International Journal of Cryptology Research 6(1): 64 - 78 (2016)

A Review on Lattice Based Cryptography Resistance to Quantum Computing

Syaiful Azman Muhammad*[1] and **Hailiza Kamarulhaili**[2]

[1]*School of Mathematical Sciences, UniversitiSains Malaysia, 11800 USM Pulau Pinang, Malaysia*

E-mail: s.azmanmuhammad@gmail.com
hailiza@usm.my
**Corresponding author*

ABSTRACT

To run Shors algorithm or any other code breaking algorithm on quantum computing machine will make most of the cryptographic hard problems such as the integer factorization problem or discrete logarithm problem collapses. These hard problems include the prominent RSA (Rivest, Shamir, Adleman) and Elliptic Curve cryptosystem. Meaning, these problems can be solved in a polynomial time on a quantum computer. However a lattice based cryptosystem is believed to be resistance to this powerful machine. Thus, in this paper, we give a review on lattice concept including fundamental parallelepiped, successive minima and LWE (learning with error). Most of the contents in this paper are focusing on successive minima where the shortest vector problem(SVP) is discussed while the issue on LWE discussed mainly on the properties and its hardness.

Keywords: Shortest vector problem(SVP), learning with error(LWE), successive minima, lattice.

1 INTRODUCTION

Though quantum computing has not been utilized as widely as it possibly can, but the cryptographers are now warned of the possibility of a huge impact on the existing cryptographic protocols and techniques. This huge impact affects several cryptographic algorithms that if the existing algorithms to crack the given techniques were to run on this powerful machine, the whole security system will be jeopardized.

Richard Feynman in 1980s, had introduced the conceptual idea of making possible improvement in speed that might be achieved by a quantum computer. However, this theoretical physics is just the first step for us to make it possible to be applied in the real world. While the first Intel processor are made up of 2300 transistors in 1971, now they are already capable of producing a microprocessor with more than 5 billion transistor. But still this processors are still limited since it depends on the simple binary option which is 0 and 1. In contrast to quantum computer, the bits is call qubits where the idea of subatomic realm of quantum physics has been applied. In subatomic realm a particle can act like a wave so that they can be a wave or a particle or particle and wave. As a result, a qubit can be 1 or 0 or 1 and 0 which make it possible to perform two equation at the same time. On the other word, we could say that the quantum computer will perform faster than a classical computer.

By knowing all those things, it is really crucial for us to think about the future of cryptography. As we all know, today RSA (Rivest, Shamir and Adlemann) cryptography has been used widely to secure all the information on the internet. Since the RSA is based on the integer factorization problem, it is known to be resistance to the classical computer. However, by using Shors algorithm on the quantum computer, it will make the integer factorization problem easy to solve in no time. Thus, it is very crucial to think about the alternative for the RSA.

There are several cryptosystem known to be resistance to the quantum computer. They are mainly from the fields of lattice theory, coding theory and the study of multivariate quadratic polynomials. Among all computational problem that are believed to be quantum resistance, lattice based problem is seems to receive the most attention during the past decade. This happen to be that way because the lattice based algorithm is very fast compared to the other algorithm.

The core problem for a lattice problem is to find the shortest vector within a lattice namely Shortest vector Problem (SVP). This problem is known to be non-deterministic polynomial time hard (NP-hard) and of course, unlike the RSA there is no known quantum algorithm to solve SVP with the help of quantum computer. Among all the lattice based cryptosystem, the number theory research unit (NTRU) cryptosystem and also LWE is the most promising cryptosystem.

This paper is organized as follows; the mathematical description of the lattices and its definition is described in Section 2. The computational problem including SVP is being stated in Section 3. The properties and the hardness of LWE is discussed in Section 4. Section 5 is the conclusion.

2 SOME PROPERTIES ON LATTICES

The following are definitions of lattices and parallelepiped respectively. One needs to have some familiarization of vector concept or linear algebra.

