Sains Malaysiana 49(6)(2020): 1471-1478
http://dx.doi.org/10.17576/jsm-2020-4906-25

A Security Upgrade on the GGH Lattice-Based Cryptosystem

(Suatu Naik-taraf Keselamatan terhadap Sistem-kripto berasaskan Kekisi GGH)

ARIF MANDANGAN, HAILIZA KAMARULHAILI & MUHAMMAD ASYRAF ASBULLAH*

ABSTRACT

Due to the Nguyen's attack, the Goldreich-Goldwasser-Halevi (GGH) encryption scheme, simply referred to as GGH cryptosystem, is considered broken. The GGH cryptosystem was initially addressed as the first practical lattice-based cryptosystem. Once the cryptosystem is implemented in a lattice dimension of 300 and above, its inventors was conjectured that the cryptosystem is intractable. This conjecture was based on thorough security analyses on the cryptosystem against some powerful attacks. This conjecture became more concrete when all initial efforts for decrypting the published GGH Internet Challenges were failed. However, a novel strategy by the Nguyen's attack for simplifying the underlying Closest-Vector Problem (CVP) instance that arose from the cryptosystem, had successfully decrypted almost all the challenges and eventually made the cryptosystem being considered broken. Therefore, the Nguyen's attack is considered as a fatal attack on the GGH cryptosystem. In this paper, we proposed a countermeasure to combat the Nguyen's attack. By implementing the proposed countermeasure, we proved that the simplification of the underlying CVP instance could be prevented. We also proved that, the upgraded GGH cryptosystem remains practical where the decryption could be done without error. We are optimistic that, the upgraded GGH cryptosystem could make a remarkable return into the mainstream discussion of the lattice-based cryptography.

Keywords: Closest vector problem; GGH cryptosystem; lattice-based cryptography; post-quantum cryptography; shortest-vector problem

ABSTRAK

Berpunca daripada serangan Nguyen, skim penyulitan Goldreich-Goldwasser-Halevi (GGH), secara ringkasnya dirujuk sebagai sistem-kripto GGH, kini dipertimbangkan sebagai suatu skim yang telah rosak, iaitu tidak lagi selamat. Pada awalnya, sistem-kripto GGH pernah dirujuk sebagai sistem-kripto berasaskan-kekisi pertama yang praktikal. Apabila sistem-kripto ini dilaksanakan dalam kekisi berdimensi 300 dan ke atas, maka para pencipta sistem-kripto ini pernah menjangkakan bahawa ia adalah selamat. Jangkaan ini telah dibuat berdasarkan analisis keselamatan yang terperinci terhadap sistem-kripto tersebut menentang beberapa serangan yang hebat. Jangkaan tersebut telah menjadi semakin kukuh apabila kesemua usaha awal untuk menyahsulitkan beberapa Cabaran GGH yang dipaparkan di Internet (Cabaran Internet GGH) telah mengalami kegagalan. Namun demikian, suatu strategi baharu oleh serangan Nguyen dengan meringkaskan contoh Masalah Vektor-Terhampir (MVT) yang hadir secara terselindung disebalik sistem-kripto GGH, telah berjaya menyahsulitkan hampir kesemua Cabaran Internet GGH. Kesannya, sistem-kripto GGH telah dipertimbangkan sebagai suatu skim yang rosak dan tidak lagi selamat. Maka, serangan Nguyen sudah sewajarnya dipertimbangkan sebagai serangan pemusnah terhadap sistem-kripto GGH. Dalam kajian ini, kami mencadangkan suatu tindakan menyelamat bagi menentang serangan Nguyen. Melalui pelaksanaan tindakan menyelamat yang dicadangkan ini, kami buktikan bahawa proses meringkaskan contoh MVT disebalik sistem-kripto GGH kini dapat dielakkan. Kami juga buktikan bahawa sistem-kripto GGH yang telah dinaik-taraf ini masih kekal praktikal yang mana proses penyahsulitannya boleh dilaksanakan tanpa sebarang kesilapan. Kami optimis bahawa sistem-kripto GGH yang telah dinaik-taraf tahap keselamatannya ini mampu membuat penampilan semula ke medan perbincangan arus perdana dalam arena kriptografi berasaskan-kekisi.

Kata kunci: Kriptografi berasaskan kekisi; kriptografi pasca kuantum; masalah vektor terhampir; masalah vektor terpendek; sistem-kripto GGH

INTRODUCTION

Since the modern era of cryptography, the security of cryptographic schemes relies on the hardness of hard mathematical problems such as the Integer Factorization Problem (IFP), Discrete Logarithm Problem (DLP) and Elliptic-Curve Discrete Logarithm Problem (ECDLP). Based on these problems, various cryptographic schemes

have been proposed. The most established schemes are the Rivest-Shamir-Adleman (RSA) cryptosystem (Rivest et al. 1978), El-Gamal cryptosystem (Elgamal 1985) and Elliptic-Curve cryptosystem (ECC) (Koblitz 1987). These cryptosystems received wide attention from global cryptography society either for theoretical interest or practical purposes. Although these cryptosystems are mainly used to provide confidentiality, various cryptographic primitives have been derived from these cryptosystems to achieve other security goals. For instance, digital signature schemes by Ismail and Hasan (2006) and Jaju and Chowhan (2015) are developed based on the RSA and El-Gamal cryptosystems, respectively, while key exchange method by Zazali and Othman (2012) is developed based on the ECC.

Due to the Shor's quantum algorithm (Shor 1994), the security of the RSA, El-Gamal and ECC would be breached since the underlying IFP, DLP, and ECDLP could be efficiently solved. Fortunately, the development of quantum computing technology is still under progress. Thus, proactive action must be taken as a preparation to combat the Shor's quantum algorithm. Current interest in cryptography is moving towards the new era known as the Post-Quantum Cryptography where the lattice-based cryptography emerges as one of the most promising candidates. The security of lattice-based cryptosystems is relying on some lattice-based problems such as the Shortest-Vector Problem (SVP), Closest-Vector Problem (CVP), Smallest-Basis Problem (SBP) etc. Unlike the IFP, DLP and ECDLP, these lattice problems are conjectured to be unaffected by any quantum algorithm (Micciancio & Regev 2009). There are various lattice-based cryptosystems have been developed such as the Ajtai-Dwork (AD) cryptosystem (Ajtai & Dwork 1997), Goldreich-Goldwasser-Halevi (GGH) cryptosystem (Goldreich et al. 1997a), NTRU Encrypt (Hoffstein et al. 1998), LWE cryptosystem (Regev 2005) and Ring-LWE cryptosystem (Lyubashevski et al. 2010). Among these cryptosystems, the GGH cryptosystem is the first scheme that was considered practical.

