SCIS 2011 The 2011 Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 25-28, 2011
The Institute of Electronics, Information and Communication Engineers

An Identity Based Encryption Scheme from Ideal Lattices

Ryouta Okuhata * Yoshifumi Manabe † Tatsuaki Okamoto ‡

Abstract— The learing with errors(LWE) problem is to distiguish random liner equtations, which have perturbed by small amount noise, from truly uniform ones. Recently the problem has served as the foundation of many cryptographic applications. Unfortunately, this is rather inefficient due to an inherent quadratic overhead in the use of standard LWE. In this paper we construct an identity based encryption scheme on the ideal learning with errors (Ideal-LWE) problem which is an algebraic variant of learning with errors (LWE). We make an identy-based encryption of LWE much more efficient through the use of Ideal-LWE.

Keywords: public-key encryption, lattices, identy-based encryption, learning with errors problem.

1 Introduction

1.1 Background

Recently, lattices have emerged as a very attractive foundation for cryptography. The appeal of lattice-based encryption mechanism stems from the fact that their strength of security is based on the worst-case hardness assumptions, and that they appear to remain secure even against quantum computers. More recently, Regev [10] defined the learning with errors (LWE) problem and proved that it enjoys similar worst-case hardness properties, under a quantum reduction. The LWE problem has proved to be versatile for cryptographic schemes, serving as the basic for secure public-key encryption under both IND-CCA secure PKE [10] and identity-based encryption [1, 11], and more. One bottleneck of schemes based on the LWE problem, however, is that they tend not to be efficient enough for practical applications. A promising approach for avoiding this inefficiency is to use a lattice that possess an extra algebraic structure.

Identy-Based Encryption(IBE) provides a public-key encryption mechanism where a public key is an arbitary string such as an email address or a telepohone number. The corresponding private key can only be generated by a Private Key Generater who has knowledge of a master secret. Agrawal, Boneh and Boyen constructed a lattice-based IBE [1]. They showed how to build a secure IBE in the standard model from the learning with errors (LWE) problem. Their cryptosysytem have two trapdoors for finding short vectors. All previous cryptosystems based on general lattices rely on average case hardness of the Learning With Errors (LWE) problem introduced in [10]. Our scheme is based on a structured varient of LWE, that is called Ideal-LWE [2].

1.2 Our Results

In this paper, we introduce an identy-based encryption on Ideal-LWE. By this change, we can make use of the trapdoor in [2] instead of the one in [1]. When the trapdoor in [2] is used, the size of plaintext that can be encrypted with the same size of key is larged than the trapdoor in [1].

2 Preliminaries

2.1 Ideal lattices

Ideal lattices are special subset of lattices that possess the computationally interesting property of being related to structured matrices and polynomials. The n-dimensional matrix-matrix and vector-matrix products then respectively cost $\tilde{\mathrm{O}}(n^2)$ and $\tilde{\mathrm{O}}(n)$ arithmetic operations instead of $\mathrm{O}(n^3)$ and $\mathrm{O}(n^2)$. Let $f \in \mathbb{Z}[x]$ be a monic dgree n polynomial. For any $g \in \mathbb{Q}[x]$,there is a pair (q, r) with $\deg(r) < n$ and $g = qf + r$. We denote r by $g \bmod f$ and identify r with the vector $\mathbf{r} \in \mathbb{Q}^n$ of its coefficient. We denote $rot_f(r) \in \mathbb{Q}^{n \times n}$ as a matrix the rows for which are $x_i r(x) \bmod f(x)'s$, for $i \in [0, n-1]$. We extend that notation to the matrices A over $\mathbb{Q}[x]/f$:

* Department of Social Informatics, Graduate School of Informatics, Kyoto Univ.
† NTT Labs, Nippon Telegraph and Telephone Corporation.
‡ NTT Labs, Nippon Telegraph and Telephone Corporation.

by replacing each $A_{i,j}$ with $rot_f(A_{i,j})$, and we obtain $rot_f(A)$. Note that $rot_f(g_1)rot_f(g_2) = rot_f(g_1 g_2)$ for any $g_1, g_2 \in \mathbb{Q}[x]/f$.

