Lattice Ciphertext Policy Attribute-based Encryption in the Standard Model

Yongtao Wang
China Information Technology Security Evaluation Center, Beijing 100085, P.R.China
(E-mail: wyt.itsec@gmail.com)
(Received Feb. 6, 2013; revised and accepted June 19, 2013)

Abstract

A lattice ciphertext policy attribute based encryption (CP-ABE) scheme is presented, in which the ciphertext policy achieved is the AND-gates on multi-valued attributes. The previous construction with AND-gates on multi-valued attributes as ciphertext policy is based on bilinear paring technology. In this paper, inspired by the recent progress of lattice identity based encryption scheme, we achieve this access structure from lattice technology. There are two constructions given, and both of them can be viewed as an extension and generalization of the lattice identity based encryption schemes proposed by Agrawal *et al.*, respectively. In addition, our constructions are shown to be secure under the learning with errors assumption in the standard model.

Keywords: Access structure, attribute-based encryption, lattice, learning with errors, standard model

1 Introduction

The notion of attribute based encryption was first introduced by Sahai and Waters [18] at EUROCRYPT'05. In their scheme, a sender can generate a ciphertext according to an attribute set ω and a user described by an attribute set γ can get a private key from the authority. When at least d (threshold parameter) attributes overlapped between ω and γ, the user is allowed to decrypt this ciphertext. The above scheme achieves threshold access structure. At present, some access structures of more complexity are achieved. Attribute based encryption scheme can be viewed as a generalization of identity based encryption (IBE) [8, 19, 21]. Substantially, the notion of attribute based encryption integrates an access structure with the notion of identity based encryption.

There are two approaches for an attribute based encryption scheme to deploy access control policy. One is Key-Policy attribute-based encryption (KP-ABE) scheme [13, 15, 20] first proposed by Goyal et al. [13]. In their cryptosystem, ciphertexts are labeled with sets of attributes, and private keys are identified by a tree-access structure in which each interior node of the tree is a threshold gate and the leaves are associated with attributes. This access tree control which ciphertexts a user is able to decrypt. The other approach to deploy policy is ciphertext-policy attribute-based encryption (CP-ABE) schemes [6, 7, 16, 22]. In these schemes, a message is encrypted with a specific access policy determined by the encrypter, and private keys issued by a trusted authority are labeled with sets of attributes. Decryption requires that the attribute set of a user matches the cipertext policy. There are many applications for both types of ABE systems, such as sharing of audit-log and broadcast encryption. In addition, all the above schemes are shown to be secure in the selective model. Lewko *et al.* [14] proposed an attribute based encryption scheme which is secure in the full model.

Lattice-based cryptography has many appealing properties, for example, it can be implemented efficiently and it is believed to be secure against quantum computer. Notice that there are several lattice identity based encryption schemes proposed. In [12], the author gives a construction of lattice IBE in the random oracle model by using trapdoor functions with preimage sampling. In the standard model, Cash *et al.* [10], Agrawal *et al.* [1] (denoted by ABB-1) and Agrawal *et al.* [2] (denoted by ABB-2) present efficient constructions for lattice IBE. At present, attribute based encryption schemes are mainly built on the technique of bilinear map. Recently, lattice ABE achieved some progresses [3, 9, 23].

In this work, we present a lattice ciphertext policy attribute based encryption scheme and give two corresponding constructions. The ciphertext policy achieved is AND-gates on multi-valued attributes. We notice that this access structure has been used before in [11] for constructing an attribute based encryption scheme, which has constant length of ciphertext. The previous construction with AND-gates on multi-valued attributes as ciphertext policy is based on bilinear paring technology. In this paper, inspired by the recent progress of lattice identity based encryption scheme, we achieve this access structure from lattice technology. Both of the constructions can be viewed as an extension and generalization of the lattice identity based encryption schemes in [1] and [2], respectively. In the first construction, a uniformly random

