'(Y_2))}{\lambda_1(L'(Y_2))} = \frac{\lambda_1(L(B))}{\|\vec{\delta_3}\|} \in \mathbb{R}^+. \tag{27}$$

Recall that, we have $\|\vec{\delta_1}\| = \sqrt{n\sigma^2 + 1}$ since $\vec{\delta}_1 = \begin{bmatrix}\vec{e}\\ 1\end{bmatrix}$ and $\vec{e} \in \{-\sigma, +\sigma\}^n$. For $\vec{\delta}_2 = \begin{bmatrix}\vec{\epsilon_1}\\ 1\end{bmatrix}$, we have

$$\|\vec{\delta_2}\| = \sqrt{\underbrace{(\pm 1)^2 + (\pm 1)^2 + \ldots + (\pm 1)^2}_{\text{added } n \text{ times}} + 1} = \sqrt{n+1},$$

since $\vec{\epsilon}_1 \in \{-1, +1\}^n$. For $\vec{\delta}_3 = \begin{bmatrix}\vec{\epsilon_2}\\ 1\end{bmatrix}$, we have

$$\|\vec{\delta_3}\| = \sqrt{\underbrace{\left(\pm\frac{1}{2}\right)^2 + \left(\pm\frac{1}{2}\right)^2 + \ldots + \left(\pm\frac{1}{2}\right)^2}_{\text{added } n \text{ times}} + 1} = \sqrt{\frac{n}{4} + 1}.$$

since $\vec{\epsilon}_2 \in \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$. Recall that $n, \sigma \in \mathbb{N}$. Therefore,

$$\|\vec{\delta_3}\| < \|\vec{\delta_2}\| < \|\vec{\delta_1}\|.$$

Since the numerators are equal, then

$$\frac{\lambda_1(L(B))}{\|\vec{\delta_1}\|} < \frac{\lambda_1(L(B))}{\|\vec{\delta_2}\|} < \frac{\lambda_1(L(B))}{\|\vec{\delta_3}\|},$$

and

$$gap\left(L'\left(X\right)\right) < gap\left(L'\left(Y_1\right)\right) < gap\left(L'\left(Y_2\right)\right).$$

Observe that, the $gap\left(L'\left(Y_2\right)\right)$ has the smallest denominator $\|\vec{\delta_3}\|$ while the $gap\left(L'\left(X\right)\right)$ has the largest denominator $\|\vec{\delta_1}\|$. Consequently, the embedded lattice $L'\left(Y_2\right)$ derived by Nguyen's embedding attack with modulus $2\sigma$ has the largest expected gap. In contrast, the embedded lattice $L'\left(X\right)$ derived from the original embedding attacks has the smallest expected gap. With the smallest $gap\left(L'\left(X\right)\right)$, the solution stage of the original embedding attacks only managed to solve the derived GGH-SVP in the lattice dimensions of 200 and below. With larger $gap\left(L'\left(Y_1\right)\right)$, the solution stage of the Nguyen's embedding attacks with modulus $\sigma$ solved the derived Nguyen$_{GGH}$-SVP1 in the lattice dimension of 350 in about 21 hours. Finally, the largest $gap\left(L'\left(Y_2\right)\right)$ in the embedded lattice $L'\left(Y_2\right)$ made the solution stage of the Nguyen's embedding attacks with modulus $2\sigma$ solved the Nguyen$_{GGH}$-SVP2 in the lattice dimension of 350 in just about 4 hours. Based on these findings, the lattice gap is identified as the main factor that caused a difference in the performance of the embedding attacks in breaking the GGH cryptosystem.

Although Nguyen's and Lee-Hahn's embedding attacks use an almost similar strategy, there is a significant difference between the ability of these attacks to break the GGH cryptosystem. To investigate the factor that triggered this difference, Nguyen's $2\sigma$ embedding attack is compared with Lee-Hahn's embedding attack. As done before, two factors that majorly influence the performance of the lattice-reduction algorithm in the solution stage of these attacks are considered. The first factor is the lattice dimension $n$. Recall that, the Nguyen's embedding attack formed the $(n+1)$-dimensional embedded lattice $L'\left(Y_2\right)$ while the Lee-Hahn's embedding attack formed the $(n-k+1)$-dimensional embedded lattice $L'\left(Z\right)$. Since , $k \in \mathbb{N}$ where $k < n$, then the embedded lattice $L'\left(Z\right)$ has smaller dimension compared to the embedded lattice $L'\left(Y_2\right)$. With smaller dimension, the implementation of lattice-reduction algorithm on the embedded lattice $L'\left(Z\right)$ would be advantageous compared to its implementation on the embedded lattice $L'\left(Y_2\right)$. This could also be why Lee-Hahn's embedding attack performs better when the value of $k$ is bigger.

