Scientific Research Publishing

Journal of Information Security, 2022, 13, 127-139
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

On the LWE Cryptosystem with More General Disturbance

Zhiyong Zheng, Kun Tian[*]

Engineering Research Center of Ministry of Education for Financial Computing and Digital Engineering, Renmin University of China, Beijing, China

Email: *tkun19891208@ruc.edu.cn

How to cite this paper: Zheng, Z.Y. 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

Received: April 27, 2022
Accepted: July 8, 2022
Published: July 11, 2022

Abstract

The main purpose of this paper is to give an extension on learning with errors problem (LWE) based cryptosystem about the probability of decryption error with more general disturbance. In the first section, we introduce the LWE cryptosystem with its application and some previous research results. Then we give a more precise estimation probability of decryption error based on independent identical Gaussian disturbances and any general independent identical disturbances. This upper bound probability could be closed to 0 if we choose applicable parameters. It means that the probability of decryption error for the cryptosystem could be sufficiently small. So we verify our core result that the LWE-based cryptosystem could have high security.

Keywords

Learning with Errors Problem, Decryption Error, Probability, General Disturbance

1. Introduction

In this section we describe a cryptosystem based on the learning with errors problem (LWE) [1] [2]. First we introduce the LWE problem. Let p be a prime number, m,n be positive integers and consider a list of equations with error as follows:

$$\begin{cases} \langle s,a_1\rangle \approx_\chi v_1 \,(\bmod p), \\ \langle s,a_2\rangle \approx_\chi v_2 \,(\bmod p), \\ \qquad\vdots \\ \langle s,a_m\rangle \approx_\chi v_m \,(\bmod p). \end{cases}$$

Here $s \in \mathbb{Z}_p^n$, $a_1, a_2, \cdots, a_m$ are chosen independently and uniformly from

$\mathbb{Z}_p^n$, and $v_1, v_2, \cdots, v_m \in \mathbb{Z}_p$. $\langle s, a_i \rangle$ is the inner product of two vectors s and a_i. The errors in these equations are generated from a probability distribution $\chi : \mathbb{Z}_p \to \mathbb{R}^+$ on $\mathbb{Z}_p$, *i.e.* for each equation, we have $v_i = \langle s, a_i \rangle + e_i$ and $e_i \in \mathbb{Z}_p$ is chosen independently based on the probability distribution χ. The problem of finding $s \in \mathbb{Z}_p^n$ from such equations is called $\mathrm{LWE}_{p,\chi}$. There is an equivalent description for the LWE problem. The input has a pair (A, v) where $A \in \mathbb{Z}_p^{m \times n}$ is chosen uniformly, and the choices of v have two cases. One case for v is chosen uniformly from $\mathbb{Z}_p^m$, the other case is $As + e$ for a uniformly chosen $s \in \mathbb{Z}_p^n$ and vector $e \in \mathbb{Z}_p^m$ chosen according to χ^m. The goal is to distinguish between these two cases with non-negligible probability. It is also equivalent with a decoding problem in *q*-ary lattices [1].

The short integer solution (SIS) problem was first introduced in the seminal work of Ajtai [3], and has served as the foundation for one-way and collision-resistant hash functions, identification schemes, digital signatures, and other "minicrypt" primitives. A very important work of Regev from 2005 introduced the LWE problem, which is the "encryption-enabling" analogue of the SIS problem [4]. In fact, the two problems are very similar, and can meaningfully be seen as duals of each other.

The LWE problem is a very robust problem and can be viewed as an extension of a well-known problem in learning theory. It remains hard even if the attacker learns extra information about the secret and errors. Regev gave the worst-case hardness theorem for LWE [4]. The complexity of the best known algorithm is running in exponential time in *n* [5] [6] [7]. This theorem is proved by giving a quantum polynomial-time reduction that uses an oracle for LWE to solve GapSVP_γ and SIVP_γ in the worst case, thereby transforming any algorithm that solves LWE into a quantum algorithm for lattice problems. The quantum nature of the reduction is meaningful since there are no known quantum algorithms for GapSVP_γ and SIVP_γ that significantly outperform classical ones, beyond generic quantum speedups. It would be very useful to have a completely classical reduction to give further confidence in the hardness of LWE, which was given in 2009 by Peikert [8]. Regev also gave a public-key cryptosystem whose semantic security can provably be based on the LWE problem, and hence on the conjectured quantum hardness of GapSVP_γ and SIVP_γ for $\gamma = O\left(n^{3/2}\right)$ [4]. LWE problem has close relationship with decoding problems in coding theory [9]-[18]. Regev's cryptosystem is secure against passive eavesdroppers since the LWE problem is hard.