vector $u_{i,j} \in \mathbb{Z}_q^n$ is chosen to represent an attribute value $v_{i,j}$, where $i \in [N], j \in [N_i]$, and we map attribute vectors to matrices by the encoding function with full-rank differences (FRD) $H : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \times n}$ described in [1]. Based on the above, we can compute $\sum_{v_{i,j} \in L} H(u_{i,j})$ for some attribute list L due to the domain of H forms an additive group. However, the private key for a user in this construction is a vector $e \in \mathbb{Z}^{2m}$. Furthermore, we give another construction, which is based on the lattice identity based encryption scheme in [2] and is a fix dimension lattice ciphertext-policy attribute-based encryption scheme (*i.e.*, $e \in \mathbb{Z}^m$). Thus, this construction has short private key. If we view the original lattice IBE in [2] as a lattice ABE supporting And-gates on two-valued attributes (*i.e.*, 1 or 0), our construction extends it to a lattice ABE that achieves And-gates on multi-valued attributes. In addition, both our constructions are shown to be secure under the learning with errors assumption in the standard model. Note that the access structure achieved in this paper is relatively simple, and it is the future work for achieving access structure of more complexity.

The rest of the paper is organized as follows. In Section 2 we recall some preliminaries. In Section 3 we describe our first construction and prove its security. The second construction and it's proof for security are presented in Section 4. Finally, we conclude in Section 5.

2 Preliminaries

In this section, we describe some preliminaries for our scheme. Throughout the paper, we say $i \in [n]$ means that $i \in \{1, 2, \ldots, n\}$. Let $S = \{s_1, s_2, \ldots, s_j\}$ be a set of vectors. The notation $\|S\|$ denotes the ℓ_2 length of the longest vector in S, $\widetilde{S}$ denotes the Gram-Schmidt orthogonalization of S and $\|\widetilde{S}\|$ denotes the Gram-Schmidt norm of S.

2.1 Access Structure and Ciphertext Policy Attribute based Encryption

Access structure. In our scheme, the policy that we achieved is AND-gates on multi-valued attributes. This access structure has been used before in [11] and is defined as follows.

Definition 1. *Let $\mathcal{U} = \{att_1, att_2, \ldots, att_N\}$ be a set of attributes. For $att_i \in \mathcal{U}$, $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,N_i}\}$ is a set of possible values, where N_i is the number of possible values for att_i. Let $L = [L_1, L_2, \ldots, L_N], L_i \in S_i$ be an attribute list for a user, and $W = [W_1, W_2, ..., W_N], W_i \in S_i$ be an access structure. The notation $L \vDash W$ expresses that an attribute list L satisfies an access structure W, namely, $L_i = W_i (i = 1, 2, \ldots, N)$.*

Note that the total number of access structures is $\Pi_{i=1}^{N} N_i$. To generate a ciphertext under some access structure W, an encryptor has to explicitly indicate a value $v_{i,*}$ from $S_i = \{v_{i,1}, v_{i,2}, \ldots, v_{i,N_i}\}$ for each $att_i \in \mathcal{U}$.

Ciphertext policy attribute based encryption. Formally, a ciphertext policy attribute based encryption scheme consists of four polynomial-time algorithms described as follows [16]:

- **Setup**: This algorithm takes as input the security parameter κ and generates a set of domain parameters consisting of a public parameter PP and a master secret key MK. It is a randomized algorithm.
- **KeyGen**: Given the public parameter PP, the master secret key MK and an attribute list L for a user, this algorithm generates a user secret key SK_L associated with L. It could be probabilistic.
- **Encrypt**: On input of the public parameter PP, an access structure W and a message M, this algorithm outputs a ciphertext C. It should be probabilistic.
- **Decrypt**: On input of a user secret key SK_L and a ciphertext C for a message M encrypted under an access structure W, this algorithm outputs the message M if $L \vDash W$.

In our scheme, each ciphertext is encrypted for a message bit $b \in \{0, 1\}$. Thus, M in the above description of algorithms means a message bit b.

The security model of our scheme is modified from the model in [1] and is defined by using the following selective security game. This game captures a strong privacy property that it is indistinguishable between the challenge ciphertext and a random element in the ciphertext space.

