Journal of Information Security, 2023, 14, 25-38
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Learning with Errors Public Key Cryptosystem with Its Security

Zhiyong Zheng, Kun Tian, Yi Zhang, Yunfan Lu

Engineering Research Center of Ministry of Education for Financial Computing and Digital Engineering, Renmin University of China, Beijing, China
Email: tkun19891208@ruc.edu.cn, ethanzhang@ruc.edu.cn, luyunfan@ruc.edu.cn

How to cite this paper: Zheng, Z.Y., Tian, K., Zhang, Y. and Lu, Y.F. (2023) Learning with Errors Public Key Cryptosystem with Its Security. *Journal of Information Security*, **14**, 25-38.
https://doi.org/10.4236/jis.2023.141003

Received: December 13, 2022
Accepted: January 15, 2023
Published: January 18, 2023

Abstract

The main purpose of this paper is to introduce the LWE public key cryptosystem with its security. In the first section, we introduce the LWE public key cryptosystem by Regev with its applications and some previous research results. Then we prove the security of LWE public key cryptosystem by Regev in detail. For not only independent identical Gaussian disturbances but also any general independent identical disturbances, we give a more accurate estimation probability of decryption error of general LWE cryptosystem. This guarantees high security and widespread applications of the LWE public key cryptosystem.

Keywords

Learning With Errors Problem, Cryptosystem, Decryption Error, Probability, Security

1. Introduction

In 2005, O. Regev proposed the first LWE public key cryptosystem in Tel Aviv University in Israel based on LWE distribution $A_{s,\chi}$. Because of this paper, Regev won the highest award for theoretical computer science in 2018—the Godel Award. The size of public key is $\tilde{O}(n^2)$ bits, and the size of private key s and ciphertext is $\tilde{O}(n)$ bits. The plaintext encrypted each time is 1 bit. In fact, the LWE public key cryptosystem is a probabilistic cryptosystem, which depends on a high probability algorithm. Since the security of LWE problem has been clearly proved, the LWE cryptosystem has received extensive attention as soon as it was proposed, and it becomes the most cutting-edge research topic in the lattice-based cryptosystem study.

Let p be a prime number, m, n be two positive integers. Given a list of equa-

tions with error as follows:

$$\begin{cases} \langle s, a_1 \rangle \approx_{\chi} v_1 \pmod{p}, \\ \langle s, a_2 \rangle \approx_{\chi} v_2 \pmod{p}, \\ \vdots \\ \langle s, a_m \rangle \approx_{\chi} v_m \pmod{p}, \end{cases}$$

where $v_i \in \mathbb{Z}_p$, $s \in \mathbb{Z}_p^n$, $a_i \in \mathbb{Z}_p^n$ are selected independently and uniformly, and $\langle s, a_i \rangle$ means the inner product of the vectors s and a_i. The errors $e_i \in \mathbb{Z}_p$ in the above equations come from a probability distribution $\chi : \mathbb{Z}_p \to \mathbb{R}^+$, *i.e.* for any $1 \le i \le m$, we have $v_i = \langle s, a_i \rangle + e_i$ and $e_i \in \mathbb{Z}_p$ is generated independently according to the probability distribution χ. The problem of finding $s \in \mathbb{Z}_p^n$ is denoted as $\mathrm{LWE}_{p,\chi}$ [1] [2]. The LWE public key cryptosystem of Regev introduced in the next section is proposed based on this problem.

The LWE problem could be regarded as an extension of a well known problem in learning theory which is believed hard to solve. Many researchers worked on the LWE problem and proved that the complexity of the best known algorithm is running in exponential time of n [3] [4] [5] [6]. An important theorem that gives the difficulty of solving the LWE problem is at least as hard as that of hard problems on lattice, such as the determination of the shortest vector problem (GapSVP) and the continuous shortest vector problem (SIVP) [3], which is proved by a quantum polynomial probabilistic reduction algorithm. Since the academic community believes that the hard problems on lattice such as the SVP, SIVP and GapSVP problems can resist quantum computing effectively, that is, there are no known quantum algorithms to solve the hard problems on lattice, so that the security of the LWE public key cryptosystem is guaranteed. We will give a detailed proof for the security of the LWE cryptosystem proposed by Regev in 2005 in section 3. However, this cryptosystem could only encrypt a single bit of plaintext and the efficiency is low. In order to encrypt multiple bits of plaintext and improve the efficiency signally, Regev presented a general LWE cryptosystem in 2009. We gave a more precise estimation probability of decryption error based on independent identical Gaussian disturbances and any general independent identical disturbances in [7], which shows that the general LWE public key cryptosystem could have high security.