Another application of LWE is fully homomorphic encryption (FHE) [19]. The earliest FHE constructions were based on average-case assumptions about ideal lattices [20] [21]. Later, Brakerski and Vaikuntanathan gave the second generation of FHE constructions, which were based on the LWE problem [22] [23]. In 2013, Gentry, Sahai, and Waters proposed an LWE-based FHE scheme that has some unique and advantageous properties, such as homomorphic multiplication does not require any key-switching step, and the scheme can be made identity-based. This yields unbounded FHE based on LWE with just an inverse-polynomial $n^{-O(1)}$ error rate [24].

Now we introduce the efficient lattice-based cryptosystem in the following which has strong theoretical security [2].

- Private key: $S \in \mathbb{Z}_q^{n\times l}$ is uniformly chosen at random.
- Public key: $A \in \mathbb{Z}_q^{m\times n}$ is uniformly chosen at random and $E \in \mathbb{Z}_q^{m\times l}$ is chosen from the distribution $\overline{\psi_\alpha}$. The public key is $(A, P = AS + E)$.
- Encryption: Given $v \in \mathbb{Z}_t^l$ from the message space and a public key (A, P), choose a vector $a \in \{-r, -r+1, \cdots, r\}^m$ uniformly at random, and compute the ciphertext $\left(u = A^{\mathrm{T}}a, c = P^{\mathrm{T}}a + f(v)\right)$.
- Decryption: Given a ciphertext (u, c) and a private key S, output $f^{-1}\left(c - S^{\mathrm{T}}u\right)$.

Here m, n, l, t, q, r are positive integers and $\alpha > 0$. $\overline{\psi_\alpha}$ is defined to be the distribution on $\mathbb{Z}_q$ obtained by sampling a normal variable with mean 0 and standard deviation $\alpha q/\sqrt{2\pi}$, rounding the result to the nearest integer and reduced modulo q. f is defined as the function from $\mathbb{Z}_t^l$ to $\mathbb{Z}_q^l$ by multiplying each coordinate by q/t and rounding to the nearest integer. f^{-1} is defined to be the 'inverse' mapping of f by multiplying each coordinate by t/q and rounding to the nearest integer. The definitions of f and f^{-1} are in the next section. The probability of decryption error in one letter for this cryptosystem is approximatively estimated in [2] as

$$\text{error probability per letter} \approx 2\left(1-\Phi\left(\frac{1}{2t\alpha}\sqrt{\frac{6\pi}{mr(r+1)}}\right)\right), \tag{1}$$

where Φ is the cumulative distribution function of the standard normal distribution, *i.e.* $\Phi(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{t^2}{2}} \mathrm{d}t$. We give a more precise upper bound estimation here

$$\text{error probability} \le 2l\left(1-\Phi\left(\frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr(r+1)}}\right)\right). \tag{2}$$

This upper bound probability could be closed to 0 if we choose α small enough. It means that the probability of decryption error for the cryptosystem could be sufficiently small. However, the above estimation is based on Gaussian disturbance. In our work, we also give the probability of decryption error for the LWE-based cryptosystem with more general disturbance. By central limit theorem [25], general disturbance could be approximated as Gaussian disturbance, then we get the following probability estimation result which is more advanced than that in [2].

$$\text{error probability} \le 2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr(r+1)}}\right)\right) + l\delta, \tag{3}$$

here β is the standard deviation of disturbance distribution, δ is positive real number.

Innovation and Contribution

Our work gives estimation probability of decryption error based on Gaussian disturbances and proves that the decryption error could be sufficiently small. The most salient innovation and contribution is that for any general disturbances, the decryption error could also be small enough. This indicates high security and reliability of LWE-based cryptosystem. In other words, this cryptosystem is secure enough against passive eavesdroppers and could be applied in many kinds of encryption process.