Definition 2.1. *(Galbraith, 2012) Let R^m be the m dimensional Euclidean space. A lattice in R^m is the set of*

$$L(b_1, b_2, \dots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \in Z \right\} \tag{1}$$

where the sequence of vector $b_1, b_2, \dots, b_n$ is called a basis vector of lattice.

By using the definition of lattice, we can equivalently defined B as the $n \times m$ matrix whose row are $b_1, b_2, \dots, b_n$, where the lattice generated by B is

$$L(B) = L(b_1, b_2, \dots, b_n) = \{xB \mid x \in Z^n\} \tag{2}$$

where n is lattice rank and m lattice dimension. If n=m , then L is called a full rank lattice.

Definition 2.2. *(A.Nitaj, 2011) Let L be a lattice with basis $(b_1, b_2, \ldots, b_n)$. The fundamental domain or parallelepiped for L is the set*

$$P(b_1, b_2, \ldots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \mid 0 \leq i < 1 \right\} \tag{3}$$

The range of x_i can be any other translation of [0,1), such as $\left[-\frac{1}{2}, \frac{1}{2}\right)$ where the size must be 1. Also it is clear that, $P(b_1, b_2, \ldots, b_n)$ is depending on the basis $(b_1, b_2, \ldots, b_n)$. The best way to choose basis $(b_1, b_2, \ldots, b_n)$ is to make sure that they will form a square parallelepiped. The crucial part is how to choose a set of vector so that it will be a basis for a lattice. Thus the following lemma will be used.

Lemma 2.1. *(J.V.D, 2011) Let $L \subset R^m$ be a lattice with rank n and let $b_1, b_2, ..., b_n \in L$ be n linearly independent lattice vector. Then $b_1, b_2, \ldots, b_n$ will form a basis of L if and only if $P(b_1, b_2, \ldots, b_n) \cap L$=$\{0\}$*

From this lemma, we can see that the parallelepiped $P(b_1, b_2, ..., b_n)$ is the set of linear combination of $b_1, b_2, \ldots, b_n$ with coefficient in [0,1), while the lattice L is the set of all their integer combination. By adding both of this set, we can clearly see that it contains all the real coefficient that cover R^m. Hence we also can write this as R^m=$\bigcup_{v \in L} (v + P(B))$

Now if we let $v_1, v_2 \in L$ and we suppose that $(v_1+P(B)) \cap (v_2+P(B)) \neq \emptyset$ for some $v_1 \neq v_2 \in L$, then we surely can have $v_1 + a = v_2 + b$ and hence $v_1 - v_2 = b - a$ where $a, b \in P(B)$. Noticed that $0 \leq a < 1$ and $0 \leq b < 1$, thus $a - b \in (-1, 1)$ and hence there is only one possible outcome we could have which is $v_1 - v_2 = 0 = b - a$.Similarly, if we do the same thing with $a, b \in P(B)$ by using $\left[-\frac{1}{2}, \frac{1}{2}\right)$ as the range of a and b, we can have $a - b \in (-1, 1)$. Since a and b is real coefficient, while v_1 and v_2 is integer coefficient, Then $v_1 - v_2 = 0 = b - a$.(Chi et al.)

Thus, the intersection between this two set is clearly $\{0\}$ which implies that, only the origin will be in the parallelepiped. Therefore, the lattice vector of parallelepiped that covers R^m will never overlap. Hence it is very clear that the range of x_i must contain 0, that is, $1 \leq x_i < 2$ cannot be used because it is does not contain 0.

The following lemma shows us that in a lattice L with $n \geq 2$, there will surely have a couple of bases that are related to some unimodular matrix U and hence telling us that the basis is not unique.

Lemma 2.2. *(A.Nitaj, 2011) Let $L \subset R^m$ be a lattice of rank n. Let $b_1, b_2, \ldots, b_n$ and $b'_1, b'_2, \ldots, b'_n$ be two bases of L. Then, there exist $n \times n$ matrix U with entries in Z and the* $\det(U)$=± 1 *such that*

$$\begin{bmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_n \end{bmatrix} = U \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \tag{4}$$

Proof. This prove can be found in (A.Nitaj, 2011). This prove is written here so that we could see that how the given two bases is equivalent.