An application of the LWE cryptosystem is the fully homomorphic encryption (FHE) [8]. The earliest FHE cryptosystem was based on average-case assumptions about ideal lattices [9] [10]. Later, Brakerski and Vaikuntanathan constructed the second FHE cryptosystem, which was based on the LWE problem [11] [12]. In 2013, the third fully homomorphic encryption algorithm based on the LWE problem was proposed by Gentry, Sahai, and Waters, which is proved that has some unique and advantageous properties [13]. It also remains some improvable techniques which need to be studied in depth [14]. The main purpose of this paper is to introduce the LWE public key cryptosystem with the proof of its security mathematically, which guarantees the widespread applications of it.

2. LWE Cryptosystem of Regev

Let $n \geq 1$, $q \geq 2$ be positive integers, χ be a given probability distribution in $\mathbb{Z}_q$. The LWE distribution $A_{s,\chi}$ is

$$\begin{cases} A_{s,\chi} = (a,b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q, \\ b \equiv_{\chi} \langle a,s \rangle + e \pmod{q}, \end{cases} \tag{1.1}$$

where $a \in \mathbb{Z}_q^n$ is uniformly distributed, $s \in \mathbb{Z}_q^n$ is the private key chosen at random, $e \in \mathbb{Z}_q$, $e \leftarrow \chi$ is called error distribution. LWE cryptosystem depends on LWE distribution $A_{s,\chi}$, and its workflow has the following three steps:

1) Public key

First we choose $s \in \mathbb{Z}_q^n$ at random as the private key, let $m = O(n \log q)$. Then we choose m samples distributed from $A_{s,\chi}$, $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, $e_i \in \mathbb{Z}_q$, $e_i \leftarrow \chi$, $1 \leq i \leq m$. Let

$$\overline{A} = [a_1, a_2, \cdots, a_m]_{n \times m} \in \mathbb{Z}_q^{n \times m},$$

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}, \quad e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}, \quad e \leftarrow \chi^m,$$

where $\overline{A}$ is a matrix uniformly at random, $e \leftarrow \chi^m$ indicates the m samples are independent. The public key of LWE cryptosystem is the following $(n+1) \times m$ matrix

$$A = \begin{pmatrix} \overline{A} \\ b' \end{pmatrix} \in \mathbb{Z}_q^{(n+1) \times m}. \tag{1.2}$$

If the uniformly random matrix $\overline{A}$ is given and saved for all the users of LWE cryptosystem, then the true public key is $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_q^m$ with size $O(m) = \tilde{O}(n)$. The public key and private key satisfy the following equation:

$$(-s', 1) A \equiv_{\chi} e' \pmod{q}. \tag{1.3}$$

2) Encryption.

In order to encrypt plaintext of 1 bit $u \in \mathbb{Z}_2$, let $x \in \{0,1\}^m$ be an uniformly distributed m dimensional vector with each entry 0 or 1. The ciphertext $c \in \mathbb{Z}_q^{n+1}$ is an $(n+1)$ dimensional vector in $\mathbb{Z}_q$, defined by

$$f_A(u) = c = Ax + \begin{pmatrix} 0 \\ u \cdot \left\lfloor \frac{q}{2} \right\rfloor \end{pmatrix} \in \mathbb{Z}_q^{n+1}, \tag{1.4}$$

where $0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}_q^n$, $u \left\lfloor \frac{q}{2} \right\rfloor \in \mathbb{Z}_q$, $\left\lfloor \frac{q}{2} \right\rfloor$ is the nearest integer to $\frac{q}{2}$. We call

f_A the encryption algorithm of LWE. In order to understand the encryption algorithm better, we give another definition of f_A.

The following set $\{1,2,\cdots,m\}$ has 2^m subsets. We choose a subset $S \subset \{1,2,\cdots,m\}$ uniformly at random which is called the index set. Then the encryption algorithm $f_A(u)$ for plaintext $u \in \mathbb{Z}_2$ is

$$c = f_A(u) = \begin{pmatrix} \sum_{i\in S} a_i \\ \sum_{i\in S} b_i + u\left\lfloor \frac{q}{2} \right\rfloor \end{pmatrix} \in \mathbb{Z}_q^{n+1}. \tag{1.5}$$

In fact, the subset S is corresponding to the uniformly chosen vector $x \in \{0,1\}^m$. The above formula (1.5) was proposed by Regev originally.

3) Decryption

We use the private key $s \in \mathbb{Z}_q^n$ for decryption of the ciphertext *c*. Actually, we only need to decrypt for the last entry of vector *c*. We have

$$f_A^{-1}(c) = (-s',1)c = (-s',1)Ax + u\left\lfloor \frac{q}{2} \right\rfloor \equiv_\chi e'x + u\left\lfloor \frac{q}{2} \right\rfloor (\mathrm{mod}\, q). \tag{1.6}$$

The error samples are much smaller than *q*, namely

$$\sum_{i\in S} e_i = e'x < \left\lfloor \frac{q}{2} \right\rfloor \Big/ 2. \tag{1.7}$$

Therefore, by comparing the distances between the right side of (1.6) and 0 or $\left\lfloor \frac{q}{2} \right\rfloor$, one can decrypt successfully:

$$f_A^{-1}(c) = \begin{cases} 0, \text{ if } (-s',1)c \text{ is closer to } 0, \\ 1, \text{ if } (-s',1)c \text{ is closer to } \left\lfloor \frac{q}{2} \right\rfloor, \end{cases} \tag{1.8}$$

finally we have $f_A^{-1}(c) = u$ and finish the whole workflow of LWE cryptosystem.