Selective security game for our lattice CP-ABE:

- **Init.** The adversary declares an access structure W^*, that he wishes to be challenged upon.
- **Setup.** The challenger runs the **Setup** algorithm of the scheme and gives the public parameters PP to the adversary.
- **Phase 1.** The adversary is allowed to issue private key queries for any attribute list L, where $L \nvDash W^*$. The challenger runs algorithm **KeyGen** to obtain a private key SK_L and returns it to the adversary.
- **Challenge.** The adversary submits a message bit $b^* \in \{0, 1\}$. The challenger flips a random coin r and chooses a random ciphertext C in the ciphertext space. If $r = 0$, it sets the challenge ciphertext $C^* =$ **Encrypt**(PP, W^*, b^*). Otherwise (*i.e.*, $r = 1$), it sets challenge ciphertext $C^* = C$. It sends C^* to the adversary.
- **Phase 2.** Phase 1 is repeated.
- **Guess.** The adversary outputs a guess r' of r.

The advantage ϵ of an adversary $\mathcal{A}$ in this game is defined as $|\Pr[r' = r] - \frac{1}{2}|$. In addition, the adversary does not declare an access structure W^* before the **Setup** stage in the adaptive security game.

Definition 2. *A lattice ciphertext policy attribute based encryption scheme is secure in the selective model if all polynomial-time adversaries have at most a negligible advantage in the above game.*

2.2 Integer Lattices and the Gram-Schmidt Norm of a Basis

In this section, we give some definitions that are directly related to our construction. For further information (such as the discrete Gaussian distribution over lattice), the reader is referred to previous literatures [1, 2, 10, 12].

Integer lattices. Let $b_1, b_2, \ldots, b_m \in \mathbb{R}^m$ be m linearly independent vectors, the m-dimensional full-rank lattice generated by those vectors is the set defined as

$$\Lambda = \mathcal{L}(b_1, b_2, \ldots, b_m) = \left\{ \sum_{i=1}^{m} x_i b_i | x_i \in \mathbb{Z} \right\}.$$

The set of the vectors $b_1, b_2, \ldots, b_m$ is a basis of the lattice Λ. In addition, if define the $m \times m$ matrix B by letting his columns are $b_1, b_2, \ldots, b_m$, we have equivalently

$$\Lambda = \mathcal{L}(B) = \mathcal{L}(b_1, b_2, \ldots, b_m) = \{Bx | x \in \mathbb{Z}^m\}.$$

Further, it is called integer lattice when $\Lambda \subseteq \mathbb{Z}^m$.

Definition 3. *([1]) For prime q, $A \in \mathbb{Z}_q^{n \times m}$ and $u \in \mathbb{Z}_q^n$, define:*

$$\Lambda_q(A) = \{e \in \mathbb{Z}^m \ s.t. \ \exists s \in \mathbb{Z}_q^n \ where \ A^\top s = e \ (mod) q\},$$
$$\Lambda_q^\perp(A) = \{e \in \mathbb{Z}^m \ s.t. \ Ae = 0 \ (mod) q\},$$
$$\Lambda_q^u(A) = \{e \in \mathbb{Z}^m \ s.t. \ Ae = u \ (mod) q\}.$$

Observe that if $t \in \Lambda_q^u(A)$ then $\Lambda_q^u(A) = \Lambda_q^\perp(A) + t$ and hence $\Lambda_q^u(A)$ is a shift of $\Lambda_q^\perp(A)$.

The Gram-Schmidt Norm of a basis. There exist a probabilistic polynomial-time algorithm to sample an uniform matrix $A \in \mathbb{Z}_q^{n \times m}$ with a basis T_A of $\Lambda_q^\perp(A)$, where T_A has low Gram-Schmidt norm [4, 5]. The following description of the theorem is from Theorem 1 of [1], which itself follows from Theorem 3.2 of [5] by taking $\delta = 1/3$.

Theorem 1. *Let $q \geq 3$ be odd and $m = \lceil 6n \log q \rceil$. There is a probabilistic polynomial-time algorithm **TrapGen**(q, n) that outputs a pair ($A \in \mathbb{Z}_q^{n \times m}$, $S \in \mathbb{Z}^{m \times m}$) such that A is statistically close to a uniform matrix in $\mathbb{Z}_q^{n \times m}$ and S is a basis for $\Lambda_q^\perp(A)$ satisfying*

$$\|\widetilde{S}\| \leq O(\sqrt{n \log q}) \quad and \quad \|S\| \leq O(n \log q)$$

with all but negligible probability in n.

2.3 Learning with Errors

We reduce the security of our constructions to the learning with errors (LWE) problem, which is a hard problem on lattices defined in [17]. Here, we follow the description in [1].