Let $b_1, b_2, \ldots, b_n$ and $b'_1, b'_2, \ldots, b'_n$ be a bases of L. By the definition, every vector $b'_i \in L$, then we could have

$$\begin{bmatrix} b'_1 \\ b'_2 \\ \vdots \\ b'_n \end{bmatrix} = \begin{bmatrix} u_{11}b_1 + u_{12}b_2 + \ldots + u_{1n}b_n \\ u_{21}b_1 + u_{22}b_2 + \cdots + u_{2n}b_n \\ \vdots \\ u_{n1}b_1 + u_{n2}b_2 + \cdots + u_{nn}b_n \end{bmatrix} \tag{5}$$

$$= \begin{bmatrix} u_{11} & u_{12} & \ldots & u_{1n} \\ u_{21} & u_{22} & \ldots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n1} & u_{n2} & \ldots & u_{nn} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \tag{6}$$

$$= U \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \tag{7}$$

Where U is $n \times n$ matrix with integer entries. This can be written as

$$(b'_1, b'_2, \ldots, b'_n)^t \;=\; U(b_1, b_2, \ldots, b_n)^t \tag{8}$$

Similarly, we also can have a $n \times n$ matrix with integer entries such that

$$(b_1, b_2, \ldots, b_n)^t \;=\; U(b'_1, b'_2, \ldots, b'_n)^t \tag{9}$$

Hence,

$$(b'_1, b'_2, \ldots, b'_n)^t \;=\; UU(b'_1, b'_2, \ldots, b'_n)^t \tag{10}$$

Which implies that,UU'=I_n where I_n is a $n \times n$ identity matrix. Thus we will have $\det(U)\det(U')$=1. Hence we can have $\det(U)$=det(U')=±1. □

According to the proof of this lemma, we know that for the case $(b'_1, b'_2, \ldots, b'_n)^t = U(b_1, b_2, \ldots, b_n)^t$, we will have $L(b_1, b_2, \ldots, b_n)^t \subset L(b'_1, b'_2, \ldots, b'_n)^t$ while for the case $(b_1, b_2, \ldots, b_n)^t = U^{-1}(b'_1, b'_2, \ldots, b'_n)^t$ we will have $L(b'_1, b'_2, \ldots, b'_n)^t \subset L(b_1, b_2, \ldots, b_n)^t$ and hence we will have $L(b_1, b_2, \ldots, b_n)^t = L(b'_1, b'_2, \ldots, b'_n)^t$ or in the other words, $(b_1, b_2, \ldots, b_n)$ and $(b'_1, b'_2, \ldots, b'_n)$ is equivalent and generate the same lattice.

Definition 2.3. *(A.Nitaj, 2011) Let L be a lattice with basis $(b_1, b_2, \ldots, b_n)$. The determinant or volume of L is*

$$\det(L) = \sqrt{\det(BB^t)} \tag{11}$$

Where B is $n \times m$ matrix of form by the row of basis.

The determinant of L is independent of our choice of basis. If B and B' is a basis of L, then by using lemma 1.2, where $B' = UB$ we will have

$$\sqrt{\det(B'B'^t)} = \sqrt{\det(UBB^tU^t)} = \sqrt{\det(BB^t)} \tag{12}$$

In addition, the determinant of L is the volume of the parallelepiped. Thus, the determinant of lattice is inversely proportional to its density. In the other word, the smaller the determinant the denser the lattice.

3 LATTICE COMPUTATIONAL PROBLEM

Problem involving inner product of the vector and distance minimization has been a centre of discussion in lattice based computations. An intuitive way to measure a distance in a lattice is by using Euclidean norm. Thus the following definition is useful here.