2. Methodology

2.1. Preliminary Property

Definition 1: $\forall x \in \mathbb{R}$, let $[x]$ be the closest integer to x, specially, $[x]$ is defined to be $x-\frac{1}{2}$ if the fractional part of x is $\frac{1}{2}$. It is trivial that $-\frac{1}{2} < x-[x] \le \frac{1}{2}$ for all $x \in \mathbb{R}$.

Lemma 1: t and q are positive integers, $t \le q$. $\forall a \in \mathbb{Z}_t$, let $f(a) = \left[\frac{q}{t}a\right] \in \mathbb{Z}_q$. $\forall b \in \mathbb{Z}_q$, let $f^{-1}(b) = \left[\frac{t}{q}b\right] \in \mathbb{Z}_t$. Then $f^{-1}(f(a)) = a$ for $\forall a \in \mathbb{Z}_t$ holds.

Remark: If $a_1 \equiv a_2 \pmod t$, we have $f(a_1) \equiv f(a_2) \pmod q$, so the definition of f is well defined and reasonable.

Proof of lemma 1: 1) If $t = q$, then we have $f(a) = [a] = a$ and

$$f^{-1}(f(a)) = f^{-1}(a) = [a] = a,\ \forall a \in \mathbb{Z}_t.$$

2) If $t < q$, then $\frac{q}{2t} > \frac{1}{2}$, we know

$$\frac{q}{t}a - \frac{1}{2} \le \left[\frac{q}{t}a\right] < \frac{q}{t}a + \frac{1}{2}.$$

It follows that

$$\frac{q}{t}a - \frac{q}{2t} < \frac{q}{t}a - \frac{1}{2} \le \left[\frac{q}{t}a\right] < \frac{q}{t}a + \frac{1}{2} < \frac{q}{t}a + \frac{q}{2t}.$$

So we can get

$$\frac{q}{t}a - \frac{q}{2t} < \left[\frac{q}{t}a\right] < \frac{q}{t}a + \frac{q}{2t}.$$

This is equivalent to

$$a - \frac{1}{2} < \frac{t}{q}\left[\frac{q}{t}a\right] < a + \frac{1}{2}.$$

and

$$-\frac{1}{2} < \frac{t}{q}\left[\frac{q}{t}a\right] - a < \frac{1}{2}.$$

Thus,

$$\left[\frac{t}{q}\left[\frac{q}{t}a\right]-a\right]=0,\ \text{and}\ \left[\frac{t}{q}\left[\frac{q}{t}a\right]\right]=a.$$

This means that

$$f^{-1}\left(f\left(a\right)\right)=a,\ \forall a\in\mathbb{Z}_t.$$

□

Lemma 2: t and q are positive integers, $t>q$. If a is uniformly chosen in $\mathbb{Z}_t$, then

$$P\left\{f^{-1}\left(f\left(a\right)\right)\neq a\right\}=1-\frac{q}{t}.$$

Proof: $t>q$, from lemma 1 we have

$$\left[\frac{q}{t}\left[\frac{t}{q}b\right]\right]=b,\ \forall b\in\mathbb{Z}_q.$$

This is equivalent to

$$f\left(\left[\frac{t}{q}b\right]\right)=b,\ \forall b\in\mathbb{Z}_q.$$

So we get

$$f^{-1}\left(f\left(\left[\frac{t}{q}b\right]\right)\right)=f^{-1}\left(b\right)=\left[\frac{t}{q}b\right],\ \forall b\in\mathbb{Z}_q.$$

Here $0,\left[\frac{t}{q}\right],\left[\frac{2t}{q}\right],\cdots,\left[\frac{(q-1)t}{q}\right]$ are different from each other in $\mathbb{Z}_t$. Next we prove that the number of a in $\mathbb{Z}_t$ satisfying $f^{-1}\left(f\left(a\right)\right)=a$ is no more than q. Let A be the set containing all the elements satisfying $f^{-1}\left(f\left(a\right)\right)=a$ in $\mathbb{Z}_t$. $\forall a_1,a_2\in A$, $a_1\neq a_2$ in $\mathbb{Z}_t$, then we have $f\left(a_1\right)\neq f\left(a_2\right)$ in $\mathbb{Z}_q$. This means the number of A is no more than q.