Definition 4. *Consider a prime q, a positive integer n, and a distribution $\mathcal{X}$ over $\mathbb{Z}_q$, all public. An $(\mathbb{Z}_q, n, \mathcal{X})$-LWE problem instance consists of access to an unspecified challenge oracle $\mathcal{O}$, being, either, a noisy pseudo-random sampler $\mathcal{O}_s$ carrying some constant random secret key $s \in \mathbb{Z}_q^n$, or, a truly random sampler $\mathcal{O}_\$$, whose behaviors are respectively as follows:*

- *$\mathcal{O}_s$: outputs samples of the form $(\mathrm{u}_i, \mathrm{v}_i) = (\mathrm{u}_i, \mathrm{u}_i^\top s + x_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where, $s \in \mathbb{Z}_q^n$ is a uniformly distributed persistent value invariant across invocations, $x_i \in \mathbb{Z}_q$ is a fresh sample from $\mathcal{X}$, and u_i is uniform in $\mathbb{Z}_q^n$.*
- *$\mathcal{O}_\$$: outputs truly uniform random samples from $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*

The $(\mathbb{Z}_q, n, \mathcal{X})$-LWE problem allows repeated queries to the challenge oracle $\mathcal{O}$. We say that an algorithm $\mathcal{A}$ decides the $(\mathbb{Z}_q, n, \mathcal{X})$-LWE problem if $|Pr[\mathcal{A}^{\mathcal{O}_s} = 1] - Pr[\mathcal{A}^{\mathcal{O}_\$} = 1]|$ is non-negligible for a random $s \in \mathbb{Z}_q^n$.

The noise distribution $\bar{\Psi}_\alpha$ is defined as follows.

Definition 5. *([1]) Consider a real parameter $\alpha = \alpha(n) \in (0, 1)$ and a prime q. Denote by $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ the group of reals $[0, 1)$ with addition 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 $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor$ the nearest integer to the real $x \in \mathbb{R}$. We denote by $\bar{\Psi}_\alpha$ the discrete distribution over $\mathbb{Z}_q$ of the random variable $\lfloor qX \rceil \bmod q$ where the random variable $X \in \mathbb{T}$ has distribution Ψ_α.*

In [17], the author shows that the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem is hard for certain noise distributions $\bar{\Psi}_\alpha$ by using a quantum reduction.

Theorem 2. *([17]) If there exists an efficient, possibly quantum, algorithm for deciding the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem for $q > 2\sqrt{n}/\alpha$ then there exists an efficient quantum algorithm for approximating the SIVP and GapSVP problems, to within $\tilde{O}(n/\alpha)$ factors in the ℓ_2 norm, in the worst case.*

3 Our Construction based on the ABB-1 Scheme

This construction is based on the lattice IBE in [1] and makes use of their sampling algorithms. In the construction, the authority can generate private keys for all user by using the algorithm **SampleLeft**. In

the simulation, the simulator can use **SampleRight** to respond the private key queries made by the adversary. We refer the reader to previous literature for the concrete definitions of those two algorithms. The inputs and outputs of the algorithms are as follows.

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

- Inputs: A rank n matrix A in $\mathbb{Z}_q^{n\times m}$, a matrix M_1 in $\mathbb{Z}_q^{n\times m_1}$, a "short" basis $T_A \in \mathbb{Z}_q^{m\times m}$ of $\Lambda_q^{\perp}(A)$, a vector $u \in \mathbb{Z}_q^n$ and a gaussian parameter $\sigma > \|\widetilde{T_A}\| \cdot \omega(\sqrt{\log(m+m_1)})$.
- Outputs: Let $F_1 = (A|M_1)$. The algorithm outputs a vector $e \in \Lambda_q^u(F_1)$ (*i.e.*, $F_1 \cdot e = u$).

Algorithm **SampleRight**$(A, B, R, T_B, u, \sigma)$:

- Inputs: A matrix A in $\mathbb{Z}_q^{n\times m}$, a rank n matrix B in $\mathbb{Z}_q^{n\times m}$, a uniform random matrix $R \in \{-1,1\}^{m\times m}$, a basis $T_B \in \mathbb{Z}_q^{m\times m}$ of $\Lambda_q^{\perp}(B)$, a vector $u \in \mathbb{Z}_q^n$ and a gaussian parameter $\sigma > \|\widetilde{T_B}\| \cdot \sqrt{m} \cdot \omega(\log m)$.
- Outputs: Let $F_2 = (A|AR+B)$. The algorithm outputs a vector $e \in \Lambda_q^u(F_2)$ (*i.e.*, $F_2 \cdot e = u$).