Definition 3.1. *(A.Nitaj, 2011) Let* $u = (u_1, u_2, \ldots, u_n)$ *and* $v = (v_1, v_2, \ldots, v_n)$ *be two vector of* R^m *. Then*

1. *The inner product of u and v is*

$$\langle u, v \rangle = u^T v = \sum_{i=1}^{n} u_i v_i \tag{13}$$

2. *The Eucledean norm of* u *is*

$$\|u\| = (\langle u, v \rangle)^{\frac{1}{2}} = \left(\sum_{i=1}^{n} u_i^2 \right)^{\frac{1}{2}} \tag{14}$$

Lattice has been used widely in the cryptography by using it for analysing the security of several cryptosystem such as NTRU and LWE. These cryptosystem are mainly using the minima distance and shortest nonzero vectors as its computational problems. Thus, the following definitions also will be needed to understand further on the lattice problem.

Definition 3.2. *(A.Nitaj, 2011) Let* L *be a lattice. The minimal distance* λ_1 *of* L *is the length of the shortest nonzero vector of* L*. Mathematically we can written it as*

$$\lambda_1 = \inf \{\|v\| \in L \mid v \in L, v \neq 0\} \tag{15}$$

or

$$\lambda_1 = \inf |\|v - u\| \in L \mid v, u \in L, v \neq u\} \tag{16}$$

Definition 3.3. *(A.Nitaj, 2011) For* $i = 1, 2, \ldots, n$*, the* i*'th successive minimum of the lattice* L *of rank* n *is*

$$\lambda_i = \min \{\max \{\|v_1\|, \|v_2\|, \ldots, \|v_n\|\}\} \tag{17}$$

where $v_1, v_2, \ldots, v_n \in L$ are linearly independent.

Finding a shortest vector in dimension 2 is easy. However when the dimension $n \geq 3$, finding the shortest vector is not an easy task anymore. This can be seen clearly in (A.Nitaj, 2011).In addition, in order to find the shortest vector, we need to make sure that the vector v must be a nonzero vector. Also we need to always remember that the shortest vector v is not unique since $\|(-v)\|$=$\|(v)\|$ for all lattice vector $v \in L$. The following are some computational problem that is believed to be hard.(J.V.D, 2011)

Definition 3.4. *(Laarhoven et al., 2012) SVP: Given a basis of L, find $y \in L$ such that $\|y\|$=$\lambda_1(L)$*

This is the main computational problem involving lattice. Since it is well known that the zero vector is trivially the shortest vector in the lattice. Thus the objective of this problem is, we want to output the shortest nonzero vector in the lattice. Usually this problem is define under Euclidean norm ℓ_2 while for norm ℓ_∞, the SVP is known to be NP-hard and has been proved by Van Emde Boas in 1981. However, norm ℓ_p for $p < \infty$ is not proven until Ajtai showed in 1998 for ℓ_2 norm is NP-hard under randomized reduction.

Since the lattice based cryptography is mainly based on the SVP. Therefore, the choice of a basis for the lattice is very crucialto solve the SVP. Note that, the lattice will have infinitely many bases when $n \geq 2$ since each unimodular matrix U give rise to a new basis of the same lattice where the new basis produce by unimodular matrix U are equivalent but still they are not equal. Thus, we can conclude that there are so many bases that can be used to form a lattice. Hence, all the bases chosen can be divided into two which is good and bad basis.

Informally, we can simply define good basis as the basis that consists of short vectors that are somehow orthogonal to each other the basis will form a square-like parallelepiped, while the bad basis is the basis that consists of long vectors that generally point in the same or opposite direction. The idea of dividing that basis into two parts is to make sure that we can only have the good basis so that the SVP can be easier to solve. The following concept will be used to define the orthogonality of a basis precisely.