Both of the encryption algorithm and decryption algorithm of LWE are probabilistic algorithms, so we should verify the correctness, namely

$$\Pr\left\{ f_A^{-1}(c) = u \right\} \geq 1 - \delta(n). \tag{1.9}$$

Here $\delta(n)$ is a negligible function of *n*, *i.e.* $\delta(n) = o\left(\frac{1}{\log^\varepsilon n}\right)$, $\forall \varepsilon > 0$, more precisely:

$$\lim_{n\to\infty} \delta(n)\log^\varepsilon n = 0, \ \forall \varepsilon > 0.$$

We prove (1.9) with given discrete Gauss distribution $\chi = \bar{\psi}_\alpha$. For $a \in \mathbb{Z}_q$, $\mathbb{Z}_q = \{0,1,\cdots,q-1\}$,

$$|a| = \begin{cases} a, \text{ if } 0 < a \leq \left\lfloor \frac{q}{2} \right\rfloor, \\ q-a, \text{ if } \left\lfloor \frac{q}{2} \right\rfloor < a \leq q-1. \end{cases} \tag{1.10}$$

For $x \in T = [0,1)$, we define

$$|x| = \begin{cases} x, \text{ if } 0 \le x < \frac{1}{2}, \\ 1-x, \text{ if } \frac{1}{2} \le x < 1. \end{cases} \tag{1.11}$$

Lemma 1.1: Let $\delta > 0$, $0 \le k \le m$, if the distribution χ^k satisfies

$$\Pr_{e \sim \chi^k}\left\{|e| < \left\lfloor \frac{q}{2} \right\rfloor / 2\right\} > 1-\delta, \tag{1.12}$$

then (1.9) holds, *i.e.*

$$\Pr\left\{ f_A^{-1}(c) = u \right\} > 1-\delta.$$

Proof: When we choose the error samples $e_i \in \mathbb{Z}_q$, $e_i \leftarrow \chi$, we can always guarantee $e_i = |e_i|$ without changing the probability distribution. By (1.7), suppose that $|S| = k$, the corresponding sample

$$e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix}, \ |e| = \sum_{i=1}^{k} |e_i| = \sum_{i=1}^{k} e_i.$$

As long as (1.7) holds, *i.e.*

$$|e| < \left\lfloor \frac{q}{2} \right\rfloor / 2 \Rightarrow f_A^{-1}(c) = u,$$

then

$$\Pr\left\{ f_A^{-1}(c) = u \right\} \ge \Pr\left\{|e| < \left\lfloor \frac{q}{2} \right\rfloor / 2\right\} > 1-\delta.$$

□

Next we prove (1.12) holds for discrete Gauss distribution $\bar{\psi}_\alpha$ in $\mathbb{Z}_q$. The following assumptions are made for the selection of parameters:

$$\begin{cases} n \ge 1, \ q \ge 2, \ n^2 \le q \le 2n^2, \\ m = (1+\varepsilon)(n+1)\log q, \ \varepsilon > 0 \text{ is any positive real number}, \\ \chi = \bar{\psi}_{\alpha(n)}, \ \alpha(n) = o\left(\frac{1}{\sqrt{n}\log n}\right), \end{cases} \tag{1.13}$$

where the symbol *o* indicates

$$\lim_{n \to 0} \alpha(n) \cdot \sqrt{n} \log n = 0.$$

For example, we can choose $\alpha(n) = \frac{1}{\sqrt{n}\log^2 n}$, or

$$\alpha(n) = \left(\sqrt{n}\log^{1+\varepsilon} n\right)^{-1}, \ \forall \varepsilon > 0.$$

Lemma 1.2: Under the condition for parameters of (1.13), for any $0 \le k \le m$, we have

$$\Pr_{e\sim\bar{\psi}_{\alpha(n)}^{k}}\left\{|e|<\left\lfloor\frac{q}{2}\right\rfloor\Big/2\right\}>1-\delta(n), \tag{1.14}$$

where $\delta(n)=o\left(\frac{1}{\log^{\varepsilon} n}\right)$, $\forall\varepsilon>0$, is a negligible function.