The security of the GGH cryptosystem is based on hardness of the CVP instance, defined as the GGH-CVP instance (Mandangan et al. 2018) together with the SBP instance, defined as the GGH-SBP instance (Mandangan et al. 2019). Although the GGH cryptosystem is unequipped with provable security features, the security of this cryptosystem has been experimentally tested by Goldreich et al. (1997a). Some powerful attacks have been launched on it such as the round-off attack, nearest-plane attack and embedding attack. As a result, these attacks failed once the cryptosystem is implemented in a lattice dimension of 200 and above. Other than these experiments, the security of the GGH cryptosystem also has been tested by Schnorr et al. (1997) via the embedding attack. This attack succeeded only in the lattice dimensions up to 150. Since that, Goldreich et al. (1997a) was conjectured that the underlying GGH-CVP instance as practically intractable in the lattice dimensions of 300 and beyond.

Later, Nguyen (1999) discovered a major flaw on the design of the GGH cryptosystem which allowing the simplification of the GGH-CVP instance. The simplified version is defined as the $\text{Nguyen}_{\text{GGH}}$-CVP instance (Mandangan et al. 2018). From that, the Nguyen's attack is developed to break the GGH cryptosystem. Instead of solving the underlying GGH-CVP instance, the Nguyen's attack is managed to solve the $\text{Nguyen}_{\text{GGH}}$-CVP instance. In this instance, the Euclidean norm of the error vector has been shortened from the original norm $\sigma\sqrt{n}$ becomes $\frac{\sqrt{n}}{2}$ where $\sigma, n \in \mathbb{N}$ are the parameters in the GGH cryptosystem. That is why the $\text{Nguyen}_{\text{GGH}}$-CVP instance is easier to solve compared to the GGH-CVP instance. As a result, the Nguyen's attack completely decrypted the GGH cryptosystem in the lattice dimensions of 200 up to 350 as published in the GGH Internet Challenges (Goldreich et al. 1997b). Due to the Nguyen's attack, the GGH cryptosystem is considered broken.

Since that, there are few attempts for improving the GGH cryptosystem can be found in literature. Nguyen (1999) himself proposed a remedy to his own attack by replacing the error vector of the GGH cryptosystem with $\vec{e} \in [-\sigma, +\sigma]^n$ or $\vec{e} \in \{\pm\sigma, \pm(\sigma-1)\}^n$. However, he rejected this idea since the Euclidean norm $\|\vec{e}\|$ would be shorter than $\sigma\sqrt{n}$ and this makes the GGH cryptosystem insecure again. Later, Yoshino and Kunihiro (2012) proposed a variant of GGH known as the GGH-YK cryptosystem. In this variant, the error vector is replaced with a larger error vector and at the same time several new parameters have been introduced. In order to generate these parameters, few conditions need to be fulfilled. Later, Barros and Schechter (2014) found that the parameterization of the GGH-YK cryptosystem is unrealistic. As an improvement, they proposed another variant known as the GGH-YK-M cryptosystem. After all, these variants made major modification on the GGH cryptosystem. The security of these variants also does no longer relying on the GGH-CVP instance.

In this paper, we upgraded the security of the GGH cryptosystem to combat the Nguyen's attack. Similar as the suggested remedy by Nguyen (1999), we replaced the error vector with a new set. Then, we proposed a new strategy to maintain the Euclidean norm $\|\vec{e}\| = \sigma\sqrt{n}$. Compared to other GGH variants, we maintained the original design of the GGH cryptosystem. We just simply repaired the flaw which was exploited by the Nguyen's attack. Our intention is to maintain the security reliance of the upgraded GGH cryptosystem on the GGH-CVP instance, so that all its security features prior the Nguyen's attack could be retained. By implementing the proposed countermeasure, we proved that the upgraded GGH Cryptosystem is unaffected by the Nguyen's attack and at the same time its decryption could be done effectively without error.

This paper is organized in the following flow. In the next section, we provide some mathematical background related to vectors, matrices and lattices. In the third section, we provide light introduction to the GGH cryptosystem and then followed by the mathematical design of the Nguyen's attack. In the fourth section, we present the proposed countermeasure together with some significant proofs related to our contribution. Finally, we conclude this paper in the final section.

MATHEMATICAL BACKGROUND

Throughout this paper, all vectors are denoted as column vectors. For instance, let $m \in \mathbb{N}$. Then $\vec{u_1} = \begin{bmatrix} u_{1,1} \\ \vdots \\ u_{m,1} \end{bmatrix} \in \mathbb{R}^m$ is a column vector with entries $u_{i,1} \in \mathbb{R}$ for all $i = 1,...,m$. Any vector $\vec{u_1} \in \mathbb{R}^m$ can be converted into an integer vector $\lceil \vec{u_1} \rfloor \in \mathbb{Z}^n$ by using the following function:

Definition 1 (Pol 2011) *For $m \in \mathbb{N}$, let $\vec{u_1} \in \mathbb{R}^m$ with entries $u_{i,1} \in \mathbb{R}$ for all $i = 1,...,m$. The rounding function on the vector $\vec{u_1}$ is defined as $\lceil \vec{u_1} \rfloor : u_{i,1} \in \mathbb{R} \to \lceil u_{i,1} \rfloor \in \mathbb{Z}$, such that $\left| u_{i,1} - \lceil u_{i,1} \rfloor \right| \le \frac{1}{2}$ for all $i = 1,...,m$.*

The length of a vector is referred to as norm. Generally, an l_p-norm is defined as follows:

Definition 2 (Serre 2010) *For $m \in \mathbb{N}$, let $\vec{u_1} \in V \subset \mathbb{R}^m$ where V is a vector space. For all $u_{i,1} \in \vec{u_1}$ where $i = 1,...,m$, the l_p-norm of the vector u_1 is defined as follows*

$$\left\| \vec{u_1} \right\|_p = \left(\sum_{i=1}^{m} \left| u_{i,1} \right|^p \right)^{\frac{1}{p}}, \left\| \vec{u_1} \right\|_\infty = \max_i \left| u_{i,1} \right|. \quad (1)$$

On the other hand, the distance between two vectors and $\vec{u_2}$ can be measured as follows:

Definition 3 (Serre 2010) *For $m \in \mathbb{N}$, let $\vec{u_1}, \vec{u_2} \in \mathbb{R}^m$. For all $u_{i,1} \in \vec{u_1}$ and $u_{i,2} \in \vec{u_2}$ where $i = 1,...,m$, the Euclidean distance between the vectors $\vec{u_1}$ and $\vec{u_2}$ can be computed as follows,*

$$\left\| \vec{u_1} - \vec{u_2} \right\|_2 = \left(\sum_{i=1}^{m} \left(u_{i,1} - u_{i,2} \right)^2 \right)^{\frac{1}{2}} \in \mathbb{R}^+. \quad (2)$$

For simplicity, we denote the Euclidean norm of any vector $\vec{u_1} \in \mathbb{R}^m$ as $\left\| \vec{u_1} \right\|$ and the Euclidean distance of the vectors $\vec{u_1}, \vec{u_2} \in \mathbb{R}^m$ as $\left\| \vec{u_1} - \vec{u_2} \right\|$.