The ideas behind the construction are as follows. For each value $v_{i,j}$, where $i \in [N], j \in [N_i]$, we will choose a uniformly random vector $u_{i,j} \in \mathbb{Z}_q^n$. Then, use the encoding function with full-rank differences (FRD) H, described as in [1], to map $u_{i,j}$ to a matrix $H(u_{i,j}) \in \mathbb{Z}_q^{n\times n}$. Thanks to the construction of H, we can compute $\sum_{v_{i,j}\in L} H(u_{i,j})$ for some attribute list L. In addition, notice that $\sum_{v_{i,j}\in L} H(u_{i,j}) \neq \sum_{v_{i,j}\in L'} H(u_{i,j})$ with overwhelming probability for $L \neq L'$ due to all $u_{i,j}$ are uniformly random. Thus, we get a lattice ciphertext policy attribute based encryption that the ciphertext policy is AND-gates on multi-valued attributes.

3.1 Description

Setup(1^λ)**:** Take a security parameter λ as input, and set the parameters q, n, m, σ, α as in [1]. The authority generates a uniformly random matrix $A \in \mathbb{Z}_q^{n\times m}$ with a short basis $T_A \in \mathbb{Z}_q^{m\times m}$ for $\Lambda_q^{\perp}(A)$ by using **TrapGen**(q, n). Choose uniformly random matrices $B, A_1 \in \mathbb{Z}_q^{n\times m}$ and a uniformly random vector $u \in \mathbb{Z}_q^n$. For each $v_{i,j}$, where $i \in [N], j \in [N_i]$, choose a uniformly random vector $u_{i,j} \in \mathbb{Z}_q^n$. Now, set the public parameter PP and the master key MK as:

$$PP = (A, B, A_1, u, \{u_{i,j}\}_{i\in[N], j\in[N_i]}) \quad MK = (T_A).$$

KeyGen(PP, MK, L)**:** Takes the the public parameter PP, the master key MK and attribute list L as inputs, the authority sets $F_L = A|A_1 + (\sum_{v_{i,j}\in L} H(u_{i,j})) \cdot B$, where H is an encoding function with full-rank differences. We assume that $\sum_{v_{i,j}\in L} H(u_{i,j}) \neq \sum_{v_{i,j}\in L'} H(u_{i,j})$ for all $L \neq L'$. Now sample the private key e_L as:

$$e_L \leftarrow \textbf{SampleLeft}(A, A_1 + (\sum_{v_{i,j}\in L} H(u_{i,j})) \cdot B, T_A, u, \sigma).$$

In addition, notice that we have $F_L \cdot e_L = u$.

Encrypt(PP, b, W)**:** Take the public parameter PP, a message bit $b \in \{0,1\}$ and a policy W as inputs, do the following:

- Set $F_W = A|A_1 + (\sum_{v_{i,j}\in W} H(u_{i,j})) \cdot B$.
- Choose a uniformly random $s \in \mathbb{Z}_q^n$ and a uniformly random matrix $R \in \{-1,1\}^{m\times m}$.
- Choose noise vectors $x \in \mathbb{Z}_q$ and $y \in \mathbb{Z}_q^m$ according to the distribution $\bar{\Psi}_\alpha$, and set $z \leftarrow R^\top y \in \mathbb{Z}_q^m$.
- Set $c_0 \leftarrow u^\top s + x + b\lfloor \frac{q}{2} \rfloor$, $c_1 \leftarrow F_W^\top s + \begin{bmatrix} y \\ z \end{bmatrix} \in \mathbb{Z}_q^{2m}$ and the ciphertext $C = (W, c_0, c_1)$.

Decrypt(PP, C, e_L)**:** Let C be encrypted under policy W. If $L \vDash W$, do the following:

- Compute $w \leftarrow c_0 - e_L^\top c_1 \in \mathbb{Z}_q$.
- If $|w - \lfloor \frac{q}{2} \rfloor| < \lfloor \frac{q}{4} \rfloor$ in $\mathbb{Z}$, output 1, otherwise, output 0.