Proof: Based on (1.13), when $n\geq n_0$, it is easy to see that

$$0\leq k\leq m\leq 4(1+\varepsilon)(n+1)\log n<\frac{n^2}{32}\leq\frac{q}{32}.$$

The k samples $e=\begin{pmatrix}e_1\\ \vdots\\ e_k\end{pmatrix}$ distributed as $\bar{\psi}_{\alpha}^{k}$ could be obtained from the k samples $x_1,x_2,\cdots,x_k$ of distribution ψ_α, where

$$x_i\in\left[0,\frac{1}{2}\right),\ e_i=\lfloor qx_i\rfloor \bmod q,\ 1\leq i\leq k.$$

Here the set of representative elements of $\mathbb{Z}_q$ is

$$\mathbb{Z}_q=\left\{a\in\mathbb{Z}\,|\,-\frac{q}{2}\leq a<\frac{q}{2}\right\}.$$

So we have

$$|e|=\sum_{i=1}^{k}|e_i|=\sum_{i=1}^{k}\lfloor qx_i\rfloor \bmod q.$$

Note that

$$\sum_{i=1}^{k}(\lfloor qx_i\rfloor-qx_i) \bmod q\leq k\leq\frac{q}{32},$$

therefore,

$$\sum_{i=1}^{k}qx_i \bmod q\leq\frac{q}{16}\Rightarrow\left(\sum_{i=1}^{k}x_i\right) \bmod 1\leq\frac{1}{16},$$

we have $|e|<\left\lfloor\frac{q}{2}\right\rfloor\Big/2$. Since $\sum_{i=1}^{k}x_i \bmod 1$ distributed as $\psi_{\sqrt{k}\alpha}$, where $\sqrt{k}\cdot\alpha=o\left(\frac{1}{\sqrt{\log n}}\right)$, so

$$\Pr\left\{\sum_{i=1}^{k}x_i \bmod 1<\frac{1}{16}\right\}=1-\delta(n),$$

where $\delta(n)=\sqrt{k}\cdot\alpha=o\left(\frac{1}{\sqrt{\log n}}\right)$. We complete the proof.

□

3. The Proof of Security

To prove the security of Regev's cryptosystem, we first prove some general properties for the probability distribution of Abel group by Impagliazzo and Zurkerman [15].

Let G be a finite Abel group, $k \geq 1$ be a positive integer. For any l elements $g_1, g_2, \cdots, g_l \in G$, suppose $x \in \{0,1\}^l$, $g = (g_1, g_2, \cdots, g_l)$, then

$$gx = \sum_{i=1}^{l} x_i g_i,\ x_i = 0 \text{ or } 1$$

is called a subsum of $\{g_1, g_2, \cdots, g_l\}$. Randomly choose $x \in \{0,1\}^l$, let gx denote the distribution of subsum, and let $U(G)$ denote the uniformly distribution on G.

Lemma 2.1: For any l elements $\{g_1, g_2, \cdots, g_l\}$ uniformly at random, the expectation of statistical distance between the distribution of subsum and the uniformly distribution on $U(G)$ is

$$E\left(\Delta\left(gx, U(G)\right)\right) \leq \left(|G|/2^l\right)^{\frac{1}{2}}.$$

Specially, the probability that the statistical distance is larger than $\left(|G|/2^l\right)^{\frac{1}{4}}$ is no more than $\left(|G|/2^l\right)^{\frac{1}{4}}$, *i.e.*

$$\Pr\left\{\Delta\left(gx, U(G)\right) \geq \left(|G|/2^l\right)^{\frac{1}{4}}\right\} \leq \left(|G|/2^l\right)^{\frac{1}{4}}.$$

Proof: Let $g = (g_1, g_2, \cdots, g_l)$ be l group elements chosen at random, $h \in G$ is a given group element. Define $P_g(h)$

$$P_g(h) = \frac{1}{2^l}\left|\left\{x \in \{0,1\}^l, gx = \sum_{i=1}^{l} x_i g_i = h\right\}\right|,$$

we call $P_g(h)$ the distribution of subsum for g. In order to prove $P_g(h)$ is close to uniformly distribution, we first prove the l_2 norm between $P_g(h)$ and the uniformly distribution is very small. In fact, we have:

$$\sum_{h \in G} P_g(h)^2 = \Pr_{x,x'}\{gx = gx'\} = \frac{1}{2^l} + \Pr_{x,x'}\{gx = gx', x \neq x'\}.$$

Note that for any $x \neq x'$,

$$\Pr_g\{gx = gx'\} = \frac{1}{|G|}.$$

So the expectation of l_2 norm for g satisfy

$$E_g\left[\sum_{h \in G} P_g(h)^2\right] \leq \frac{1}{2^l} + \frac{1}{|G|}.$$

Finally, we have the following estimation

$$\begin{aligned}
\underset{g}{E}\left[\sum_{h\in G}\left|P_g(h)-\frac{1}{|G|}\right|\right] &\le \underset{g}{E}\left[|G|^{\frac{1}{2}}\left(\sum_{h\in G}\left(P_g(h)-\frac{1}{|G|}\right)^2\right)^{\frac{1}{2}}\right] \\
&= |G|^{\frac{1}{2}}\underset{g}{E}\left[\left(\sum_{h\in G}P_g(h)^2-\frac{1}{|G|}\right)^{\frac{1}{2}}\right] \\
&= |G|^{\frac{1}{2}}\left[\underset{g}{E}\left(\sum_{h\in G}P_g(h)^2\right)-\frac{1}{|G|}\right]^{\frac{1}{2}} \\
&\le \left(|G|/2^l\right)^{\frac{1}{2}}.
\end{aligned}$$

We complete the proof.