Property 1 (Lemma 2.3 in [2])
Let $k \geq 0$ and $n = 2^k$. Then $f(x) = x^n+1$ is irreducible in $\mathbb{Q}[x]$. Its expansion factor EF(f,2) $\leq \sqrt{2}$. Also, for any $g = \sum_{i<n} g_i\ x_i \in \mathbb{Q}[x]/f$, we have rot_f(g) = $rot_f(\bar{g})$ where $\bar{g} = g_0$ - $\sum_{1<i\leq n} g_{n-i}\ x_i$. Furthermore, if q is a prime such that $2n \mid (q\text{-}1)$, then $f(x)$ has n degree 1 factors in $\mathbb{Z}_q[x]$. Finally, if k $\geq$2 and q is a prime with $q \equiv 3\ mod\ 8$ then $f = f_1 f_2 mod\ q$ where, for any $i \in \{0,1\}$, we have that f_i is irreducible in $\mathbb{Z}_q[x]$ and can be written $f_i = x^{\frac{n}{2}} + t_i x^{\frac{n}{4}} - 1$ with $t_i \in \mathbb{Z}_q$.

2.2 Ideal-LWE

The Learning With Errors problem with parameters $q(\cdot)$, $m(\cdot)$, and a distribution $\chi(\cdot)$ on $\mathbb{R}/[1,q(\cdot)]$ ($LWE_{q,m;\chi}$) is as given hereafter. Given n, matrix $G \in \mathbb{Z}_{q(n)}^{m(n)\times n}$ sampled uniformly at random and $G\mathbf{s} + \mathbf{e} \in (\mathbb{R}/[1, q(n)])^n$, where $\mathbf{s} \in \mathbb{Z}_{q(n)}^n$ is chosen uniformly at random and the coordinates of $\mathbf{e} \in (\mathbb{R}/[q(n)])^{m(n)}$ are independently sampled from χ(n) , find $\mathbf{s}$.
The Ideal Learning With Errors with parameters $q(\cdot)$, $m(\cdot)$, a distribution $\chi(\cdot)$ on $\mathbb{R}/[1,q(\cdot)]$ and f ($Ideal - LWE^f_{q,m;\chi}$) is the same as above, except that G is of the form $G = rot_f(\mathbf{g})$ with $\mathbf{g}$ chosen uniformly in $(\mathbb{Z}_q[x]/f)^m$.

Definition 1 For q prime, let $\mathbf{R} = \mathbb{Z}/(x^n+1)$, $A \in \mathbf{R}$, $u \in \mathbf{R}$, define:

$$\Lambda_q(R) := \{e \in \mathbf{R}\ \exists s.t.\ s \in \mathbf{R}\ where\ A^T s = e \pmod q\}$$
$$\Lambda_q{}^{\perp}(R) := \{e \in \mathbf{R}\ s.t.\ \ Ae = 0 \pmod q\}$$
$$\Lambda_q{}^{u}(R) := \{e \in \mathbf{R}\ s.t.\ \ Ae = u \pmod q\}$$

2.3 Discrete Gaussians

Let L be a subset of $\mathbf{Z}\mathbf{F}^m$. For any vector c $\in \mathbf{R}^m$ and any positive parameter $\sigma \in \mathbf{R}_{>0}$, define:

$\rho_{\sigma,c}(x) = \exp(\text{-}\pi\ \frac{\|x-c\|^2}{\sigma^2})$: A Gaussian-shaped function on $\mathbf{R}^m$ with center c and parameter σ,
$\rho_{\sigma,c}(L) = \sum_{x\in L} \rho_{\sigma,c}(x)$: the (always converging) sum of $\rho_{\sigma,c}$ over L,
$\mathcal{D}_{L,\sigma,c}$: the discrete Gaussian distribution over L with parameters σ and c,

$$\forall y \in L\ ,\ \mathcal{D}_{L,\sigma,c}(\text{y}) = \frac{\rho_{\sigma,c}(y)}{\rho_{\sigma,c}(L)}$$

We abbreviate $\rho_{\sigma,0}$ and $\mathcal{D}_{L,\sigma,0}$ as ρ_σ and $\mathcal{D}_{L,\sigma}$. We write ρ to denote ρ_1. The distribution $\mathcal{D}_{L,\sigma,c}$ will most often be defined over the lattice $L = \Lambda_q{}^{\perp}(A)$ for ring elements $A \in \mathbf{R}^m$ or over a coset $L = t + \Lambda_q{}^{\perp}(A)$ where $t \in \mathbb{Z}^m$.