Matrices are denoted by using capital letters. For instance, let $m, n \in \mathbb{N}$. Then $B \in \mathbb{R}^{m \times n}$ is an $m \times n$-matrix with elements $b_{i,j} \in \mathbb{R}$ for all $i = 1,...,m$ and $j = 1,...,n$. The matrix B and its entries can be represented as $B = \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \end{bmatrix}$. For any square integer matrix, the inverse of this matrix is not necessarily an integer matrix as well. However, there is an integer square matrix with special property where the inverse of this matrix is guaranteed to be an integer matrix as well. This kind of matrix is called a unimodular matrix.

Definition 4 (Galbraith 2012). *For $n \in \mathbb{N}$, let $U \in \mathbb{Z}^{n \times n}$. If $\det(U) = \pm 1$, then U is a unimodular matrix.*

The lattice $L \subset \mathbb{R}^m$ is defined as follows:

Definition 5 (Galbraith 2012) *For $m, n \in \mathbb{N}$ with $m \ge n$, let $V = \{\vec{v_1},...,\vec{v_n}\}$ be a set of linearly independent vectors $\vec{v_1},...,\vec{v_n} \in \mathbb{R}^m$. The lattice $L \subset \mathbb{R}^m$ that is spanned by the basis V, denoted as $L(V)$, is the set of all integer linear combinations of the vectors $\vec{v_1},...,\vec{v_n}$. It is denoted as follows,*

$$L(V) = \left\{ \sum_{i=1}^{n} a_i \vec{v_i} \,\middle|\, a_i \in \mathbb{Z}, \vec{v_i} \in V \ \forall i = 1,...n \right\}.$$

The set V that spans the lattice L is called the basis for the lattice L and the vectors $\vec{v_1},...,\vec{v_n} \in \mathbb{R}^m$ are referred to as the basis vectors. The number of these basis vectors is called the dimension of the lattice L, denoted as dim (L), and the number of entries in each basis vector is called the rank of the lattice L, denoted as rank (L). If dim (L) = rank (L), then the lattice L is called a full-rank lattice. From here, we only consider full-rank lattices in our further discussion.

Consider a full-rank lattice $L \subset \mathbb{R}^n$ that is spanned by the basis $\{\vec{b_1},...,\vec{b_n}\}$ where $\vec{b_1},...,\vec{b_n} \in \mathbb{R}^n$. The basis $\{\vec{b_1},...,\vec{b_n}\}$ can be represented as a square matrix $B \in \mathbb{R}^{n \times n}$. Since the set $\{\vec{b_1},...,\vec{b_n}\}$ is linearly independent, the matrix B is non-singular with $\det(B) \ne 0$. Now, the lattice L can be represented in the following simpler form, $L = \{B\vec{a} \,|\, \vec{a} \in \mathbb{Z}^n\}$. Other than the basis B, the lattice L also can be spanned by other bases.

Lemma 1 (Galbraith 2012) *For $n \in \mathbb{N}$, let $G, B \in \mathbb{R}^{n \times n}$ be non-singular matrices. The matrices G and B generate the same lattice $L \subset \mathbb{R}^n$, denoted as $L(G) = L(B) = L$, if and only if these matrices are related by a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ such that $G = BU$.*

The orthogonality of lattice basis can be measured by using dual orthogonality-defect as follows,

Definition 6 (Goldreich et al. 1997a) *For* $n \in \mathbb{N}$, *let* $\vec{b_1},...,\vec{b_n} \in \mathbb{R}^n$ *and* $B = \{\vec{b_1},...,\vec{b_n}\}$ *be a basis for the lattice* $L \subset \mathbb{R}^n$. *The dual orthogonality-defect of the basis* B *is*

$$orth_{defect}(B)^* = \frac{\prod_{i=1}^{n} \|\vec{b_i^*}\|}{|\det(B^{-1})|} \quad (3)$$

where $\|\vec{b_i^*}\|$ *is the Euclidean norm of the* i*-th row vector in* B^{-1}.

The Shortest-Vector Problem (SVP) and the Closest-Vector Problem (CVP) are defined as the following:

Definition 7 (Hoffstein et al. 2008) *Given the basis B for a lattice* $L \subset \mathbb{R}^n$, *the Shortest-Vector Problem (SVP) is to find a shortest non-zero vector* $v \in L$ *with minimum Euclidean norm* $\|\vec{v}\|$.

Definition 8 (Hoffstein et al. 2008) *Given the basis B for a lattice* $L \subset \mathbb{R}^n$ *and a target vector* $t \in \mathbb{R}^n$, *the Closest-Vector Problem (CVP) is to find a vector* $w \in L$ *that minimizes the Euclidean distance* $\|\vec{t} - \vec{w}\|$.

GGH CRYPTOSYSTEM

To describe the GGH cryptosystem, consider a communication scenario where Bob wants to send a secret message to Alice, and they decide to use the GGH cryptosystem. As the recipient, Alice initiates her key generation process by choosing a security parameter $n \in \mathbb{N}$ which denotes the dimension of the lattice L. Then, Alice generates her private key as a non-singular matrix $G \in \mathbb{R}^{n \times n}$ that consists of reasonably short and orthogonal basis vectors $\vec{g_1}, \vec{g_2},..., \vec{g_n} \in \mathbb{R}^n$ as its columns. The orthogonality of the generated G will be measured before it can be accepted as the private key. If the value of the dual orthogonality-defect of the generated G is close to 1, then the basis G is accepted as a private key. Otherwise, a new G is generated until the desired orthogonality feature is attained. This is important to ensure that the private basis is a good basis with reasonably short and orthogonal basis vectors. From the accepted private basis G, the value of threshold parameter $\sigma \in \mathbb{N}$ is determined. The threshold parameter σ is required to fulfill the following condition to avoid decryption error:

Theorem 1 (Goldreich et al. 1997a) *Let G be the private basis,* $\rho \in \mathbb{R}^+$ *denotes the maximum* l_1*-norm of the rows of* G^{-1}. *As long as the threshold parameter* $\sigma \in \mathbb{N}$ *satisfies* $\sigma < \frac{1}{2\rho}$, *there is no decryption error can occur*.