Notice that the above Encrypt and Decrypt algorithms are the same as the construction in the standard model of [1], except that the methods that we compute F_L, F_W and e_L. This construction extends the original lattice identity based encryption to a lattice ABE supporting And-gates on multi-valued attributes.

3.2 Analysis of the Construction

When $L \vDash W$, we have the following equation

$$w = c_0 - e_L^\top c_1 = b\lfloor \frac{q}{2} \rfloor + x - e_L^\top \begin{bmatrix} y \\ z \end{bmatrix}.$$

For more details about the discussion of the error term (it is bounded by $\tilde{O}(q\alpha\sigma m)$) and the concrete setting of the security parameters q, m, α, and σ, we refer the reader to previous literature [1].

Some extensions are as follows. As mentioned in [1, 12], the same ephemeral randomness s can be reused for encrypting multi message bits. This result is also hold true in our setting. In addition, we can improve the above construction to achieve adaptively secure CP-ABE. Choose uniformly random matrices $A_{i,j} \in \mathbb{Z}_q^{n\times m}$ for $i \in [N], j \in [N_i]$ and set F_L as

$$F_L = A|C + \sum_{v_{i,j}\in L} A_{i,j},$$

where A, C and $A_{i,j}$ for $i \in [N], j \in [N_i]$ are matrices in the public parameters. In the adaptive security model, if

we view the original lattice identity based encryption in [1] as a lattice ABE supporting And-gates on two-valued attributes (*i.e.*, 1 or 0), this construction extends it to a lattice ABE that achieves And-gates on multi-valued attributes.

Now we show that the first construction is secure in the standard model under the learning with errors assumption.

Theorem 3. *The advantage of an adversary in the selective game is negligible under the* $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$*-LWE assumption in our above construction.*

Proof. We prove this theorem along the line of the proof of theorem 6 in [1]. Suppose there exists a PPT adversary, $\mathcal{A}$, that can attack our scheme in the Selective model with advantage ϵ. We build a simulator $\mathcal{B}$ that can decide the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem with advantage ϵ. The simulator $\mathcal{B}$ uses the adversary $\mathcal{A}$ to distinguish the LWE oracle $\mathcal{O}$. First $\mathcal{B}$ queries the LWE oracle $\mathcal{O}$ for $m+1$ times and receives fresh pairs $(\mathrm{u}_k, \mathrm{v}_k) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $k \in \{0, 1, 2, \ldots, m\}$, then $\mathcal{B}$ proceeds as follows:

- **Init:** $\mathcal{A}$ announces to $\mathcal{B}$ the challenge access structure $W^* = (W_1^*, W_2^*, \ldots, W_N^*)$.
- **Setup:** $\mathcal{B}$ prepares the public parameters as follows.
  - Set u to be u_0 and construct A by letting the k-th column of A to be u_k for $k = 1, 2, \ldots, m$ from the LWE pairs.
  - $\mathcal{B}$ chooses a uniformly random matrix $R^* \in \{-1, 1\}^{m \times m}$, and let R^* be the random matrix used for generating the challenge ciphertext C^*.
  - Generate a uniformly random matrix B by invoking algorithm $\mathbf{TrapGen}(q, n)$ and retain the basis $T_B \in \mathbb{Z}_q^{m \times m}$ for $\Lambda_q^\perp(B)$.
  - For each $v_{i,j}$, where $i \in [N], j \in [N_i]$, choose a uniformly random vector $u_{i,j} \in \mathbb{Z}_q^n$.
  - Set $A_1 = AR^* - \sum_{v_{i,j} \in W^*} H(u_{i,j}) \cdot B$ and give the parameters $(A, B, A_1, u, \{u_{i,j}\}_{i \in [N], j \in [N_i]})$ to $\mathcal{A}$.