Above all, it shows that $0,\left[\frac{t}{q}\right],\left[\frac{2t}{q}\right],\cdots,\left[\frac{(q-1)t}{q}\right]$ are just all the numbers in $\mathbb{Z}_t$ such that $f^{-1}\left(f\left(a\right)\right)=a$. Based on a is uniformly chosen in $\mathbb{Z}_t$, then

$$P\left\{f^{-1}\left(f\left(a\right)\right)\neq a\right\}=1-\frac{q}{t}.$$

□

Corollary 1: t, q and l are positive integers.

$\forall a=\left(a_1,a_2,\cdots,a_l\right)\in\mathbb{Z}_t^l$, let $f\left(a\right)=\left(\left[\frac{q}{t}a_1\right],\left[\frac{q}{t}a_2\right],\cdots,\left[\frac{q}{t}a_l\right]\right)\in\mathbb{Z}_q^l$.

$\forall b=\left(b_1,b_2,\cdots,b_l\right)\in\mathbb{Z}_q^l$, let $f^{-1}\left(b\right)=\left(\left[\frac{t}{q}b_1\right],\left[\frac{t}{q}b_2\right],\cdots,\left[\frac{t}{q}b_l\right]\right)\in\mathbb{Z}_t^l$. If a is uniformly chosen in $\mathbb{Z}_t^l$ and $a_1,a_2,\cdots,a_l$ are independent, then

$$P\left\{f^{-1}\left(f\left(a\right)\right)\neq a\right\}=\max\left\{0,1-\left(\frac{q}{t}\right)^l\right\}.$$

Proof: If $t \le q$, from lemma 1, we have

$$f^{-1}\left(f\left(a_i\right)\right) = a_i,\ \forall a_i \in \mathbb{Z}_t,\ \forall 1 \le i \le l.$$

So

$$f^{-1}\left(f\left(a\right)\right) = a,\ \forall a \in \mathbb{Z}_t^l.$$

$$P\left\{f^{-1}\left(f\left(a\right)\right) \ne a\right\} = 0 = \max\left\{0, 1 - \left(\frac{q}{t}\right)^l\right\}.$$

If $t > q$, from lemma 2, we have

$$P\left\{f^{-1}\left(f\left(a_i\right)\right) = a_i\right\} = \frac{q}{t},\ a_i \in \mathbb{Z}_t,\ \forall 1 \le i \le l.$$

Since $a_1, a_2, \cdots, a_l$ are independent, therefore,

$$P\left\{f^{-1}\left(f\left(a\right)\right) = a\right\} = \left(\frac{q}{t}\right)^l,\ a \in \mathbb{Z}_t^l.$$

$$P\left\{f^{-1}\left(f\left(a\right)\right) \ne a\right\} = 1 - \left(\frac{q}{t}\right)^l = \max\left\{0, 1 - \left(\frac{q}{t}\right)^l\right\}.$$

□

2.2. Probability of Decryption Error Based on Gaussian Disturbance

Now we can calculate the probability of decryption error for the LWE-based cryptosystem. As described in the first section, assume S be the private key, $\left(A, P\right)$ be the public key, and we choose $v \in \mathbb{Z}_t^l$ from the message space, encrypt v and then decrypt it. The ciphertext is $\left(u = A^{\mathrm{T}} a, c = P^{\mathrm{T}} a + f\left(v\right)\right)$. The decryption result is

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

Here the decryption result $f^{-1}\left(E^{\mathrm{T}} a + f\left(v\right)\right) \in \mathbb{Z}_t^l$. The decryption error occurs if $f^{-1}\left(E^{\mathrm{T}} a + f\left(v\right)\right) \ne v$. Since all the parameters are taken to guarantee security and efficiency of the cryptosystem, here we set $q > t$ and obtain the following theorem.