The second factor to be considered is the gap in the embedded lattices $L'\left(Y_2\right)$ and $L'\left(Z\right)$. Recall that, the expected gap in the lattice $L'\left(Y_2\right)$ is measured as $gap\left(L'\left(Y_2\right)\right) = \dfrac{\lambda_1(L(B))}{\|\vec{\delta_3}\|}$ where $\lambda_1\left(L\left(B\right)\right)$ is the first minimum of the lattice $L\left(B\right)$ and $\vec{\delta_3}$ is a short vector in the embedded lattice $L'\left(Y_2\right)$. Proposition 3.1 proved that $\|\epsilon_2\| = \dfrac{\sqrt{n}}{2}$ where $\vec{\varepsilon_2} \in \left\{-\dfrac{1}{2}, \dfrac{1}{2}\right\}^n$. Recall that, we have $\|\vec{\delta_3}\| = \sqrt{\dfrac{n}{4}+1}$ for $\vec{\delta_3} = \begin{bmatrix}\vec{\epsilon_2}\\ 1\end{bmatrix}$. On the other hand, Lemma 3.8 stated that $\delta_4 = \begin{bmatrix}\vec{\epsilon}\\ 1\end{bmatrix}$ is a short vector in the embedded lattice $L'\left(Z\right)$. It is the desired solution for the LeeHahn$_{GGH}$-SVP. Thus, $\|\vec{\delta_4}\|$ is considered as the first minimum of the embedded lattice $L'\left(Z\right)$, i.e., $\lambda_1\left(L'\left(Z\right)\right) = \|\vec{\delta_4}\|$. Since the basis $Z$ is constructed mainly using the basis $B_2$ for the sub-lattice $L^*\left(B_2\right)$, then the shortest vector in the lattice $L^*\left(B_2\right)$ is considered as the second minimum of the embedded lattice $L'\left(Z\right)$, i.e., $\lambda_2\left(L'\left(Z\right)\right) = \lambda_1\left(L^*\left(B_2\right)\right)$. Hence, the expected gap of the embedded lattice $L'\left(Z\right)$ is obtained as follows:

$$gap\left(L'\left(Z\right)\right) = \frac{\lambda_2\left(L'\left(Z\right)\right)}{\lambda_1\left(L'\left(Z\right)\right)} = \frac{\lambda_1\left(L^*\left(B_2\right)\right)}{\lambda_1\left(L'\left(Z\right)\right)} = \frac{\lambda_1(L^*(B_2))}{\|\vec{\delta_4}\|} \in \mathbb{R}^+, \tag{28}$$

Since $\vec{\epsilon} = \vec{\varepsilon}_2 \in \left\{-\frac{1}{2}, \frac{1}{2}\right\}^n$, then $\|\vec{\delta_4}\| = \|\vec{\delta_3}\| = \sqrt{\frac{n}{4} + 1}$. Despite having different numerators, the $gap\left(L'\left(Y_2\right)\right)$ and $gap\left(L'\left(Z\right)\right)$ share a common denominator value. As described by [9], the fast growth of the length of the shortest vector predicted by the Gaussian Heuristic is mainly due to the very fast growth of the determinant. Since the basis $B_2 \in \mathbb{R}^{n\times(n-k)}$ is a non-square matrix, then $\det\left(L^*\left(B_2\right)\right) = \sqrt{\det\left(B_2 B_2^T\right)}$. On the other hand, $\det\left(L\left(B\right)\right) = \left|\det\left(B\right)\right|$ since the basis $B \in \mathbb{R}^{n\times n}$ is a square matrix. Using the Gaussian Heuristic, the shortest vectors in the lattices $L\left(B\right)$ and $L^*\left(B_2\right)$ are estimated respectively as the following:

$$\lambda_1\left(L\left(B\right)\right) \approx \sqrt{\frac{n}{2\pi e}}\left(\det\left(L\left(B\right)\right)\right)^{\frac{1}{n}} = \sqrt{\frac{n}{2\pi e}}\left(\left|\det\left(B\right)\right|\right)^{\frac{1}{n}},$$

and

$$\lambda_1\left(L^*\left(B_2\right)\right) \approx \sqrt{\frac{n-k}{2\pi e}}\left(\det\left(L^*\left(B_2\right)\right)\right)^{\frac{1}{n-k}} = \sqrt{\frac{n-k}{2\pi e}}\left(\left(\det\left(B_2 B_2^T\right)\right)^{\frac{1}{2}}\right)^{\frac{1}{n-k}}.$$

Since $k < n$ and $B_2$ is a sub-matrix from the basis $B$, then $\lambda_1\left(L^*\left(B_2\right)\right) > \lambda_1\left(L\left(B\right)\right)$. Note that, $\|\vec{\delta_4}\| = \|\vec{\delta_3}\|$. Therefore,

$$\frac{\lambda_1\left(L^*\left(B_2\right)\right)}{\|\vec{\delta_4}\|} > \frac{\lambda_1(L(B))}{\|\vec{\delta_3}\|},$$
$$gap\left(L'\left(Z\right)\right) > gap\left(L'\left(Y_2\right)\right).$$

With smaller dimension and larger expected gap of the embedded lattice $L'\left(Z\right)$ compared to the embedded lattice $L'\left(Y_2\right)$, implementation of a lattice-reduction algorithm in the solution stage of Lee-Hahn's embedding attack performed better. These factors allowed Lee-Hahn's embedding attack to break the GGH cryptosystem in the lattice dimensions of 400 and beyond, while Nguyen's embedding attack failed.