Moreover, the public basis $B \in \mathbb{R}^{n \times n}$ is also determined from the private basis G. The basis B is another basis that spans the same lattice L as spanned by the basis G, i.e. $L(G) = L(B) = L \subset \mathbb{R}^n$. According to *Lemma 1*, these bases are mathematically related as $G = BU$ where $U \in \mathbb{Z}^{n \times n}$ is a unimodular matrix. Thus, the public basis B is derived from the private basis G as $B = GU^{-1}$. Unlike the private basis G, the basis B can only be accepted as a public basis if the value of its dual orthogonality defect is far from 1 to ensure that the public basis is a bad basis with long and highly non-orthogonal basis vectors. The generation of the public basis B completes the Alice's key generation process. Thus, the public basis B together with the threshold parameter σ are transmitted to Bob while the private basis G and the unimodular matrix U are kept privately.

Upon receiving the public basis B and the threshold parameters σ from Alice, Bob proceeds with the following steps prior to the encryption process. Firstly, a small vector $\vec{e} \in \mathbb{Z}^n$ is generated by randomly selecting all its entries from the small set $\{-\sigma, +\sigma\}$. Although the value of the σ is considered as public information, the arrangement of the entries $e_i \in \vec{e}$ for all $i = 1,...,n$ is totally determined by Bob. Even Alice does not know the exact arrangement of the entries $-\sigma$ and $+\sigma$ in the vector $\vec{e}$. The small vector $\vec{e}$ is referred to as an error vector. Next, the secret message is encoded into the plaintext vector $\vec{m} \in \mathbb{Z}^n$. Then, the encryption is done as the following,

$$\vec{c} = B\vec{m} + \vec{e} \quad (4)$$

where $\vec{c} \in \mathbb{R}^n$ is a ciphertext vector. Since B is a basis for the lattice L and $\vec{m} \in \mathbb{Z}^n$ is an integer vector, then $B\vec{m} \in L(B) = L$. The ciphertext $\vec{c}$ is transmitted from Bob to Alice.

Upon receiving the ciphertext $\vec{c}$ from Bob, Alice initiates the decryption process by executing the Babai's round-off method using her private basis G. Firstly, the ciphertext $\vec{c}$ is represented as $\vec{c} = G\vec{x}$ where $\vec{x} \in \mathbb{R}^n$ is an unknown vector. The vector $\vec{x}$ is computed as $\vec{x} = G^{-1}\vec{c}$. By using the rounding function as defined in Definition 1, each entry $x_i \in \mathbb{R}$ is rounded for all $i = 1,...,n$ to form an integer vector $[\vec{x}] \in \mathbb{Z}^n$. Finally, the decryption is performed as follows,

$$\vec{m}' = U[\vec{x}] \in \mathbb{Z}^n \quad (5)$$

Effective decryption yields $\vec{m}' = \vec{m}$ where the vector $\vec{m}$ contains the encoded secret message from Bob. This indicates that the decryption process succeeds without error.

Lemma 2 (Goldreich et al. 1997a) *Let G be a private basis, B be a public basis,* $\vec{e}$ *be an error vector and U be a unimodular matrix such that* $G = BU$. *Decryption of the GGH Cryptosystem succeeds if* $[G^{-1}\vec{e}] = \vec{0}$.

The security of the GGH cryptosystem relies on the presumed hardness of the GGH-CVP instance which can be explicitly defined as the following:

Definition 9 (Mandangan et al. 2018) *Let* $n,\sigma \in \mathbb{N}$ *where* n *denotes a lattice dimension and* σ *denotes a threshold parameter respectively,* $B \in \mathbb{R}^{n\times n}$ *be a basis for a full-rank lattice* $L \subset \mathbb{R}^n$, *and* $\vec{c} \in \mathbb{R}^n$ *be a ciphertext vector such that* $c = v + e$ *where* $\vec{v} \in L$ *and* $\vec{e} = \{-\sigma, +\sigma\}^n$ *is an error vector. Given* B, σ *and* $\vec{c}$, *the GGH-CVP instance is a problem to find the lattice vector* $\vec{v}$ *that is located closest to the ciphertext vector* $\vec{c}$ *such that Euclidean distance* $\|\vec{c} - \vec{v}\|$ *is minimum.*

Since $\vec{c} = \vec{v} + \vec{e}$ and the lattice vector $\vec{v}$ is located closest to the ciphertext vector $\vec{c}$, then the Euclidean norm $\|\vec{c} - \vec{v}\| = \|\vec{e}\|$ is minimum. As stated by Nguyen (1999), the norm is $\|\vec{c} - \vec{v}\| = \|\vec{e}\| = \sigma\sqrt{n}$. With this norm, the underlying GGH-CVP instance has been experimentally tested, analyzed and conjectured to be intractable in (Goldreich et al. 1997a). Therefore, we consider $\sigma\sqrt{n}$ as the benchmark norm in the GGH-CVP instance.

THE NGUYEN'S ATTACK

The Nguyen's attack is consisting a sequence of four stages namely the elimination, simplification, reduction and solution stages. The elimination stage aims to obtain partial information from the secret vector $\vec{m} \in \mathbb{Z}^n$ by eliminating the error vector $\vec{e}$ from the encryption equation 4. Since the threshold parameter σ is a public information, the Nguyen's attack generates an integer vector $\vec{s} = \{+\sigma\}^n$. Thus, the following equations hold,

$$\vec{c} + \vec{s} = B\vec{m} + \vec{e} + \vec{s}$$
$$\frac{\vec{c} + \vec{s} - B\vec{m}}{2\sigma} = \frac{\vec{e} + \vec{s}}{2\sigma}. \quad (6)$$

Since $\vec{e} = \{-\sigma, +\sigma\}^n$ and $\vec{s} = \{+\sigma\}^n$, then $\vec{e} + \vec{s} = \{0, 2\sigma\}^n$. Thus, $\frac{\vec{e} + \vec{s}}{2\sigma} = \{0,1\}^n \in \mathbb{Z}^n$. By equation , $\frac{\vec{c} + \vec{s} - B\vec{m}}{2\sigma} \in \mathbb{Z}^n$ as well. This implies that, the following congruence holds

$$\vec{c} + \vec{s} \equiv B\vec{m} \pmod{2\sigma} \quad (7)$$

Observe that, the error vector $\vec{e}$ has been eliminated from the encryption equation. The only unknown value in the congruence (7) is the plaintext vector $\vec{m} \in \mathbb{Z}^n$. Thus, the Nguyen's attack solves the congruence (7) for the unknown vector $\vec{m}$ by computing,

$$\vec{m} \equiv B^{-1}(\vec{c} + \vec{s}) \pmod{2\sigma} \quad (8)$$

where $B^{-1}(\vec{c} + \vec{s}) \bmod 2\sigma = \vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^n$ is the desired partial information by the Nguyen's attack. Since the elimination stage is completed, the attack can proceed to the most crucial stage, which is the simplification of the underlying GGH-CVP instance. In this stage, the vector $B\vec{m}_{2\sigma}$ is inserted into the encryption equation (4) as follows

$$\vec{c} - B\vec{m}_{2\sigma} = B(\vec{m} - \vec{m}_{2\sigma}) + \vec{e}. \quad (9)$$