Theorem 1: t, q, l, m, r are positive integers and $q > t$. $v \in \mathbb{Z}_t^l$, f is defined in the previous section, $E_{m \times l}$ is a Gaussian disturbance matrix with each element chosen independently from the Gaussian distribution with mean 0 and standard deviation $\alpha q / \sqrt{2\pi}$, $a \in \left\{-r, -r+1, \cdots, r\right\}^m$ is uniformly chosen at random. Then we have the following inequality of the probability of decryption error.

$$P\left\{f^{-1}\left(E^{\mathrm{T}} a + f\left(v\right)\right) \ne v\right\} \le 2l\left(1 - \Phi\left(\frac{q-t}{2\alpha t q}\sqrt{\frac{6\pi}{mr\left(r+1\right)}}\right)\right).$$

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

Proof: In order to compute the probability of decryption error, we consider one letter first, *i.e.* the probability of $f^{-1}\left(E_i^{\mathrm{T}}a+f(v_i)\right)\neq v_i$, here v_i is the *i*th coordinate of v, $E_{m\times l}=(E_1,E_2,\cdots,E_l)$ and $f^{-1}\left(E_i^{\mathrm{T}}a+f(v_i)\right)$ is the *i*th coordinate of $f^{-1}\left(E^{\mathrm{T}}a+f(v)\right)$. From lemma 1 we know that $f^{-1}\left(f(v_i)\right)=v_i$ for any $v_i\in\mathbb{Z}_t$ under this condition. We have

$$-\frac{1}{2}<\frac{q}{t}v_i-\left[\frac{q}{t}v_i\right]\leq\frac{1}{2}.$$

$$-\frac{t}{2q}\leq\frac{t}{q}\left[\frac{q}{t}v_i\right]-v_i<\frac{t}{2q}.$$

So if $\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|<\frac{1}{2}-\frac{t}{2q}$, we get

$$\left|\frac{t}{q}E_i^{\mathrm{T}}a+\frac{t}{q}\left[\frac{q}{t}v_i\right]-v_i\right|<\frac{1}{2}-\frac{t}{2q}+\frac{t}{2q}=\frac{1}{2}.$$

$$\left[\frac{t}{q}E_i^{\mathrm{T}}a+\frac{t}{q}\left[\frac{q}{t}v_i\right]-v_i\right]=0.$$

$$\left[\frac{t}{q}E_i^{\mathrm{T}}a+\frac{t}{q}\left[\frac{q}{t}v_i\right]\right]=v_i.$$

$$f^{-1}\left(E_i^{\mathrm{T}}a+f(v_i)\right)=v_i.$$

It means that if $\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|<\frac{1}{2}-\frac{t}{2q}$, we can get $f^{-1}\left(E_i^{\mathrm{T}}a+f(v_i)\right)=v_i$. Equivalently, if $f^{-1}\left(E_i^{\mathrm{T}}a+f(v_i)\right)\neq v_i$, *i.e.* the decryption error occurs in the *i*th letter, then $\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\geq\frac{1}{2}-\frac{t}{2q}$. So the probability of decryption error in one letter is no more than the probability of $\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\geq\frac{1}{2}-\frac{t}{2q}$, *i.e.*

$$P\left\{f^{-1}\left(E_i^{\mathrm{T}}a+f(v_i)\right)\neq v_i\right\}\leq P\left\{\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\geq\frac{1}{2}-\frac{t}{2q}\right\}.$$

The next step we estimate the probability of $\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\geq\frac{1}{2}-\frac{t}{2q}$. Since each coordinate of E_i is chosen independently from the Gaussian distribution with mean 0 and standard deviation $\alpha q/\sqrt{2\pi}$ and the sum of independent Gaussian variables is still a Gaussian variable, $E_i^{\mathrm{T}}a$ is also a Gaussian distribution variable. $a=(a_1,a_2,\cdots,a_m)$ and each a_i is chosen from $\{-r,-r+1,\cdots,r\}$ uniformly at random, then

$$E(a_i)=\frac{-r+(-r+1)+\cdots+r}{2r+1}=0.$$

$$Var(a_i)=\frac{(-r)^2+(-r+1)^2+\cdots+r^2}{2r+1}=\frac{r(r+1)}{3}.$$

$$E\left(E_i^{\mathrm{T}}a\right)=0.$$

$$Var\left(E_i^{\mathrm{T}}a\right)=\left(\frac{\alpha q}{\sqrt{2\pi}}\right)^2\cdot\frac{r(r+1)}{3}m=\frac{\alpha^2q^2mr(r+1)}{6\pi}.$$