## 5 Result and Discussion

Although Lee-Hahn's embedding attack emerges as the most powerful attack on the GGH cryptosystem, it depends heavily on Nguyen's embedding attack to be completely executed. Without the partially decrypted plaintext $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^n$ which is obtained by Nguyen's embedding attack, the guessing stage of the Lee-Hahn's embedding attack could not be done, and the $k$-actual plaintext values could not be obtained. Consequently, the simplification stage of Lee-Hahn's embedding attack could not be performed, and the GGH-CVP remains in its original form. Nguyen's embedding attack is crucial in developing Lee-Hahn's embedding attack. That means Nguyen's embedding attack could be considered a fatal attack on the GGH cryptosystem. Furthermore, the factors that made the performance of the original, Nguyen's and Lee-Hahn's embedding attacks contrast from each other are also investigated. As a result, the performance of these attacks is mainly determined by the efficiency of the implemented lattice algorithms in the solution stage of these attacks. The more efficient lattice-reduction algorithms could perform, the more powerful these attacks could perform. Performance of these algorithms is highly influenced by the dimension and gap of the embedded lattices $L'\left(X\right), L'\left(Y_1\right), L'\left(Y_2\right)$ and $L'\left(Z\right)$ that are formed by those attacks. The findings are summarized as follows:

Table 1: Comparison in terms of dimension of the embedded lattices.

| Embedding attack | Original | Nguyen's $\sigma$ | Nguyen's $2\sigma$ | Lee-Hahn's |
|---|---|---|---|---|
| Embedded lattice | $L'(X)$ | $L'(Y_1)$ | $L'(Y_2)$ | $L'(Z)$ |
| Lattice dimension | $n+1$ | $n+1$ | $n+1$ | $n-k+1$ |

Table 2: Comparison in terms of expected gap of the embedded lattices.

| Expected gaps | Attacks | Winner |
|---|---|---|
| $gap(L'(Y_2)) > gap(L'(X))$ | Nguyen's $2\sigma$ vs Original embedding | Nguyen's $2\sigma$ attack |
| $gap(L'(Y_2)) > gap(L'(Y_1))$ | Nguyen's $2\sigma$ vs Nguyen's $\sigma$ | Nguyen's $2\sigma$ attack |
| $gap(L'(Z)) > gap(L'(Y_2))$ | Nguyen's $2\sigma$ vs Lee-Hahn's | Lee-Hahn's attack |

Table 3: Comparison in terms of norm of the expected shortest vector.

| Embedding attacks | Original | Nguyen's $\sigma$ | Nguyen's $2\sigma$ | Lee-Hahn's |
|---|---|---|---|---|
| Expected shortest vector | $\vec{\delta}_1 = \begin{bmatrix} \vec{e} \\ 1 \end{bmatrix}$ | $\vec{\delta}_2 = \begin{bmatrix} \vec{\epsilon_1} \\ 1 \end{bmatrix}$ | $\vec{\delta}_3 = \begin{bmatrix} \vec{\epsilon_2} \\ 1 \end{bmatrix}$ | $\vec{\delta}_4 = \begin{bmatrix} \vec{\epsilon} \\ 1 \end{bmatrix}$ |
| Norm of shortest vector | $\sqrt{n\sigma^2+1}$ | $\sqrt{n+1}$ | $\sqrt{\frac{n}{4}+1}$ | $\sqrt{\frac{n}{4}+1}$ |

Observe that, the embedded lattice $L'(Z)$ has smaller dimension then lattice $L'(Y_2)$ as shown in Table 1. In addition, the expected gap in lattice $L'(Z)$ is larger than the expected gap in lattice $L'(Y_2)$, as provided in Table 2. Consequently, Lee-Hahn's embedding attack becomes more powerful than Nguyen's embedding attack. Furthermore, Table 3 shows that the vectors $\vec{\delta}_4 \in L'(Z)$ and $\vec{\delta}_3 \in L'(Y_2)$ share the shortest norms. The norm of these shortest vectors $\vec{\delta}_3$ and $\vec{\delta}_4$ play crucial roles in determining the lattice gap. With shortest norms $\|\vec{\delta}_3\|$ and $\|\vec{\delta}_4\|$, the Nguyen's $2\sigma$ and Lee-Hahn's embedding attacks outperformed the other two embedding-based attacks.