□

The security of LWE public key cryptosystem by Regev is ascribed to the following theorem, which is the most important result in this section.

Theorem 1: For any $\varepsilon>0$, $m\ge(1+\varepsilon)(n+1)\log q$, if there is a probabilistic polynomial time algorithm W which distinguishes the plaintext $u=0$ or $u=1$ from the ciphertext c, then there exists a polynomial time algorithm solving the $\text{D-LWE}_{n,q,\chi,m}$ problem.

Proof: The public key of LWE cryptosystem is $A=\begin{pmatrix}\bar{A}\\ b'\end{pmatrix}$, where $\bar{A}\in\mathbb{Z}_q^{n\times m}$ is a matrix uniformly at random, $b=\begin{pmatrix}b_1\\ \vdots\\ b_m\end{pmatrix}\in\mathbb{Z}_q^m$ is an m dimensional vector chosen uniformly. The encryption function $f_A(u)$ is

$$c=f_A(u)=Ax+\begin{pmatrix}0\\ u\left\lfloor\frac{q}{2}\right\rfloor\end{pmatrix}\in\mathbb{Z}_q^{n+1},\ x\in\{0,1\}^m.$$

Since W is a probabilistic polynomial time algorithm, suppose $P_0(W)$ is the probability that decrypting $u=0$ from $f_A(0)$ by W, and $P_1(W)$ is the probability that decrypting $u=1$ from $f_A(1)$, *i.e.*

$$\begin{cases}P_0(W)=\Pr\{W(f_A(0))=0\}.\\ P_1(W)=\Pr\{W(f_A(1))=1\}.\end{cases}\tag{2.1}$$

If $b\in\mathbb{Z}_q^m$ is uniformly at random, then LWE distribution $A_{s,\chi}$ is uniformly LWE distribution. Let $P_u(W)$ be the probability of decryption successfully by W under the condition of uniformly distribution $A_{s,\chi}$. Suppose that

$$\left|P_0(W)-P_1(W)\right|\ge\frac{1}{n^\delta},\ \delta>0.\tag{2.2}$$

Under the assumption of (2.2), we will construct a new algorithm W' satisfying

$$\left|P_0(W')-P_u(W')\right| \geq \frac{1}{2n^{\delta}}. \tag{2.3}$$

By (2.2), we have

$$\left|P_0(W)-P_u(W)\right| \geq \frac{1}{2n^{\delta}}, \text{ or } \left|P_1(W)-P_u(W)\right| \geq \frac{1}{2n^{\delta}}.$$

If the first inequality of the above formula holds, let $W'=W$. If the second inequality of the above formula holds, then construct W' as follows. Let the function σ be $f_A(u) \to f_A(u)+\begin{pmatrix} 0 \\ \frac{q-1}{2} \end{pmatrix}$. Thus, σ maps the LWE distribution $(\bar{A},b)$ to $\left(\bar{A},b+\frac{q-1}{2}\right)$. If b is uniformly at random, so is $b+\frac{q-1}{2}$. We define W' to be the decryption on LWE distribution $\left(\bar{A},b+\frac{q-1}{2}\right)$ by W. According to (1.5),

$$P_0(W)=P_1(W'),\ P_1(W)=P_0(W'),$$

So W' is the algorithm which satisfies (2.3).

Let $s \in \mathbb{Z}_q^n$, the public key sample satisfies distribution of $(\bar{A},b) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m = A_{s,\chi}$. Let $P_0(s)$ be the probability of decryption $u=0$ successfully by W', *i.e.*

$$P_0(s)=\Pr\left\{W'\left(f_A(0)\right)=0\right\}.$$

Similarly, let $P_u(s)$ be the probability of decryption successfully by W' if $(\bar{A},b)$ is uniformly at random. Suppose

$$\left|E_s\left[P_0(s)\right]-E_s\left[P_u(s)\right]\right| \geq \frac{1}{2n^{\delta}}, \tag{2.4}$$

We define

$$Y=\left\{s \in \mathbb{Z}_q^n \mid \left|P_0(s)-P_u(s)\right| \geq \frac{1}{4n^{\delta}}\right\}. \tag{2.5}$$