Therefore $E_i^{\mathrm{T}}a$ is treated as a normal distribution with mean 0 and standard deviation $\alpha q\sqrt{mr(r+1)}/\sqrt{6\pi}$. We have

$$\begin{aligned}&P\left\{\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\ge\frac{1}{2}-\frac{t}{2q}\right\}=P\left\{\left|E_i^{\mathrm{T}}a\right|\ge\frac{q-t}{2t}\right\}\\&=P\left\{\left|E_i^{\mathrm{T}}a\right|\Big/\left(\alpha q\sqrt{mr(r+1)}\Big/\sqrt{6\pi}\right)\ge\frac{q-t}{2t}\Big/\left(\alpha q\sqrt{mr(r+1)}\Big/\sqrt{6\pi}\right)\right\}\\&=P\left\{\left|E_i^{\mathrm{T}}a\right|\Big/\left(\alpha q\sqrt{mr(r+1)}\Big/\sqrt{6\pi}\right)\ge\frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr(r+1)}}\right\}\\&=2\left(1-\Phi\left(\frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr(r+1)}}\right)\right).\end{aligned}$$

So we get the following inequality for probability of decryption error of the LWE-based cryptosystem

$$\begin{aligned}&P\left\{f^{-1}\left(E^{\mathrm{T}}a+f(v)\right)\ne v\right\}\\&\le lP\left\{f^{-1}\left(E_i^{\mathrm{T}}a+f(v_i)\right)\ne v_i\right\}\\&\le lP\left\{\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\ge\frac{1}{2}-\frac{t}{2q}\right\}\\&=2l\left(1-\Phi\left(\frac{q-t}{2\alpha tq}\sqrt{\frac{6\pi}{mr(r+1)}}\right)\right).\end{aligned}$$

□

This upper bound probability estimation is more precise than (1). 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-based cryptosystem could be made very small with an appropriate setting of parameters.

2.3. Probability of Decryption Error for General Disturbance

In this section we estimate the probability of decryption error for the LWE-based cryptosystem when the noise matrix $E=\left(E_{ij}\right)_{m\times l}$ is chosen independently from a general common variable.

Theorem 2: t,q,l,r are positive integers and $q>t$, m is a undetermined positive integer. $v\in\mathbb{Z}_t^l$, f is defined in the second section, $E_{m\times l}$ is a general disturbance matrix with each element chosen independently from a common random variable of mean 0 and standard deviation β, $a\in\{-r,-r+1,\cdots,r\}^m$ is uniformly chosen at random. For any $\delta>0$, we can find positive integer m, such that the following inequality of the probability of decryption error holds.

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

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

Proof: Similarly as the proof of theorem 1, we need to estimate the probability of $\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\geq\frac{1}{2}-\frac{t}{2q}$. Since the coordinates of E_i^{T} are independent identically distributed, E_i^{T} and a are also independent, by central limit theorem [25], $E_i^{\mathrm{T}}a$ is approximately normal distribution with mean 0 and standard deviation $d=\sqrt{mVar\left(E_{ij}\right)Var\left(a_i\right)}=\beta\sqrt{mr\left(r+1\right)/3}$. Thus, for any sufficiently small $\delta>0$, there is a positive integer m such that

$$\begin{aligned}&P\left\{\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\geq\frac{1}{2}-\frac{t}{2q}\right\}=P\left\{\left|E_i^{\mathrm{T}}a\right|\geq\frac{q-t}{2t}\right\}\\&=P\left\{\left|E_i^{\mathrm{T}}a\right|\Big/\left(\beta\sqrt{mr\left(r+1\right)/3}\right)\geq\frac{q-t}{2t}\Big/\left(\beta\sqrt{mr\left(r+1\right)/3}\right)\right\}\\&=P\left\{\left|E_i^{\mathrm{T}}a\right|\Big/\left(\beta\sqrt{mr\left(r+1\right)/3}\right)\geq\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right\}\\&=2\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+\varepsilon.\end{aligned}$$