## 6 Conclusion

The original, Nguyen's, and Lee-Hahn's embedding attacks have the reduction and solution stages in common. The simplification stage in Nguyen's and Lee-Hahn's embedding attacks considerably impacted the ability of these attacks to break the GGH cryptosystem. Without this stage, the GGH-CVP remains in its original form, and the embedding attack on this problem will only

manage to reach lattice dimensions not more than 200. As shown before, the shorter the norm of the error vector in the GGH-CVP variants, the larger the expected gap of the embedded lattices. By maintaining the norm as $\sigma\sqrt{n}$, then the size of the lattice gap permits the embedding attacks to work only in low lattice dimensions as previously faced by the original embedding attacks for solving the GGH-CVP. If these countermeasures could be implemented, any strategy in future which aims to improve the embedding attack's ability to break the GGH cryptosystem could be circumvented. Finally, Nguyen's embedding attack is the fatal attack on the GGH cryptosystem. Thus, the security of the GGH cryptosystem could be upgraded by thwarting Nguyen's embedding attack. The flaw exploited by Nguyen's embedding attack must be revamped. Strengthening the security of the GGH cryptosystem to make it resistant to Nguyen's embedding attack would potentially make the GGH cryptosystem survives.

**Acknowledgement** All authors would like to thank anonymous reviewers for all their constructive comments and recommendations for the betterment of this paper. Universiti Malaysia Sabah financially supports this study through the Research Grant SBK0508-2021.

**Conflicts of Interest** The authors declare no conflict of interest.

## References

[1] A. Dadheech (2018). Preventing information leakage from encoded data in lattice-based cryptography. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1952–1955. IEEE. https://doi.org/10.1109/ICACCI.2018.8554942.

[2] S. D. Galbraith (2012). *Mathematics of Public Key Cryptography*. Cambridge University Press, Cambridge.

[3] N. Gama & P. Q. Nguyen (2008). Predicting lattice reduction. In *Advances in Cryptology – EUROCRYPT 2008*, pp. 31–51. Springer, Berlin, Heidelberg.

[4] O. Goldreich, S. Goldwasser & S. Halevi (1997). The GGH cryptosystem challenges. In *http://groups.csail.mit.edu/cis/lattice/challenge.html,*.

[5] O. Goldreich, S. Goldwasser & S. Halevi (1997). 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*, pp. 112–131. Springer, Berlin, Heidelberg.

[6] O. Goldreich, D. Micciancio, S. Safra & J.-P. Seifert (1999). Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Information Processing Letters*, *71*(2), 55–61. https://doi.org/10.1016/S0020-0190(99)00083-6.

[7] E. Goodaire (2013). *Linear Algebra: Pure & Applied*. World Scientific Publishing Company, New Jersey.

[8] J. Hoffstein, J. Pipher, J. H. Silverman, J. Hoffstein, J. Pipher & J. H. Silverman (2014). *An Introduction to Cryptography*. Springer, New York.

[9] M. S. Lee & S. G. Hahn (2010). Cryptanalysis of the GGH cryptosystem. *Mathematics in Computer Science*, *3*, 201–208. https://doi.org/10.1007/s11786-009-0018-5.

[10] A. Mandangan, H. Kamarulhaili & M. A. Asbullah (2021). An upgrade on the key generation algorithm of the GGH-MKA lattice-based encryption scheme. *Malaysian Journal of Mathematical Sciences*, *15*(S), 25–37.

[11] A. Mandangan, H. Kamarulhaili & M. A. Asbullah (2020). A security upgrade on the GGH lattice-based cryptosystem. *Sains Malaysiana*, *49*(6), 1471–1478. http://dx.doi.org/10.17576/jsm-2020-4906-25.

[12] D. Micciancio & O. Regev (2009). Lattice-based cryptography. In D. J. Bernstein, J. Buchmann & E. Dahmen (Eds.), *Post-quantum cryptography*, pp. 147–191. Springer Berlin Heidelberg,.

[13] P. Nguyen (1999). Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from CRYPTO'97. In *Annual International Cryptology Conference*, pp. 288–304. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48405-1_18.

[14] T. Plantard & W. Susilo (2009). Broadcast attacks against lattice-based cryptosystems. In *International Conference on Applied Cryptography and Network Security*, pp. 456–472. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-01957-9_28.

[15] A. Sipasseuth, T. Plantard & W. Susilo (2019). Enhancing Goldreich, Goldwasser and Halevi's scheme with intersecting lattices. *Journal of Mathematical Cryptology*, *13*(3-4), 169–196. http://dx.doi.org/10.1515/jmc-2016-0066.