It's easy to prove: if $s \in \mathbb{Z}_q^n$ is uniformly distributed, then we have

$$|Y|/q^n \geq \frac{1}{4n^{\delta}}.$$

Therefore, in order to prove theorem 1, we need to find an algorithm Z to determine whether the LWE distribution $A_{s,\chi}$ is uniformly at random for any $s \in Y$. The construction of algorithm Z: let R be a probability distribution on $\mathbb{Z}_q^n$ which is uniform LWE distribution or general LWE distribution when $s \in Y$, *i.e.*

$$R = \text{uniform LWE distribution, or } R=A_{s,\chi},\ s \in Y.$$

Let $\bar{A}=[a_1,\cdots,a_m] \in \mathbb{Z}_q^{n\times m}$, $b=\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_q^m$ be m random samples from dis-

tribution R. Let $P_0(R)$ be the probability of decryption $u=0$ successfully by W', where $(a,b)=A_{s,\chi}$, $s\in Y$. In the same way, suppose $P_u(R)$ is the probability of decryption $u=0$ successfully by W' if R is uniform LWE distribution. We estimate $P_0(R)$ and $P_u(R)$ by using the algorithm W' polynomial times so that the error could be controlled within $\frac{1}{64n^{\delta}}$. If $\left|P_0(R)-P_u(R)\right|\geq\frac{1}{16n^{\delta}}$, then the algorithm Z is effective, otherwise it is noneffective.

We first confirm: if R is uniform LWE distribution, then Z is noneffective with high probability. Because in this case, $(\bar{A},b)\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$, b is uniformly at random. According to lemma 2.1, the Abel group $G=\mathbb{Z}_q^n\times\mathbb{Z}_q$, we have

$$\left|P_0(R)-P_u(R)\right|\leq 2^{-\Omega(n)},$$

In this case, Z is noneffective.

If $R=A_{s,\chi}$, where $s\in Y$, we are to prove the algorithm Z is effective with probability $\frac{1}{\mathrm{Poly}(n)}$, *i.e.* one can distinguish $s\in Y$ from uniform distribution. Since $\left|P_0(R)-P_u(R)\right|\geq\frac{1}{4n^{\delta}}$, in the average sense we get

$$\Pr\left\{\left|P_0(R)-P_u(R)\right|\geq\frac{1}{8n^{\delta}}\right\}\geq\frac{1}{8n^{\delta}}.$$

Thus, the algorithm Z is effective for $A_{s,\chi}$, $s\in Y$ with positive probability. We complete the proof of theorem 1.

□

4. General LWE-Based Cryptosystem

We introduced the LWE cryptosystem proposed by Regev in section 2, and proved its security in section 3. However, it could only encrypt a single bit of plaintext and the efficiency is low. Based on the definition and properties of rounding function, Regev presented a general LWE cryptosystem in 2009, which could encrypt multiple bits of plaintext $v\in\mathbb{Z}_t^l$ with size $O(t^l)$ and improve the efficiency signally. In this section, we introduce general LWE cryptosystem first. Then we discuss the probability of decryption error for this cryptosystem and prove that it could be sufficiently small with suitable parameters. So we verify our core result that the LWE cryptosystem could have high security.

Definition 3.1: Let t,q,l be positive integers, we define function $F:\mathbb{Z}_t^l\to\mathbb{Z}_q^l$ as

$$F(a)=\left(\left\lfloor\frac{q}{t}a_1\right\rfloor,\left\lfloor\frac{q}{t}a_2\right\rfloor,\cdots,\left\lfloor\frac{q}{t}a_l\right\rfloor\right)\in\mathbb{Z}_q^l,\ \forall a=(a_1,a_2,\cdots,a_l)\in\mathbb{Z}_t^l,\quad(3.1)$$

and the "inverse function" $F^{-1}:\mathbb{Z}_q^l\to\mathbb{Z}_t^l$ as

$$F^{-1}(b)=\left(\left\lfloor\frac{t}{q}b_1\right\rfloor,\left\lfloor\frac{t}{q}b_2\right\rfloor,\cdots,\left\lfloor\frac{t}{q}b_l\right\rfloor\right)\in\mathbb{Z}_t^l,\ \forall b=(b_1,b_2,\cdots,b_l)\in\mathbb{Z}_q^l. \quad (3.2)$$

Let t,q,m,n,l,r be positive integers, $q>t$, function F and its "inverse function" are defined in 3.1. The workflow of general LWE cryptosystem is as follows:

1) Selection of private key S: $S\in\mathbb{Z}_q^{n\times l}$ is an $n\times l$ matrix uniformly at random in $\mathbb{Z}_q$.

In the LWE cryptosystem introduced in section 2, the private key is an n dimensional randomly chosen vector $s\in\mathbb{Z}_q^n$. To encrypt more general plaintext $v\in\mathbb{Z}_t^l$, we randomly select l private keys $s_1,s_2,\cdots,s_l\in\mathbb{Z}_q^n$ independently and form an $n\times l$ matrix $S=[s_1,s_2,\cdots,s_l]$. This is the private key S for general LWE cryptosystem.

2) Public key.