Property 2. The follwing lemma is a substitute for the ideal-LWE lemma following from [4] and [1] that captures standard properties of these distributions. The first two properties follow from Lemma 4.4 of [7] and Corollary 3.16 of [10] (using Lemma 3.1 from [6] to bound the smoothing parameter). We state in property (2) a stronger version of Regev's Corollary 3.16 found in [2]. The last properties are algorithms from [6].

Lemma. Let A be ring element in $R = \mathbf{Z}_q[x]/(x^n+1)$ with k$\geq$0, $n = 2^k$. Then for $c \in \mathbb{R}^m$ and $u \in \mathbf{R}$, we have the following.
1. Pr$[x \sim \mathcal{D}_{\Lambda_q^u(A),\sigma} : |x| > \sqrt{m}\sigma] \leq$ negl(n).

2. A set of O$(m \log m)$ samples from $\mathcal{D}_{\Lambda_q^u(A),\sigma}$ contains a full rank set in $\mathbb{Z}^m$, except with negligible probality.

3. There is a PPT algorithm **SamplePre**(A, T_A, u, σ) that returns $x \in \Lambda_q{}^u(A)$ sampled from a distribution statically close to $\mathcal{D}_{\Lambda_q^u(A),\sigma}$ whatever $\Lambda_q{}^u(A)$ is not empty.

This **SamplePre** algorithm is needed to generate master key in the proposed encryption system.

Definition2. Consider a real parameter $\alpha = \alpha(n) \in$ (0,1) and a prime q. Denote by $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ the group pf reals [0,1) with adition modulo 1. Denote by Ψ_α the distribution over $\mathbb{T}$ of a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$ then reduced modulo 1. Denote by $\lfloor \text{x} \rceil = \lfloor x + \frac{1}{2} \rfloor$ the nearest integer to the real $x \in \mathbb{R}$. We denote by $\overline{\Psi_\alpha}$ the distribution over $\mathbb{Z}_q$ of the random variable $\lfloor \text{qX} \rceil$ mod$q$ where the random varieble $X \in \mathbb{T}$ has distribution Ψ_α.

Property 3.(Lemma 19 in [1]) Let e be some vector in $\mathbb{Z}^m$ and let $y \xleftarrow{R} \overline{\Psi_\alpha}$. Then the quantity $|e^T y|$ treated as an integer in [0,q-1] satisfies

$$|e^T y| \leq \|e\| q\alpha\omega(\sqrt{log\ m}) + \|e\|\frac{\sqrt{m}}{2}$$

with all but negligible probability in m.

2.4 The Norm of a Random Matrix

Recall that norm of a matrix $R \in \mathbb{R}^{k\times m}$ is defined as $\|R\| := sup_{\|u\|=1}\|Ru\|$. We will need the following lemma from Litvak et al. [8] to bound the norm of a random matrix in $\{-1,1\}^{m\times m}$. A similar lemma appears in [9, Lemma 2.2].

Property 4(Lemma 7 in [1]) Let R be an $m \times m$ matrix chosen at random from $\{-1,1\}^{m\times m}$. Then for all vectors $u \in \mathbb{R}^m$ we have

$$Pr[\|R\| > C\sqrt{m}] < e^{-m}$$

for some universal constant C (taking $C = 16$ is sufficient).

2.5 Sampling Algoritms

Let A and B be a ring element in $\mathbf{R}$ and let be $R \in \mathbf{R}$ and R's coefficients must be a $\in$ {-1,1}. The proposed construction makes use of matrices in the form $F = (A \mid AR + B) \in \mathbf{R}^{2m}$ and we need to sample short ring elements in ${\Lambda_q}^u$ (F) for u in $\mathbf{R}$. More precisely, we define the following algorithm:

SampleLeft takes a basis for ${\Lambda_q}^{\perp}$(A) and outputs short vector $e \in {\Lambda_q}^u$(F).