Definition 3.5. *(Galbraith, 2012) Let $b_1, b_2, \ldots, b_n$ be an ordered basis in R^m. The orthogonality defect of the basis is*

$$\frac{\prod_{i=1}^{n} \|b_i\|}{\det(L)} \tag{18}$$

In practices we will always start with the fixed norm which usually is Euclidean norm. While the given basis respect to the given norm is often quite bad. Therefore, to solve this problem, we can start with the lattice basis reduction. The idea of lattice basis reduction is to allow us to find another basis that can be as orthogonal as possible so that we can have the good lattice basis. Therefore, the following lemma is sufficient to be stated here. The proof of this lemma can be found in (Galbraith, 2012)

Lemma 3.1. *Let $b_1, b_2, \ldots, b_n$ be an ordered basis for lattice L in R^m and let $b_1^*, b_2^*, \ldots, b_n^*$ be the Gram Schmidt orthogonalisation, then*

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\| \tag{19}$$

One of the classical methods to do the basis reduction is known as Gram-Schmidt Orthogonalisation (GSO). Given the basis $(b_1, b_2, \ldots, b_n)$, the GSO process produces a set of orthogonal vectors $(b_1^*, b_2^*, \ldots, b_n^*)$ such that

$$span(b_1, b_2, \ldots, b_n) = span(b_1^*, b_2^*, \ldots, b_n^*) \tag{20}$$

The Gram-Schmidt Orthogonalisation can be done iteratively as below:

1. Set b_1^*=b_1.
2. For each $k \geq 2$, set $b_k^* := b_k - proj_{Lk}(b_k)$

where $L_n = span(b_1, b_2, \ldots, b_n) = span(b_1^*, b_2^*, \ldots, b_n^*)$ and $proj_L(v)$ is the projection of a vector v onto a subspace L.

Once we obtain the orthogonal vectors $(b_1^*, b_2^*, \ldots, b_n^*)$, we can express each of the original vectors b_k in terms of b_k=$\sum_{j=1}^{k-1} \mu_j b_j^* + b_k^*$ where μ_j are some real numbers. Thus, we can have the following matrix

$$B^* = UB \tag{21}$$

Where B has $(b_1, b_2, \ldots, b_n)$ as the columns, B^* has $(b_1^*, b_2^*, \ldots, b_n^*)$ as the columns and U is $n \times n$ matrix with $\det(U) = 1$. Since we know that $\det(U) = 1$, thus we have $\det(B)$=$\det(B^*)$=$\det(L)$. Note that,

$$\|b_k\|^2 = \sum_{j=1}^{k-1} \mu_j \|b_j^*\|^2 + \|b_k^*\|^2 \tag{22}$$

since all b_j^*'s are orthogonal. Therefore, $\|b_k\|^2 \geq \|b_k^*\|$ and hence we have $\|b_k\| \geq \|b_k^*\|$ for all $k = 1, 2, \ldots, n$. Since

$$\|b_k\| \geq \|b_k^*\| \tag{23}$$

and

$$\det(B) = \det(B^*) = \det(L) \tag{24}$$

hence from the lemma 3.1 we have

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\| \leq \prod_{i=1}^{n} \|b_i\| \tag{25}$$

Thus, from here we can clearly see that the orthogonality defect of B is at least 1. Therefore, if we consider the basis given to us is orthogonal, then $\|b_k\|$=$\|b_k^*\|$ and hence

$$\det(L) = \prod_{i=1}^{n} \|b_i^*\| = \prod_{i=1}^{n} \|b_i\| \tag{26}$$

It is clear that

$$\frac{\prod_{i=1}^{n} \|b_i\|}{\det(L)} = 1 \tag{27}$$

As a conclusion, we can say that the given basis is good if $\frac{\prod_{i=1}^{n} \|b_i\|}{\det(L)}$ not much larger than 1.