Here $\left|\varepsilon\right|\leq\delta$. Then we get the following inequality for probability of decryption error of the LWE-based cryptosystem for general disturbance

$$\begin{aligned}&P\left\{f^{-1}\left(E^{\mathrm{T}}a+f\left(v\right)\right)\neq v\right\}\\&\leq lP\left\{f^{-1}\left(E_i^{\mathrm{T}}a+f\left(v_i\right)\right)\neq v_i\right\}\\&\leq lP\left\{\left|\frac{t}{q}E_i^{\mathrm{T}}a\right|\geq\frac{1}{2}-\frac{t}{2q}\right\}\\&=2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+l\varepsilon\\&\leq 2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+l\delta.\end{aligned}$$

□

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

Example 1: Let $t=2$, $q=5$, $l=1$, $m=1$, $r=1$, $\delta=10^{-3}$, $v\in\mathbb{Z}_2$ is uniformly chosen at random, the disturbance E is a random variable with the distribution ψ_β such that $P\{E=k\}=\frac{\beta^k}{2\cdot k!}\mathrm{e}^{-\beta}$ for integer k and $P\{E=0\}=\mathrm{e}^{-\beta}$ with parameter $\beta=10^{-3}$, $a\in\{-1,0,1\}$ is uniformly chosen at random. Then the probability of decryption error

$$\begin{aligned}&P\left\{f^{-1}\left(Ea+f\left(v\right)\right)\neq v\right\}=P\left\{\left[\frac{2}{5}\left(Ea+\left[\frac{5}{2}v\right]\right)\right]\neq v\right\}\\&=\frac{1}{2}P\left\{\left[\frac{2}{5}Ea\right]\neq 0\right\}+\frac{1}{2}P\left\{\left[\frac{2}{5}\left(Ea+2\right)\right]\neq 1\right\}\\&\leq\frac{1}{2}P\{E\neq 0\}+\frac{1}{2}P\{E\neq 0\}\\&=1-P\{E=0\}=1-\mathrm{e}^{-0.001}<10^{-3}.\end{aligned}$$

On the other hand,

$$2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+l\delta>10^{-3}.$$

So it follows that

$$P\left\{f^{-1}\left(Ea+f\left(v\right)\right)\neq v\right\}\leq 2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+l\delta.$$

The inequality in theorem 2 holds.

Example 2: Let $t=2$, $q=5$, $l=1$, $m=1$, $r=1$, $\delta=10^{-4}$, $v\in\mathbb{Z}_2$ is uniformly chosen at random, the disturbance E is a Laplace distribution variable with parameter $\lambda=0.05$ and probability density function $f\left(x\right)=\frac{1}{2\lambda}\mathrm{e}^{-\frac{|x|}{\lambda}}$ rounding to the nearest integer, $a\in\{-1,0,1\}$ is uniformly chosen at random. Similarly as example 1, the probability of decryption error

$$\begin{aligned}&P\left\{f^{-1}\left(Ea+f\left(v\right)\right)\neq v\right\}=P\left\{\left[\frac{2}{5}\left(Ea+\left[\frac{5}{2}v\right]\right)\right]\neq v\right\}\\&\leq 1-P\{E=0\}=1-\int_{-\frac{1}{2}}^{\frac{1}{2}}\frac{1}{2\lambda}\mathrm{e}^{-\frac{|x|}{\lambda}}\mathrm{d}x=\mathrm{e}^{-10}<10^{-4}.\end{aligned}$$

On the other hand,

$$2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+l\delta>10^{-4}.$$

It follows that

$$P\left\{f^{-1}\left(Ea+f\left(v\right)\right)\neq v\right\}\leq 2l\left(1-\Phi\left(\frac{q-t}{2\beta t}\sqrt{\frac{3}{mr\left(r+1\right)}}\right)\right)+l\delta.$$

The inequality in theorem 2 holds.

3. Results and Conclusion

In this work we first introduce the LWE problem and LWE-based cryptosystem.

We give a more precise estimation probability of decryption error based on independent identical Gaussian disturbances. The salient significance of our work is that for any general independent identical disturbances, we also give the estimation probability of decryption error using central limit theorem. The upper bound probability could be closed to 0 if we choose applicable parameters. It means that the probability of decryption error for the cryptosystem could be sufficiently small. Then we confirm that the LWE-based cryptosystem could have high security.