2.5.1 Algorithm SampleLeft

Algorithm **SampleLeft**(A, M_1, T_A, u, σ):
Inputs:

a ring element A in $\mathbf{R}^m$ and a ring element M_1 in $\mathbf{R}^m$, a "short" basis of ${\Lambda_q}^{\perp}(A)$ and a ring element $u \in \mathbf{R}$, a gaussion parameter $\sigma > \|\tilde{T}_A\| \cdot \omega(\sqrt{log(2m)})$. (1)

Output: Let $F_1 := (A|M_1)$. The algorithm outputs a vector $e \in \mathbf{R}^{m+m_1}$ sampled from a distribution statically close to $\mathcal{D}_{\Lambda_q^u(F_1)}$. In paticular, $e \in {\Lambda_q}^u(F_1)$.

The algorithm appears in Theorem 3.4 in [1] and in the signing algorithm in [31]. For completeness, we briefly review the algorithm.

1. Sample random ring element $e_2 \in \mathbf{R}^m$ distributed statically close to $\mathcal{D}_{\mathbf{R},\sigma}$. ,
2. Run $e \xleftarrow{R}$ **SamplePre**(A, T_A, y, σ) where $y = u - (\mathrm{M}\cdot e_2) \in \mathbf{R}$.
3. Output $e \leftarrow (e_1,e_2) \in \mathbf{R}^{2m}$

We have $(A \mid M_1)\cdot e = u \mod q$ and hence $e \in {\Lambda_q}^u(F_1)$. Theorem 3.4 in [3] shows that the ring element e is sampled from distribution statistically close to $\mathcal{D}_{\Lambda_q^u(F_1)}$.

Property 5. This property from theorem 14 in [1]. Let $q > 2, m > n$ *and* $\sigma > \|\tilde{T}_A\| \cdot \omega(\sqrt{log(2m)})$. Then **SampleLeft**($A, M_1, T_A, u, \sigma$) taking inputs as in (1), outputs a vector $e \in \mathbf{R}^{2m}$ distributed statically close to $\mathcal{D}_{\Lambda_q^u(F_1)}$, where $F_1 := (A|M_1)$.

2.6 Trapdoor in Ideal-LWE

The following Theorem can be mainly derived from [2]. The purpose of this section is to demonstrate how to create a **TrapGen** algorithm that generates a master key in this encryption system. In Ajtai and Alwen-Peikert [1], a few uniformly distributed random vectors $(\mathbf{g}_i)_{i\leq\sigma}$ are first generated and then are used as the seed to produce other random vectors $(\mathbf{g}_i)_{i>\sigma}$ that are seemingly uniformly distributed. Using this property, the following algorithm is generated.

For $g_1, g_2, \ldots, g_r \in \mathbf{R}$, we denote by $H(g_1, g_2, \ldots, g_r)$ random variable $\sum_{i\leq 0} b_i g_i \in \mathbf{R}$ where b_i are degree $< n$ polynomials with coefficients chosen independently and uniformly in $\mathcal{D}$. Let $\mathbf{g}$ be in $\mathbf{R}^m$ with $\mathbf{R} = \mathbb{Z}_q/f$ and a full-rank set S of small linearly independent vectors belonging to lattice $G^{\perp} = rot_f(\mathbf{g})$. For this, it suffices to find rank m set of R_0-linearly independent short vectors in module $M^{\perp}(\mathbf{g}) = \{\mathbf{a} \in \mathbf{R_0^m} | \langle \mathbf{a}, \mathbf{g} \rangle \equiv 0 \mod q\}$, with $\mathbf{R}_0 = \mathbb{Z}[x]/f$.
We first generate some seed elements $g_1, g_2, \ldots, g_\sigma$ in $\mathbf{R}$. They will be the first elements of Ideal-LWE instantiation. They need sufficient yield so that arbitrary elements of $\mathbf{R}$ can be written up as linear combinations of them. From the seed, derive some intermediate ring elements $h_1, h_2, \ldots, h_m$. Among them, there should be a sufficient number of elements that are uniformly distributed in $\mathbf{R}$, so that we may use Theorem 3.2 in [3]. The first h_i's have the technical purpose of allowing to have small relations between $g_1, g_2, \ldots, g_\sigma, h_{\sigma+1}, \ldots, h_m$. More precisely, we will have:

$$[A|B](g_1, g_2, \ldots, g_\sigma, h_{\sigma+1}, \ldots, h_m)^T = (0, \ldots, 0)^T \quad (1)$$