However, in practice, it is not a necessity to have the exact short vector. Thus, this give rise to the discussion on the approximate SVP (SVPγ)(J.V.D, 2011). The following are several definitions related to SVPγ

Definition 3.6. *(Laarhoven et al., 2012) SVPγ: Given a basis of L and an approximation factor $\gamma \geq 1$, find $y \in L$ such that $0 < \|y\| \leq \gamma\lambda_1(L)$.*

SVPγ is known to be NP-hard under quasi polynomial time reduction where for $\gamma = 2^{\log(n)^{\frac{1}{2}\epsilon}}$ where n is the dimension of the lattice and $\epsilon > 0$ is an arbitrarily small constant. This result can be found in (Khot, 2005). However, in practice by knowing reduced basis will not be sufficient to find the $\lambda_1(L)$. In fact, finding the $\lambda_1(L)$ is hard as finding the actual shortest vector. Therefore, it is much easier to replace the $\lambda_1(L)$ with the $vol(L)^{\frac{1}{d}}$ where d is the rank of lattice since the $vol(L)$ is actually the $\det(L)$ and can be found by using the basis of L. Thus, this gives rise to the Hermite Variant of Approximate SVP (HSVPγ).

Definition 3.7. *(Laarhoven et al., 2012) HSVPγ: Given a basis of L and an approximation factor $\gamma > 0$, find $y \in L$ such that $0 < \|y\| \leq \gamma vol(d)^{\frac{1}{d}}$*

The Lenstra, Lenstra Lovasz (LLL) algorithm has been used to solve HSVPγ in polynomial time for $\gamma = \left(\sqrt{\frac{4}{3} + \epsilon}\right)^{\frac{d-1}{2}}$. In practice, γ=1.02^d, while by using a better algorithm such as Block Korkine Zolatorev (BKZ) algorithm we could have γ=1.01^d. The proofs can be found in(Laarhoven et al., 2012) in section 4.2 and 4.4. The following definition is about the decisional approximation SVP, GapSVPγ and approximate shortest independent vector problem, SIVPγ will be sufficient to state here in order to understand LWE problems.

Definition 3.8. *(Laarhoven et al., 2012) GapSVPγ: Given a basis of L,a radius $r > 0$ and an approximation of factor $\gamma > 1$, return YES if $\lambda_1(L) \leq r$, return NO if $\lambda_1(L) \geq \gamma r$ and return YES or NO otherwise.*

Definition 3.9. *(Peikert et al., 2016) SIVPγ: Given a basis of L, output a set $S = \{s_i\} \subset L$ of n linearly independent lattice vector where $\|s_i\| \leq \gamma(n)\lambda_n(L)$ for all i.*

4 THE LEARNING WITH ERROR (LWE) PROBLEM

The LWE has been used widely in a cryptographic construction and was introduced by Regev in 2005. LWE mainly use the worst case lattice problem and hence make all the cryptographic construction based on it secure since it is well known that the worst case lattice problem is very hard. LWE is parameterized with the positive integer n and q, and an error distribution χ over Z. χ is usually taken to be a discrete Gaussian of width αq for some $\alpha < 1$, which is often called the relative error rate (Peikert et al., 2016). The following definition is about the LWE distribution.

Definition 4.1. *(Fitzpatrick, 2014) Let n and q be positive integers, χ be a probability distribution on Z_q and s be a secret vector following the uniform distribution on Z_q^n. We denote by $L_{s,\chi}^{(n)}$ the probability distribution on $Z_q^n \times Z_q$ obtained by choosing a from the uniform distribution on Z_q^n, choosing $e \in Z$ according to χ, and returning (a, b)=$(a, \langle a, s\rangle + e) \in Z_q^n \times Z_q$*

LWE problem can be divided into two main problems. The first one is known as search while the other one is called decision. Search-LWE is the problem where we need to find the secret s with the given LWE samples. While decision-LWE is the problem in which we need to distinguish between LWE samples and uniformly random one. In addition, this problem has been parameterized by the number m available sample. Formally we defined these two problems as follow

Definition 4.2. *(Peikert et al., 2016)*

1. *Search-LWE*
   Given m independent samples $(a_i, b_i) \in Z_q^n \times Z_q$ drawn from $L_{s,\chi}^{(n)}$ for a uniformly random $s \in Z_q^n$ (fixed for all sample), find s

2. *Decision-LWE*
   Given m independent samples $(a_i, b_i) \in Z_q^n \times Z_q$ where every sample is distributed according to either $L_{s,\chi}^{(n)}$ for a uniformly random $s \in Z_q^n$(fixed for all sample) or the uniform distribution over $Z_q^n \times Z_q$, distinguish which is the case (with non-negligible advantage).