4. Discussion

Future Work

Although we have reached our objective in this work, there are still many interesting works to study in this research area in the future. We will focus on the fully homomorphic encryption (FHE) based cryptosystem later, which is an application of LWE [20] [21] [22] [23] [24]. Fully homomorphic encryption was known to have abundant applications in cryptography, but for three decades no plausibly secure scheme was known until 2009. To date, the FHE based cryptography has more than three generations. The third generation FHE scheme based on LWE problem is proved that has some unique and advantageous properties [24]. It also remains some improvable techniques which need to be studied in depth.

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 Thirty-Seventh 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] Ajtai, M. (1996) Generating Hard Instances of Lattice Problems. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, Philadelphia, 22-24 May 1996, 99-108. https://doi.org/10.1145/237814.237838

[4] 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

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

[6] 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

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

[8] Peikert, C. (2009) Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem. *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, Bethesda, 31 May-2 June 2009, 333-342. https://doi.org/10.1145/1536414.1536461

[9] Ajtai, M. (2005) Representing Hard Lattices with O(n log n) Bits. *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, Baltimore, 22-24 May 2005, 94-103. https://doi.org/10.1145/1060590.1060604

[10] Ajtai, M. and 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, 4-6 May 1997, 284-293. https://doi.org/10.1145/258533.258604

[11] Alekhnovich, M. (2003) More on Average Case vs Approximation Complexity. 44*th Annual IEEE Symposium on Foundations of Computer Science*, Cambridge, 11-14 October 2003, 298-307. https://doi.org/10.1109/SFCS.2003.1238204

[12] Regev, O. (2004) New Lattice Based Cryptographic Constructions. *Journal of the ACM*, **51**, 899-942. https://doi.org/10.1145/1039488.1039490

[13] Kawachi, A., Tanaka, K. and Xagawa, K. (2007) Multi-Bit Cryptosystems Based on Lattice Problems. *Public Key Cryptography*, *PKC* 2007, Beijing, 16-20 April 2007, 315-329. https://doi.org/10.1007/978-3-540-71677-8_21

[14] Peikert, C. (2007) Limits on the Hardness of Lattice Problems in l_p Norms. *Twenty-Second Annual IEEE Conference on Computational Complexity*, San Diego, 13-16 June 2007, 333-346. https://doi.org/10.1109/CCC.2007.12

[15] Peikert, C., Vaikuntanathan, V. and Waters, B. (2008) A Framework for Efficient and Composable Oblivious Transfer. *Annual Cryptology Conference*, Santa Barbara, 17-21 August 2008, 1-28. https://doi.org/10.1007/978-3-540-85174-5_31

[16] Signing, V., Tegue, G., Kountchou, M., Njitacke, Z., Tsafack, N., Nkapkop, J., *et al.* (2022) A Cryptosystem Based on a Chameleon Chaotic System and Dynamic DNA Coding. *Chaos*, *Solitons & Fractals*, **155**, Article ID: 111777. https://doi.org/10.1016/j.chaos.2021.111777

[17] Ding, J. (2004) A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation. *Public Key Cryptography*, *PKC* 2004, Singapore, 1-4 March 2004, 305-318. https://doi.org/10.1007/978-3-540-24632-9_22

[18] Asokan, N., Kostiainen, K., Ginzboorg, P., Ott, J., Luo, C., Asokan, P. *et al.* (2007) Applicability of Identity-Based Cryptography for Disruption-Tolerant Networking. *Proceedings of the* 1*st International MobiSys Workshop on Mobile Opportunistic Networking*, San Juan, 11 June 2007, 52-56. https://doi.org/10.1145/1247694.1247705

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

[20] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, Bethesda, 31 May-2 June 2009, 169-178. https://doi.org/10.1145/1536414.1536440

[21] Van 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

[22] 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

[23] Brakerski, Z. and Vaikuntanathan, V. (2011) Efficient Fully Homomorphic Encryption from (Standard) LWE. 2011 *IEEE* 52*nd Annual Symposium on Foundations of Computer Science*, Palm Springs, 22-25 October 2011, 97-106. https://doi.org/10.1109/FOCS.2011.12

[24] 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

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