where $A \in \mathbf{R}_0^{(m-\sigma)\times\sigma}$ and $B \in \mathbf{R}_0^{(m-\sigma)\times(m-\sigma)}$ have small entries. B is lower triangular with 1's on the diagonal.
Since the last r of polynomials $h_{m-r-1}, \ldots, h_m$ are uniformly distributed in $\mathbf{R}$, we take them as the last g_i's, and we construct the missing g_i's by:

$$g_i = \begin{cases} h_i + H(h_{m-r+1}, \ldots, h_m), i \in [\sigma+1, m-r], \\ h_i, \qquad\qquad\qquad\qquad i \in [m-r+1, m] \end{cases} \quad (2)$$

Thanks to Theorem 3.2 in [2], we see that whenever were the first h_i's, the uniformly of last ones provides a close to uniform distribution of $(g_1, \ldots, g_m)$. We have that, for all $i \in [\sigma+1, m-r]$,
$g_i = h_i + \sum_{j=m-r+1}^{m} y_{i,j} h_j$, where each $y_{i,j}$ is a degree $< n$ polynomial with coefficients chosen independently and uniformly in D. We define $C \in \mathbf{R}_0^{m-\sigma\times m-\sigma}$ as follows:

$$C = \left[\begin{array}{c|c} Id_{m-\sigma-r} & (y_{i,j}) \\ \hline 0 & Id_r \end{array}\right]$$

Equation (2) implies that

$C \cdot (h_{\sigma+1}, \cdots, h_m)^T = (g_\sigma, \cdots, g_m)^T$ and $[A|B \cdot C] \cdot (g_1, \cdots, g_m)^T = (0, \cdots, 0)^T$.

Then we define:
$h_{m-r-\sigma+i} = 2^{-1} g_i$ for $i \le \sigma$, where the inverse is taken as modulo q.
This give us σ additional relations, since (for $i \le \sigma$):

$$\begin{aligned} 2g_{m-r-\sigma+i} &= 2h_{m-r-\sigma+i} + 2H(h_{m-r+1}, \cdots, h_m) \\ &= g_i + 2H(g_{m-r+1}, \cdots, g_m) mod\ q \end{aligned} \quad (3)$$

Let $2g_{m-r-\sigma+i} = g_i + 2\sum_{j=m-r+1}^{m} z_{i,j} g_j$ over $\mathbb{Z}$, where each $z_{i,j}$ is a degree $< n$ polynomial which has coefficients chosen uniformly and independently from D. We define $\sigma \times (m-\sigma)$ matrix K:

$K = [0| - 2Id_\sigma | 2(z_{i,j})]$.

From Equation(3), we have that $[Id_\sigma|K] \cdot (g_1, \cdots, g_m)^T \equiv (0, \cdots, 0)^T mod\ q$. As a result, we obtain uniformly distributed g_i's and relations of the type (over R):

$$\left[\begin{array}{c|c} A & B \cdot C \\ \hline Id_\sigma & K \end{array}\right] \begin{bmatrix} g_1 \\ \vdots \\ g_m \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

where A and B are those of Equation(1), $C \in R_0^{(m-\sigma)\times(m-\sigma)}$ is upper triangular with $1's$ on its diagonal, and $K \in R_0^{\sigma\times(m-\sigma)}$ is divisible by 2. All these matrices have small entries.
Next, we show a construction method for A and B. We start by generating $h_{m-r+1}, \ldots, h_m$ uniformly and independently in R. Additionally, we set $h_{m-r-\sigma+i} = 2^{-1} g_i$ for $i \le \sigma$. For any $i \in [m-r-\sigma+1, m]$, we write h_i as a linear combination over $\mathbf{R}$ of the seeds: $h_i = \sum_{j\le\sigma} x_{i,j} g_j$. We use the binary decompositions of these polynomials to write: $h_i = \sum_{k=0}^{\kappa-1} \sum_{j\le\sigma} x_{i,j,k} g_j 2^k$,with $\kappa = \lceil \log q \rceil$. The $x_{i,j,k}$'s are polynomials with $\{0,1\}$-coefficients.
We use the $x_{i,j,k}$'s in A. The latter starts with $k+\sigma$ blocks of $R_0^{\kappa\times\sigma}$. The ith blocks is made of the $x_{i,j,k}$'s(for$j \le s$ *and* $0 \le k \le \kappa-1$) by decreasing the value of k.
Matrix B is as follows

$$B = \left[\begin{array}{ccc|c} T & & & \\ & \ddots & & \\ & & T & \\ \hline & E & Id & \end{array}\right],$$

where there are $r+\sigma$ blocks T and $E[i,j]$ = -1 if $i = j\kappa$ and 0 otherwise.