LWE is believed to be hard because of three main reasons. First, the best known algorithm of LWE problem is run in exponential time. Second, LWE is actually the generalisation of learning parities with noise (LPN) over the finite field Z_q and it is known to be NP-hard which make the LWE problem more attractive. The last reason the LWE problem is known to be hard because based on the assumption that GapSVPγ and SIVPγ being a hard problem (Regev, 2010). Here we also state the worst case hardness problem of LWE with the following theorem.

Theorem 4.1. *(Peikert et al., 2016) For any $m = poly(n)$, any modulus $q \leq 2^{poly(n)}$, and any (discretized) Gaussian error distribution χ of parameter $\alpha q \geq 2\sqrt{n}$ where $0 < \alpha < 1$, solving the decision-LWE problem is at least as hard as quantumly solving GapSVPγ and SIVPγ on arbitrary n- dimensional lattices, for some $\gamma = O\left(\frac{n}{\alpha}\right)$.*

The proof of this theorem is provided in(Regev, 2009) and can be divided into two main parts, where the first part is the search-LWE which is as hard as worst case lattice problem via a quantum reduction. While the second part is the decision-LWE and shown to be equivalent as search-LWE, via an elementary classical reduction where this equivalence is applicable on polynomially bounded prime moduli $q = poly(n)$.

5 CONCLUSION

In this review, we provide preparatory and necessary foundations for lattice based cryptography. We have gathered from basic definition of lattices up to methods and techniques used in lattice based cryptography. Most importantly, creating a better basis from the bad ones requires basic knowledge from linear algebra and vector analysis concepts. The study of lattice based cryptography is now considered to be a promising area of interest as lattices hard problem is known to be resistance to quantum computing. While preparing for this article, the authors are now attempting to look at the possibility of discrepancy estimates between the bad and the good basis and hoping to get new properties related to this idea. As part of our on-going research, we will also do a diagnostic study on the concept of Learning With Errors (LWE), where up to this instant, the LWE-based cryptography is known to have strong security against the quantum computer. We also attempt to provide elegant mathematical framework for lattice based cryptography, where these could further extend the existing building blocks necessary for strong cryptographic protocols.

6 ACKNOWLEDGMENT

The authors would like to express their gratitude to The Ministry of Higher Education and Universiti Sains Malaysia for the Research University Grant Scheme (RUI), Universiti Sains Malaysia, 2016.

REFERENCES

A.Nitaj (2011). Lattice Based Cryptosystems. Revised to 1994.

Chi, D. P., Choi, J. W., San Kim, J., and Kim, T. (2015). Lattice Based Cryptography for Beginners.

Fitzpatrick, R. (2014). *Some Algorithms for Learning with Errors*. PhD thesis, , Royal Holloway University of London, London.

Galbraith, S. D. (2012). *Mathematics of Public Key Cryptography*. Cambridge University Press, New York, NY, USA, 1st edition.

J.V.D, P. (2011). Lattice-based cryptography. Master's thesis, Eindhoven University of Technology, Eindhoven.

Khot, S. (2005). Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM (JACM)*, 52(5):789–808.

Laarhoven, T., van de Pol, J., and de Weger, B. (2012). Solving hard lattice problems and the security of lattice-based cryptosystems. *IACR Cryptology ePrint Archive*, 2012:533.

Peikert, C. et al. (2016). *Decade of Lattice Cryptography*. World Scientific.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34.

Regev, O. (2010). The learning with errors problem. *Invited survey in CCC*.