Since $\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}$, then there exists $\vec{k} \in \mathbb{Z}^n$ such that

$$\vec{m} - \vec{m}_{2\sigma} = 2\sigma\vec{k}. \quad (10)$$

The insertion of the equation (10) into equation (9) yields

$$\frac{\vec{c} - B\vec{m}_{2\sigma}}{2\sigma} = B\vec{k} + \frac{\vec{e}}{2\sigma}. \quad (11)$$

For simplicity, denote $\frac{\vec{c} - B\vec{m}_{2\sigma}}{2\sigma} = \vec{p} \in \mathbb{R}^n$ which is a known vector, $B\vec{k} = \vec{q} \in L$ which is an unknown lattice vector and $\frac{e}{2\sigma} = \vec{\varepsilon} \in \mathbb{R}^n$ which is an unknown vector. Since $\vec{e} = \{-\sigma, +\sigma\}^n$, then

$$\vec{\varepsilon} = \frac{\vec{e}}{2\sigma} = \left\{-\frac{\sigma}{2\sigma}, +\frac{\sigma}{2\sigma}\right\}^n = \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n. \quad (12)$$

Obviously, the vector $\vec{\varepsilon}$ is smaller than the error vector $\vec{e}$. The equation can be rewritten as $\vec{p} = \vec{q} + \vec{\varepsilon}$. From this equation, a new GGH-CVP instance can be defined as follows:

Definition 10 (Mandangan et al. 2018) *For* $n \in \mathbb{N}$, *let* $B \in \mathbb{R}^{n\times n}$ *be a basis for a full-rank lattice* $L \subset \mathbb{R}^n$, $\vec{p} \in \mathbb{R}^n$ *be a target vector and* $\vec{\varepsilon} = \left\{-\frac{1}{2}, +\frac{1}{2}\right\}^n$ *be an error vector such that* $\vec{p} = \vec{q} + \vec{\varepsilon}$ *where* $\vec{q} \in L$. *Given B and* $\vec{P}$, *the* Nguyen$_{\text{GGH}}$*-CVP instance is a problem to find the lattice vector* $\vec{q}$ *that is located closest to the target vector* $\vec{P}$ *such that Euclidean distance* $\|\vec{p} - \vec{q}\|$ *is minimum.*

As stated by Nguyen (1999), the Euclidean norm $\|\vec{p} - \vec{q}\| = \frac{\sqrt{n}}{2}$. It is much shorter than the benchmark norm $\sigma\sqrt{n}$. Consequently, the Nguyen$_{\text{GGH}}$-CVP instance becomes easier to be solved compared to the original GGH-CVP instance. The remaining stages of the Nguyen's attack are the reduction and solution stages. In the reduction stage, an embedding technique is used to reduce the Nguyen$_{\text{GGH}}$-CVP instance into an SVP instance. Finally, the derived SVP instance is solved in the solution stage by using high quality lattice reduction algorithms.

COUNTERMEASURE AGAINST THE NGUYEN'S ATTACK

To strengthen the security of the GGH Cryptosystem, the flaw that is exploited by the Nguyen's attack must be repaired. For that purpose, we proposed a countermeasure to prevent the elimination stage of the Nguyen's attack by making the congruence $\vec{c} + \vec{s} \equiv B\vec{m} \pmod{2\sigma}$ does not hold anymore. The proposed countermeasure is given in the following lemma:

Lemma 3 For $n,\sigma \in \mathbb{N}$ *where* $\sigma > 2$ *, let* $B \in \mathbb{R}^{n\times n}$ *be a public basis,* $\vec{m} \in \mathbb{Z}^n$ *be a plaintext vector,* $\vec{c} \in \mathbb{R}^n$ *be a cipher text vector,* $\vec{e} \in \mathbb{Z}^n$ *be an error vector and* $s = \{+\sigma\}^n$ *be an integer vector such that* $\vec{c} + \vec{s} = B\vec{m} + \vec{e} + s$. *If all entries of the vector* $\vec{e}$ *are selected randomly from the set* $E = \{(\sigma-2),(\sigma-1),\sigma,(\sigma+1)\}$, *then* $\vec{c} + \vec{s} \not\equiv B\vec{m} \pmod{2\sigma}$.

Proof

Assume that all entries of $\vec{e}$ are selected randomly from the set $E = \{(\sigma-2),(\sigma-1),\sigma,(\sigma+1)\}$ where first four entries of $\vec{e}$ as $e_1 = (\sigma-2), e_2 = (\sigma-1), e_3 = \sigma, e_4 = (\sigma+1)$ and last entry as $e_n = (\sigma-2)$. Thus,

$$\frac{\vec{e}+\vec{s}}{2\sigma} = \frac{1}{2\sigma}\left(\begin{bmatrix}\sigma-2\\ \sigma-1\\ \sigma\\ \sigma+1\\ \vdots\\ \sigma-2\end{bmatrix} + \begin{bmatrix}\sigma\\ \sigma\\ \sigma\\ \sigma\\ \vdots\\ \sigma\end{bmatrix}\right) = \frac{1}{2\sigma}\begin{bmatrix}2\sigma-2\\ 2\sigma-1\\ 2\sigma\\ 2\sigma+1\\ \vdots\\ 2\sigma-2\end{bmatrix} = \begin{bmatrix}1-\frac{1}{\sigma}\\ 1-\frac{1}{2\sigma}\\ 1\\ 1+\frac{1}{2\sigma}\\ \vdots\\ 1-\frac{1}{\sigma}\end{bmatrix} \notin \mathbb{Z}^n$$

since $\sigma \in \mathbb{N}$ and $\sigma > 2$. Given that $\vec{c} + \vec{s} = B\vec{m} + \vec{e} + \vec{s}$. Thus, the following equation holds,

$$\frac{c+s-Bm}{2\sigma} = \frac{e+s}{2\sigma}.$$

Since $\frac{\vec{e}+\vec{s}}{2\sigma} \notin \mathbb{Z}^n$, then $\frac{\vec{c}+\vec{s}-B\vec{m}}{2\sigma} \notin \mathbb{Z}^n$ as well. This implies that $c + s \not\equiv B\vec{m} \pmod{2\sigma}$.