When the private key $S\in\mathbb{Z}_q^{n\times l}$ is fixed, in order to choose samples from LWE distribution, we first select m uniform n dimensional vectors $a_1,a_2,\cdots,a_m\in\mathbb{Z}_q^n$ in $\mathbb{Z}_q^n$ and form a uniform random matrix

$$A=[a_1,a_2,\cdots,a_m]_{n\times m}\in\mathbb{Z}_q^{n\times m}.$$

Then we generate $m\times l$ noise matrix samples $E=(E_{ij})_{m\times l}$ from distribution $\bar{\psi}_\alpha$, *i.e.* $E_{ij}\in\mathbb{Z}_q$, $E_{ij}\leftarrow\bar{\psi}_\alpha$, $1\le i\le m$, $1\le j\le l$, and the $m\times l$ samples are mutually independent. Finally we get an $m\times l$ matrix P

$$P=A^{\mathrm{T}}S+E=\begin{pmatrix}\langle a_1,s_1\rangle+E_{11} & \cdots & \langle a_1,s_l\rangle+E_{1l}\\ \vdots & \ddots & \vdots\\ \langle a_m,s_1\rangle+E_{m1} & \cdots & \langle a_m,s_l\rangle+E_{ml}\end{pmatrix}_{m\times l}.$$

The public key of LWE cryptosystem is (A,P), which is similar to that in section 2. Here we only change the public key from $b\in\mathbb{Z}_q^m$ to $m\times l$ matrix $P\in\mathbb{Z}_q^{m\times l}$. If the uniformly random matrix A is given and saved for all the users of LWE cryptosystem, then the true public key is the matrix P, and the public key and private key satisfy the following equation

$$P-A^{\mathrm{T}}S\equiv_{\bar{\psi}_\alpha}E\pmod q.$$

3) Encryption.

To encrypt multiple bits of plaintext $v\in\mathbb{Z}_t^l$, let $a\in\{-r,-r+1,\cdots,r\}^m$ be an m dimensional vector with each entry selected uniformly in $\{-r,-r+1,\cdots,r\}$, *i.e.* a is uniformly distributed. Ciphertext $\begin{pmatrix}u\\ c\end{pmatrix}$ is an $n+l$ dimensional vector, defined by

$$g_{A,P}(v)=\begin{pmatrix}u\\ c\end{pmatrix},\ u=Aa,\ c=P^{\mathrm{T}}a+F(v),$$

where F is defined in (3.1), and $g_{A,P}$ is called the encryption algorithm of LWE cryptosystem.

4) Decryption.

Given ciphertext (u,c) and the private key S, we compute $F^{-1}(c-S^{\mathrm{T}}u)$ as

the result of decryption. We have

$$\begin{aligned} F^{-1}\left(c-S^{\mathrm{T}}u\right) &= F^{-1}\left(P^{\mathrm{T}}a+F\left(v\right)-S^{\mathrm{T}}u\right) \\ &= F^{-1}\left(\left(A^{\mathrm{T}}S+E\right)^{\mathrm{T}}a+F\left(v\right)-S^{\mathrm{T}}Aa\right) \\ &= F^{-1}\left(E^{\mathrm{T}}a+F\left(v\right)\right). \end{aligned}$$

We need to calculate the probability of decryption error for this cryptosystem, namely, the probability of $F^{-1}\left(E^{\mathrm{T}}a+F\left(v\right)\right)\neq v$. The following theorem 2 gives a more precise upper bound estimation than [2] for this probability, which is proved in [7].

Theorem 2: Suppose $q>t$, we have the following inequality of the probability of decryption error

$$\Pr\left\{F^{-1}\left(E^{\mathrm{T}}a+F\left(v\right)\right)\neq v\right\}\leq 2l\left(1-\Phi\left(\frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr\left(r+1\right)}}\right)\right). \tag{3.3}$$

Here Φ is the cumulative distribution function of the standard normal distribution, *i.e.* $\Phi\left(x\right)=\int_{-\infty}^{x}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t$.

The upper bound could be as closed as 0 if we choose α small enough. It means that the probability of decryption error for the LWE cryptosystem could be made very small with an appropriate setting of parameters.

We could also estimate the probability of decryption error for the LWE cryptosystem when the noise matrix $E=\left(E_{ij}\right)_{m\times l}$ is chosen independently from a general common variable, rather than Gauss distribution. By central limit theorem [16], general disturbances could be approximated as Gaussian disturbances. We have the following theorem 3 which is proved in [7].

Theorem 3: $q>t$, $E=\left(E_{ij}\right)_{m\times l}$, each element E_{ij} is selected independently from a common random variable of mean 0 and standard deviation β. For any $\delta>0$, we can find positive integer m, such that the following inequality of the probability of decryption error holds,

$$\Pr\left\{F^{-1}\left(E^{\mathrm{T}}a+F\left(v\right)\right)\neq v\right\}\leq 2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+l\delta. \tag{3.4}$$

Here Φ is the cumulative distribution function of the standard normal distribution, *i.e.* $\Phi\left(x\right)=\int_{-\infty}^{x}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t$.