3 Encoding Identities as Ring Elements

The proposed construction uses encoding function H: $=\mathbf{R} \to \mathbf{R}^m$ to map identities in $\mathbf{R}$.

Now, for input $u = a_0 + a_1 \mathrm{X} + \ldots + a_{n-1}\ X^{n-1} \in \mathbf{R}$ define the polynomial $g_u(\mathrm{X}) = \sum_{i=0}^{n-1} u_i\ X^i \in \mathbf{R}[\mathrm{X}]$.

Define $H(u)$ as

$$H = \begin{pmatrix} g(X) \\ X \cdot g(X) \bmod f \\ X^2 \cdot g(X) \bmod f \\ \vdots \\ X^{m-1} \bmod f \end{pmatrix}$$

This completes the construction. Since for all primes q and integers $n > 1$ there are irreducible polynomials in $\mathbb{Z}_q[X]$ of degree n, the construction can accommodate any pair of q and n.

4 Construction of IBE Based on Ideal-LWE

Setup(λ): On input a security parameter λ, set parameters q,n,m,σ,α as specified in the section below. Procedure:

1. Select a uniformly random ring element $\mathbf{g} \in \mathbf{R}^m$.

2. Use algorithm **TrapGen**($\mathbf{g}$, m) to generate $T_A \in \mathbf{R}^{m \times m}$ such that $\|T_A\| \leq \sqrt{\sigma n + 9(m-\sigma)}$.

3. Select two unifomly random vectors A_1,B in $\mathbf{R}^m$

4. Select a uniformly random ring element u $\stackrel{R}{\leftarrow}$ $\mathbf{R}$

5. Output the public parameters and master key,

$\mathbf{PP} = \left(A_0, A_1, B_0, \text{u} \right)$; $\mathbf{MK} = \left(T_{A_0} \right) \in \mathbf{R}^{m \times m}$

Extract(PP , MK , id): On input public parameters PP, a master key MK , and an identity id $\in \mathbf{R}^m$, do:

1. Sample e $\in \mathbf{R}^{2m}$ as e $\leftarrow$ **SampleLeft**(A_0, $A_1 + H(id)$, T_{A_0}, u, σ) where H is a map as defined in Section 3. Note that A_0 is rank n w.h.p as explained in Section 4.1.

2. Output $\mathbf{SK}_{id} := e \in \mathbf{R}^{2m}$

Let $F_{\mathbf{id}} := (A_0 \mid A_1 + H(id)B)$, then $F_{\mathbf{id}} = u$ in $\mathbf{R}$ and e is distributed as by Property 3.

Encrypt(PP, id, b_i): On input public parameters **PP** , an identity id, and message b_i $(i = 1, \ldots, m) \in \{0,1\}^m \in \mathcal{D}$, do:

1. Set $\mathbf{F}_{id} \leftarrow (A_0 \mid A_1 + \text{H(id)} \cdot \text{B}) \in \mathbf{R}^{2m}$

2. Choose a uniformly random $s \stackrel{R}{\leftarrow} \mathbf{R}$

3.Choose a uniformly random $m \times m$ $\mathbf{Y} \stackrel{R}{\leftarrow} \{0,1\}^{m \times m}$

4. Choose noise vector x's each coefficient $\stackrel{\overline{\Psi_\alpha}^m}{\leftarrow}$ $\mathbf{R}^m$and y's each coefficient $\stackrel{\overline{\Psi_\alpha}^m}{\leftarrow}$ $\mathbf{R}$, and set $z \leftarrow R^T \text{y} \in \mathbf{R}^m$ (the distribution is as in Definition 2),