Now, we demonstrate the effect of the proposed countermeasure in the following example:

Example 1 Consider two different sets $E_1 = \{-\sigma, +\sigma\}$ and $E_2 = \{(\sigma-2),(\sigma-1),\sigma,(\sigma+1)\}$. Let $n = 10, \sigma = 3$. Then $E_1 = \{-3, 3\}$ and $E_2 = \{1, 2, 3, 4\}$. Suppose that $\vec{e} = [3\ \ 3\ \ -3\ \ 3\ \ 3\ \ -3\ \ 3\ \ 3\ \ -3\ \ 3]^T$ where $e_i \in E_1$ for all $e_i \in e$ where i = 1, ..., 10. Thus,

$$\frac{\vec{e}+\vec{s}}{2\sigma} = \frac{1}{2(3)}\left(\begin{bmatrix}3\\ 3\\ -3\\ 3\\ 3\\ -3\\ 3\\ 3\\ -3\\ 3\end{bmatrix} + \begin{bmatrix}3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\end{bmatrix}\right) = \frac{1}{6}\begin{bmatrix}6\\ 6\\ 0\\ 6\\ 6\\ 0\\ 6\\ 6\\ 0\\ 6\end{bmatrix} = \begin{bmatrix}1\\ 1\\ 0\\ 1\\ 1\\ 0\\ 1\\ 1\\ 0\\ 1\end{bmatrix} \in \mathbb{Z}^{10}$$

which leads to the formation of the congruence $\vec{c} + \vec{s} \equiv B\vec{m} \pmod{2\sigma}$ by the Nguyen's attack. Now, suppose that $\vec{e} = [2\ \ 4\ \ 2\ \ 4\ \ 2\ \ 4\ \ 1\ \ 3\ \ 2\ \ 4]^T$ where $e_i \in E_2$ for all $e_i \in \vec{e}$ i = 1, ..., 10. Thus,

$$\frac{\vec{e}+\vec{s}}{2\sigma} = \frac{1}{2(3)}\left(\begin{bmatrix}2\\ 4\\ 2\\ 4\\ 2\\ 4\\ 1\\ 3\\ 2\\ 4\end{bmatrix} + \begin{bmatrix}3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\\ 3\end{bmatrix}\right) = \frac{1}{6}\begin{bmatrix}5\\ 7\\ 5\\ 7\\ 5\\ 7\\ 4\\ 6\\ 5\\ 7\end{bmatrix} \notin \mathbb{Z}^{10}$$

This implies that, $c + s \not\equiv B\vec{m} \pmod{2\sigma}$.

In the following lemma, we proposed a strategy to maintain the Euclidean norm $\|\vec{e}\|$ as well as the Euclidean distance $\|\vec{c} - B\vec{m}\|$ as $\sigma\sqrt{n}$.

Lemma 4 Suppose that $n,\sigma,k,t \in \mathbb{N}$ *where* $\sigma > 2, k = 4\sigma - 2$ *and* $n = kt$. *Let* $B \in \mathbb{R}^{n\times n}$ *be a public basis,* $\vec{m} \in \mathbb{Z}^n$ *be a plaintext vector with encoded secret message,* $\vec{c} \in \mathbb{R}^n$ *be a ciphertext vector and* $\vec{e} \in \mathbb{Z}^n$ *be an error vector which is related as* $\vec{c} = B\vec{m} + \vec{e}$. *If all the entries of the error vector* e *are selected randomly from the set* $E = \{(\sigma-2),(\sigma-1),\sigma,(\sigma+1)\}$ *based on the following distributions for all* $i = 1,...,n$,

$$e_i = \begin{cases} (\sigma-2), \text{ for } \frac{n}{k} \text{ number of entries,} \\ (\sigma-1), \text{ for } \frac{(k-2)n}{2k} \text{ number of entries,} \\ \sigma, \text{ for } \frac{n}{k} \text{ number of entries,} \\ (\sigma+1), \text{ for } \frac{(k-2)n}{2k} \text{ number of entries,} \end{cases}$$

then $\|\vec{c} - B\vec{m}\| = \|\vec{e}\| = \sigma\sqrt{n}$.

Proof

Since $e_i + e_j = e_j + e_i$ for all $i, j = 1,...,n$ and $i \neq j$, then the entries with equal value can be accumulated together as follows,

$$\|\vec{c} - B\vec{m}\| = \|\vec{e}\|$$

$$= \sqrt{\sum_{i=1}^{\frac{n}{k}}(\sigma-2)_i^2 + \sum_{i=1}^{\frac{(k-2)n}{2k}}(\sigma-1)_i^2 + \sum_{i=1}^{\frac{n}{k}}(\sigma)_i^2 + \sum_{i=1}^{\frac{(k-2)n}{2k}}(\sigma+1)_i^2}$$

$$= \sqrt{\frac{n}{k}(\sigma-2)^2 + \frac{(k-2)n}{2k}(\sigma-1)^2 + \frac{n}{k}\sigma^2 + \frac{(k-2)n}{2k}(\sigma+1)^2}$$

$$= \sqrt{n\left(\frac{k\sigma^2 - 4\sigma + k + 2}{k}\right)}$$

Since $k = 4\sigma - 2$, therefore

$$\|\vec{c} - B\vec{m}\| = \sqrt{n\left(\frac{(4\sigma-2)\sigma^2 - 4\sigma + (4\sigma-2) + 2}{(4\sigma-2)}\right)} = \sqrt{n\left(\frac{(4\sigma-2)\sigma^2}{4\sigma-2}\right)}$$

$$= \sqrt{n\sigma^2} = \sigma\sqrt{n}.$$

We combine the results of the Lemma 3 and Lemma 4 in the following theorem:

Theorem 2 Consider the setup for the GGH cryptosystem as described in Lemma 4. By implementing this setup, the GGH cryptosystem does not affected by the Nguyen's attack anymore.

Proof

In *Lemma 3*, we proved that $\vec{c}+\vec{s} \not\equiv B\vec{m} \pmod{2\sigma}$ once the entries of the error vector e are randomly selected from the proposed set $E=\{(\sigma-2),(\sigma-1),\sigma,(\sigma+1)\}$ instead of the original set $\{-\sigma,+\sigma\}$. That means, $\vec{c}+\vec{s} \not\equiv B\vec{m} \pmod{2\sigma}$ could not be solved for the plaintext vector $\vec{m} \in \mathbb{Z}^n$ to obtain the partial information $\vec{m}_{2\sigma} \in \mathbb{Z}_{2\sigma}^n$ such that $\vec{m} \equiv \vec{m}_{2\sigma} \pmod{2\sigma}$. Without the vector $\vec{m}_{2\sigma}$, the Nguyen's attack could not proceed to its simplification stage. Therefore, the GGH-CVP instance remains in its original form. In the GGH-CVP instance, the Euclidean norm $\|\vec{c}-B\vec{m}\| = \|\vec{e}\| = \sigma\sqrt{n}$ since $\vec{e} = \{-\sigma,+\sigma\}^n$. With norm $\sigma\sqrt{n}$, the GGH cryptosystem has been experimentally tested, analyzed and conjectured by Goldreich et al. (1997a) as intractable in the lattice dimensions of 300 and beyond. As proved in *Lemma 4*, the Euclidean norm $\|\vec{c}-B\vec{m}\| = \|\vec{e}\|$ is maintained as $\sigma\sqrt{n}$ once the entries of the error vector e are randomly chosen from the set E and distributed based on the proposed distributions. Therefore, the GGH cryptosystem is considered surviving against the Nguyen's attack.