This probability could also be closed to 0 if we choose the parameter $\beta\sqrt{m}$ and δ small enough. Therefore the probability of decryption error of the LWE cryptosystem for general disturbance could be made very small, which leads to high security.

5. Conclusion

In this work, we introduce the LWE cryptosystem of Regev, and give a detailed proof for the security of LWE public key cryptosystem by Regev. We also intro-

duce general LWE cryptosystem presented by Regev in order to encrypt multiple bits of plaintext and improve the efficiency signally. For not only independent identical Gaussian disturbances but also any general independent identical disturbances, we give a more accurate estimation probability of decryption error of general LWE cryptosystem. The upper bound probability could be closed to 0 if we choose applicable parameters, which means that the probability of decryption error for general LWE cryptosystem could be sufficiently small. So we verify that the LWE public key cryptosystem could have high security.

Acknowledgements

The authors would like to thank the editors and reviewers for their constructive comments, which help improve the study significantly.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Regev, O. (2005) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Proceedings of the* 37*th Annual ACM Symposium on Theory of Computing*, Baltimore, 22-24 May 2005, 84-93. https://doi.org/10.1145/1060590.1060603

[2] Micciancio, D. and Regev, O. (2009) Lattice-Based Cryptography. In: Bernstein, D.J., Buchmann, J. and Dahmen, E., Eds., *Post-Quantum Cryptography*, Springer, Berlin, 147-191. https://doi.org/10.1007/978-3-540-88702-7_5

[3] Regev, O. (2009) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, **56**, Article No. 34. https://doi.org/10.1145/1568318.1568324

[4] Ajtai, M., Kumar, R. and Sivakumar, D. (2001) A Sieve Algorithm for the Shortest Lattice Vector Problem. *Proceedings of the* 33*rd Annual ACM Symposium on Theory of Computing*, Heraklion, 6-8 July 2001, 601-610. https://doi.org/10.1145/380752.380857

[5] Blum, A., Kalai, A. and Wasserman, H. (2003) Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model. *Journal of the ACM*, **50**, 506-519. https://doi.org/10.1145/792538.792543

[6] Kumar, R. and Sivakumar, D. (2001) On Polynomial Approximation to the Shortest Lattice Vector Length. *Proceedings of the* 12*th Annual ACM-SIAM Symposium on Discrete Algorithms*, Washington DC, 7-9 January 2001, 126-127.

[7] Zheng, Z. and Tian, K. (2022) On the LWE Cryptosystem with More General Disturbance. *Journal of Information Security*, **13**, 127-139. https://doi.org/10.4236/jis.2022.133008

[8] Rivest, R., Adleman, L. and Dertouzos, M. (1978) On Data Banks and Privacy Homomorphism. In: DeMillo, R.A., Ed., *Foundations of Secure Computation*, Academic Press, New York, 169-180.

[9] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. *Proceedings of the* 41*st Annual ACM Symposium on Theory of Computing*, Bethesda, 31 May-2

June 2009, 169-178. https://doi.org/10.1145/1536414.1536440

[10] Dijk, M., Gentry, C., Halevi, S. and Vaikuntanathan, V. (2010) Fully Homomorphic Encryption over the Integers. *International Conference on Theory and Applications of Cryptographic Techniques*, French Riviera, 30 May-3 June 2010, 24-43. https://doi.org/10.1007/978-3-642-13190-5_2

[11] Brakerski, Z. and Vaikuntanathan, V. (2011) Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. *Annual Cryptology Conference*, Santa Barbara, 14-18 August 2011, 505-524. https://doi.org/10.1007/978-3-642-22792-9_29

[12] Brakerski, Z. and Vaikuntanathan, V. (2011) Efficient Fully Homomorphic Encryption from (Standard) LWE. *IEEE* 52*nd Annual Symposium on Foundations of Computer Science*, Palm Springs, 22-25 October 2011, 831-871. https://doi.org/10.1109/FOCS.2011.12

[13] Gentry, C., Sahai, A. and Waters, B. (2013) Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. *Annual Cryptology Conference*, Santa Barbara, 18-22 August 2013, 75-92. https://doi.org/10.1007/978-3-642-40041-4_5

[14] Islam, M., Islam, M., Islam, N. and Shabnam, B. (2018) A Modified and Secured RSA Public Key Cryptosystem Based on "n" Prime Numbers. *Journal of Computer and Communications*, **6**, 78-90. https://doi.org/10.4236/jcc.2018.63006

[15] Impagliazzo, R. and Zuckerman, D. (1989) How to Recycle Random Bits. *Proceedings of the* 30*th Annual IEEE Symposium on Foundations of Computer Science* (*FOCS*), Research Triangle Park, 30 October-1 November 1989, 248-253. https://doi.org/10.1109/SFCS.1989.63486

[16] Riauba, B. (1975) A Central Limit Theorem for Dependent Random Variables. *Lithuanian Mathematical Journal*, **15**, 185-200. https://doi.org/10.1007/BF00975432