5. Set $c_0 \leftarrow u^T s + x + b_i \; X^i \; \lfloor \frac{q}{2} \rfloor \in \mathbf{R}$

$$c_1 \leftarrow F_{id}^T \cdot s + \begin{bmatrix} y \\ z \end{bmatrix} \in \mathbf{R}^{2m}$$

6. Output the cipertext $\mathbf{CT} := (c_0, c_1) \in \mathbf{R}^m \times \mathbf{R}^{2m}$.

Decrypt(PP , SK_{id} , CT): On input parameters PP , a private key $SK_{id} := e_{id}$, and a ciphertext CT = (c_0 , c_1) , do:

1. Compute $w \leftarrow c_0$ - $e_{id}^T c_1 \in \mathbf{R}$.

2. Compute X_i's coefficient of w and $\lfloor \frac{q}{2} \rfloor$ treating them as integers in $\mathbf{R}$.

4.1 Correctness

When the cryptosystem is operated as specified, we have,

$$w = c_0 - e_{id}^T c_1 = b_i X^i \lfloor \frac{q}{2} \rfloor + \underbrace{x - e_{id}^T \begin{bmatrix} y \\ z \end{bmatrix}}_{error\ term}$$

The norm for the error term is bounded by w.h.p.

Proof. Letting $e_{id} = (e_1 | e_2)$ with $e_1, e_2 \in \mathbf{R}^2$ the error term is

$$x - e_1^T y - e_2^T z = x - e_1^T y - e_2^T R^T y = x - (e_1 - Y e_2)^T y$$

By Property 2, we have $\|e_{id}\| \leq \sigma\sqrt{2m}$ w.h.p.
Hence, by Property 4, we have $\|e_1 - Y e_2\| \leq \|e_1\| + \|Y e_2\| \leq O(\sigma m)$.

Then, by Property 3 the error term is bounded by

$$|x - e_{id}^T \begin{bmatrix} y \\ z \end{bmatrix}|_i \leq |x|_i + |(e_1 - Ye_2)^T y|_i \leq \{q\alpha m\omega(\sqrt{logm}) + O(\sigma m^{\frac{3}{2}})\}_i$$

as required.

参考文献

[1] Shweta Agrawal, Dan Boneh, Xavier Boyen Efficient Lattice (H)IBE in the Standard Model., Cryptology ePrint Archive,Report 2010/113 2010. http://eprint.iacr.org/.

[2] Damien Stehle, Ron Steinfeld, Keisuke Tanaka, Keita Xagawa *Efficient Public Key Encryption Based on Ideal Lattices*, Cryptology ePrint Archive, Report 2009/285, 2009. http://eprint.iacr.org/.

[3] David Cash, Dennis Hofheinz, and Eike Kiltz. *How to delegate a lattice basis.* , Cryptology ePrint Archive, Report 2009/351, 2009. http://eprint.iacr.org/.

[4] Chris Peikert. *Bonsai trees (or, arboriculture in the lattice-based cryptography).*, Cryptology ePrint Archive, Report 2009/359, 2009. http://eprint.iacr.org/.

[5] Shweta Agrawal, Dan Boneh, and Xavier Boyen. *Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE*, CRYPTO 2010, LNCS volume 6223, pages 98-115. 2010.

[6] C. Gentry, C.Peikert, and V.Vaikuntanathan. *Trapdoors for hard lattices and new cryptographic constructions*, In Proc.of STOC'08, pages 197-206,2008

[7] Daniele Micciancio and Oded Regev. *Worst-case to average-case reductions based on gaussian measures.* In Proc. of FOCS'04, pages 372-381, 2004

[8] A.Litvak, A.Pajor, M.Rudelson, and N. Tomczak-Jaegermann. *Smallest singular value of random matrices and geometry of random polytypes.*, Advance in Mathematics, 195(2):491-523,2005.

[9] Joel Alwen and Chris Peikert. *Generating shorter bases for hard random lattices*, In Proc. of STACS'09, pages 75-86 , 2009.

[10] Oded Regev, *On lattices, learning with errors, random liner codes, and cryptography.*, J.ACM 56(6) (2009); Preliminary version in STOC 2005

[11] Cash, D., Hofheinz, D., Klitz, E., Peikert, C.: *Bonsai trees, or how to delegate a lattice basis.* In: EUROCRYPT 2010