In the following theorem, we prove that the decryption of the upgraded GGH cryptosystem works effectively without error.

Theorem 3 Consider the setup for the GGH cryptosystem as described in Lemma 4. Then, let $G \in \mathbb{R}^{n\times n}$ be the private basis and $\rho \in \mathbb{R}^+$ denotes the maximum l_1-norm of the rows in $G^{-1} \in \mathbb{R}^{n\times n}$ such that $\sigma < \frac{1}{2\rho}$. Then, the decryption of the GGH cryptosystem can be done without an error.

Proof

As stated in *Lemma 2*, decryption error in the GGH cryptosystem can be avoided when $\lceil G^{-1}\vec{e} \rfloor = \vec{0}$. For simplicity, denote $G^{-1}\vec{e} = \vec{r} \in \mathbb{R}^n$. To obtain $\lceil \vec{r} \rfloor = \vec{0}$, it is required that $|r_i| < \frac{1}{2}$ for all $i = 1,...,n$. Since $G \in \mathbb{R}^{n\times n}$ is a private basis, then G is a non-singular square matrix. There exists an inverse matrix G^{-1} such that $GG^{-1} = I$ where $I \in \mathbb{Z}^{n\times n}$ is an identity matrix. Represent the elements of the matrix G^{-1} as

$$G^{-1} = \begin{bmatrix} g_{1,1}^* & g_{1,2}^* & \cdots & g_{1,n}^* \\ g_{2,1}^* & g_{2,2}^* & \cdots & g_{2,n}^* \\ \vdots & \vdots & \ddots & \vdots \\ g_{n,1}^* & g_{n,2}^* & \cdots & g_{n,n}^* \end{bmatrix}.$$

Thus, $\vec{r} = G^{-1}\vec{e}$. In vectors and matrix form, we have

$$\begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} g_{1,1}^* & g_{1,2}^* & \cdots & g_{1,n}^* \\ g_{2,1}^* & g_{2,2}^* & \cdots & g_{2,n}^* \\ \vdots & \vdots & \ddots & \vdots \\ g_{n,1}^* & g_{n,2}^* & \cdots & g_{n,n}^* \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} g_{1,1}^* e_1 + g_{1,2}^* e_2 + \cdots + g_{1,n}^* e_n \\ g_{2,1}^* e_1 + g_{2,2}^* e_2 + \cdots + g_{2,n}^* e_n \\ \vdots \\ g_{n,1}^* e_1 + g_{n,2}^* e_2 + \cdots + g_{n,n}^* e_n \end{bmatrix}.$$

For $y \in \mathbb{N}$ and $1 \le y \le n$, suppose that the y-th row of the G^{-1} has the maximum l_1-norm. Consider the y-th entry of the vector r as follows,

$$|r_y| = |g_{y,1}^* e_1 + g_{y,2}^* e_2 + g_{y,3}^* e_3 + g_{y,4}^* e_4 + \cdots + g_{y,n}^* e_n|.$$

Suppose that the first four entries of the error vector $\vec{e}$ are chosen as $e_1 = (\sigma-2), e_2 = (\sigma-1), e_3 = \sigma$ and $e_4 = (\sigma+1)$. Then,

$$\begin{aligned} |r_y| &= |g_{y,1}^*(\sigma-2) + g_{y,2}^*(\sigma-1) + g_{y,3}^*\sigma + g_{y,4}^*(\sigma+1) + \cdots + g_{y,n}^* e_n| \\ &= (\sigma-2)|g_{y,1}^*| + (\sigma-1)|g_{y,2}^*| + \sigma|g_{y,3}^*| + (\sigma+1)|g_{y,4}^*| + \cdots + e_n|g_{y,n}^*| \\ &= \sigma|g_{y,1}^*| - 2|g_{y,1}^*| + \sigma|g_{y,2}^*| - |g_{y,2}^*| + \sigma|g_{y,3}^*| + \sigma|g_{y,4}^*| + |g_{y,4}^*| + \cdots + e_n|g_{y,n}^*| \\ &= \sigma|g_{y,1}^*| + \sigma|g_{y,2}^*| + \sigma|g_{y,3}^*| + \sigma|g_{y,4}^*| + \cdots + \sigma|g_{y,n}^*| - 2|g_{y,1}^*| - |g_{y,2}^*| + |g_{y,4}^*| + \cdots \\ &= \sigma\left(|g_{y,1}^*| + |g_{y,2}^*| + |g_{y,3}^*| + |g_{y,4}^*| + \cdots + |g_{y,n}^*|\right) - \left(2|g_{y,1}^*| + |g_{y,2}^*| - |g_{y,4}^*| + \cdots\right) \\ &= \sigma\rho_y - \tilde{\rho}_y \end{aligned}$$

where $\tilde{\rho}_y < \rho_y$. Since ρ is the maximum l_1-norm of the rows in G^{-1} and $\sigma < \frac{1}{2\rho}$, then

$$\tilde{\rho}_y < \rho_y < \rho < \frac{1}{2\sigma}.$$

Hence,

$$|r_y| < \sigma\rho - \rho$$

$$|r_y| < \sigma\left(\frac{1}{2\sigma}\right) - \frac{1}{2\sigma}$$

$$|r_y| < \frac{1}{2} - \frac{1}{2\sigma}.$$

Since $\sigma \in \mathbb{N}$ and $\sigma > 2$, therefore

$$|r_y| < \frac{1}{2}.$$

Decryption of the GGH cryptosystem is done as follows,

$$\begin{aligned} \vec{m}' &= U\left[G^{-1}\vec{c}\right] \\ &= U\left[G^{-1}\left(B\vec{m}+\vec{e}\right)\right], \text{ since } \vec{c} = B\vec{m}+\vec{e} \\ &= \left[B^{-1}GG^{-1}B\vec{m}\right] + U\left[G^{-1}\vec{e}\right], \text{ since } G = BU \\ &= \vec{m} + U\left[G^{-1}\vec{e}\right], \text{ since } BB^{-1} = GG^{-1} = I \text{ and } \vec{m} \in \mathbb{Z}^n \end{aligned}$$

For all $i = 1,...,n$, we showed that $|r_y| < \frac{1}{2}$ where $r_i \in \vec{r}$ and $\vec{r} = G^{-1}\vec{e}$. This implies that $\lceil G^{-1}\vec{e} \rfloor = \vec{0}$. Therefore, $\vec{m}' = \vec{m} + U(\vec{0}) = \vec{m}$ which indicates that no decryption error occurs.

DISCUSSION AND CONCLUSION

We proposed a countermeasure to upgrade the security of the GGH cryptosystem against the fatal attack on it, which is the Nguyen's attack. The proposed countermeasure is applicable for any value of threshold parameter $\sigma > 2$ and not only limited to the standard choice of $\sigma = 3$. Without major alteration on the original design of the GGH cryptosystem, the security reliance

of the cryptosystem on the original GGH-CVP instance is maintained. However, thorough security analyses on upgraded GGH cryptosystem is demanded to build more confidence on it. Current technology and sophisticated attacks including the lattice reduction algorithms must be taken into consideration. With its efficiency, practicality and upgraded security features, we are optimistic that the GGH cryptosystem could be one of the most competitive lattice-based cryptosystems.

ACKNOWLEDGEMENTS

The present research is partially supported by the Putra-Grant - GP/2017/9552200 and supported by Universiti Sains Malaysia, Universiti Malaysia Sabah and the Ministry of Education, Malaysia.

REFERENCES

Ajtai, M. & Dwork, C. 1997. A public-key cryptosystem with worst-case/average-case equivalence. *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing.* El Paso, Texas. pp. 284-293.

Barros, C.F.de. & Schechter, L.M. 2014. GGH may not be dead after all. *Proceedings of XXXV Brazilian National Congress in Applied and Computational Mathematics (CNMAC2014)*. Natal, Brazil.

Elgamal, T. 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transaction on Information Theory* 31(4): 469-472.

Galbraith, S.D. 2012. *Mathematics of Public Key Cryptography*. 1st ed. New York: Cambridge University Press.

Goldreich, O., Goldwasser, S. & Halevi, S. 1997a. Public-key cryptosystems from lattice reduction problems. *Proceedings of 17th Annual International Cryptology Conference.* Santa Barbara, California, USA. pp. 112-131.

Goldreich, O., Goldwasser, S. & Halevi, S. 1997b. *Challenges for the GGH Cryptosystem.* http://groups.csail.mit.edu/cis/lattice/challenge.html.

Hoffstein, J., Pipher, J. & Silverman, J.H. 1998. NTRU: A new high-speed public key cryptosystem. *Proceedings of the Third International Algorithmic Number Theory Symposium, ANTS'98*. pp. 267-288.

Hoffstein, J., Pipher, J. & Silverman, J.H. 2008. *An Introduction to Mathematical Cryptography.* New York: Springer-Verlag.

Ismail, E.S. & Hasan, Y.A. 2006. A new version of ElGamal signature scheme. *Sains Malaysiana* 35(2): 69-72.

Jaju, S.A. & Chowhan, S.S. 2015. A modified RSA algorithm to enhance security for digital signature. *2015 International Conference and Workshop on Computing and Communication (IEMCON)*. Vancouver, Canada. pp. 1-5.

Koblitz, N. 1987. Elliptic curve cryptosystems. *Mathematics of Computation* 48(177): 203-209.

Lyubashevsky, V., Peikert, C. & Regev, O. 2010. On ideal lattices and learning with errors over rings. *Annual International Conference on the Theory and Applications of Cryptographic Techniques.* Berlin, Heidelberg. pp. 1-23.

Mandangan, A., Kamarulhaili, H. & Asbullah, M.A. 2019. On the smallest-basis problem underlying the GGH lattice-based cryptosystem. *Malaysian Journal of Mathematical Sciences* 13(S): 1-11.

Mandangan, A., Kamarulhaili, H. & Asbullah, M.A. 2018. On the underlying hard lattice problems of GGH encryption scheme. *Proceedings of the* 6th International *Cryptology and Information Security Conference 2018 (CRYPTOLOGY2018)*. Port Dickson, Negeri Sembilan, Malaysia. pp. 42-50.

Micciancio, D. & Regev, O. 2009. Lattice-based cryptography. In *Post-Quantum Cryptography*, edited by Bernstein, D.J., Buchmann, J. & Dahmen, E. Berlin, Heidelberg: Springer.

Nguyen, P. 1999. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97. In *Advances in Cryptology - CRYPTO' 99*, edited by Wiener, M. Berlin, Heidelberg: Springer.

Pol, J.H.v.d. 2011. Lattice-based cryptography. Master of Science Theses, Eindhoven University of Technology (Unpublished).

Regev, O. 2005. On lattices, learning with errors, random linear codes, and cryptography. *Stoc '05: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*. Baltimore, MD, USA. pp. 84-93.

Rivest, R.L., Shamir, A. & Adleman, L. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21(2): 120-126.

Schnorr, C.P., Fischlin, M., Koy, H. & May, A. 1997. Lattice attacks on GGH Cryptosystem. *Rump session of Crypto '97*.

Serre, D.N. 2010. *Matrices: Theory and Applications*. 2nd ed. Heidelberg London: Springer-Verlag.

Shor, P.W. 1994. Algorithms for quantum computation: Discrete logarithms and factoring. *35th Annual Symposium on Foundations of Computer Science.* Santa Fe, NM, USA. pp. 124-134.

Yoshino, M. & Kunihiro, N. 2012. Improving GGH cryptosystem for large error vector. *Information Symposium on Information Theory and its Applications (ISITA).* pp. 416-420.

Zazali, H.H. & Othman, W.A.M. 2012. Key exchange in Elliptic Curve Cryptography based on the decomposition problem. *Sains Malaysiana* 41(7): 907-910.

Arif Mandangan & Hailiza Kamarulhaili
School of Mathematical Sciences
Universiti Sains Malaysia
11800 USM Penang, Pulau Pinang
Malaysia

Arif Mandangan
Mathematics, Real Time Graphics and Visualization Laboratory
Faculty of Sciences & Natural Resources
Universiti Malaysia Sabah
Jalan UMS
88400 Kota Kinabalu, Sabah
Malaysia

Muhammad Asyraf Asbullah*
Laboratory of Cryptography Analysis and Structure
Institute for Mathematical Sciences
Universiti Putra Malaysia
43400 UPM Serdang, Selangor Darul Ehsan
Malaysia

Muhammad Asyraf Asbullah*
Centre of Foundation Studies for Agricultural Science
Universiti Putra Malaysia
43400 UPM Serdang, Selangor Datul Ehsan
Malaysia

*Corresponding author; email: ma_asyraf@upm.edu.my

Received: 9 August 2019
Accepted: 12 February 2020