  Notice that these parameters have the correct distributions.
- **Phase 1:** $\mathcal{B}$ can use the trapdoor T_B to respond to private key queries. Assume that $\mathcal{A}$ queries a private key for L, where $L \not\models W^*$. $\mathcal{B}$ first computes $B' = (\sum_{v_{i,j} \in L} H(u_{i,j}) - \sum_{v_{i,j} \in W^*} H(u_{i,j})) \cdot B$ and sets $F_L = A|AR^* + B'$. Then it responds as

$$e_L \leftarrow \mathbf{SampleRight}(A, B', R^*, T_B, u, \sigma).$$

  By construction, we have

$$\begin{aligned} F_L &= A|AR^* + B' \\ &= A|AR^* + (\sum_{v_{i,j} \in L} H(u_{i,j}) - \sum_{v_{i,j} \in W^*} H(u_{i,j})) \cdot B \\ &= A|AR^* - (\sum_{v_{i,j} \in W^*} H(u_{i,j})) \cdot B + (\sum_{v_{i,j} \in L} H(u_{i,j})) \cdot B \\ &= A|A_1 + (\sum_{v_{i,j} \in L} H(u_{i,j})) \cdot B \end{aligned}$$

  Thus, the above values F_L and e_L have the correct forms.
- **Challenge:** $\mathcal{B}$ receives a message bit $b^* \in \{0, 1\}$ from $\mathcal{A}$ and generates the challenge ciphertext that encrypted under the access structure W^* as follows.
  - Set $\mathrm{v}^* = [\mathrm{v}_1, \mathrm{v}_2, \ldots, \mathrm{v}_m]^\top \in \mathbb{Z}_q^m$, $c_0^* = \mathrm{v}_0 + b^* \lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q$, and $c_1^* = \begin{bmatrix} \mathrm{v}^* \\ (R^*)^\top \mathrm{v}^* \end{bmatrix} \in \mathbb{Z}_q^{2m}$, where $\mathrm{v}_0, \mathrm{v}_1, \ldots, \mathrm{v}_m$ from the LWE instance.
  - $\mathcal{B}$ chooses a random bit $r \in \{0, 1\}$. If $r = 0$, return $C^* = (W^*, c_0^*, c_1^*)$ to $\mathcal{A}$ as the challenge ciphertext. If $r = 1$, choose randomly $c_0 \in \mathbb{Z}_q$ and $c_1 \in \mathbb{Z}_q^{2m}$ and return (W^*, c_0, c_1) to $\mathcal{A}$ as the challenge ciphertext.

  It is easy to see that the above challenge ciphertext has the correct distribution. When $\mathcal{O} = \mathcal{O}_s$, by the setting of the public parameters, we have $F_{W^*} = A|AR^*$ and $\mathrm{v}^* = A^\top s + y$ for some random noise vector $y \in \mathbb{Z}_q^m$ with distribution $\bar{\Psi}_\alpha$. Therefore, c_0^* and c_1^* have the correct forms. When $\mathcal{O} = \mathcal{O}_\$$, the challenge ciphertext is uniform in $\mathbb{Z}_q \times \mathbb{Z}_q^{2m}$.
- **Phase 2:** The simulator works as in **Phase 1**.
- **Guess:** $\mathcal{B}$ receives a guess r' for r from $\mathcal{A}$, and outputs r' as the answer to the LWE challenge.

Thus $\mathcal{B}$ has advantage ϵ to decide the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem. This completes the proof. □

4 Our Construction based on the ABB-2 Scheme

This construction uses the technology of lattice basis delegation in fixed dimension and is based on the Hierarchical IBE [2]. The following algorithms are useful for our construction. The reader is referred to [2, 12] for more details about these algorithms.

Algorithm $\mathbf{SamplePre}(A, T_A, u, \sigma)$:

- Inputs: A matrix A in $\mathbb{Z}_q^{n \times m}$ $(q \geq 2, m > n)$, a basis $T_A \in \mathbb{Z}_q^{m \times m}$ of $\Lambda_q^\perp(A)$, a vector $u \in \mathbb{Z}_q^n$ and a gaussian parameter $\sigma > \|\widetilde{T_A}\| \cdot \omega(\sqrt{\log m})$.

- Outputs: A vector $x \in \Lambda_q^u(A)$, which is sampled from a distribution statistically close to $\mathcal{D}_{\Lambda_q^u(A),\sigma}$. The distribution $\mathcal{D}_{\Lambda_q^u(A),\sigma}$ is a discrete Gaussian distribution over $\Lambda_q^u(A)$ with parameter σ.

Let $\mathcal{D}_{m\times m}$ denote the distribution on matrices in $\mathbb{Z}^{m\times m}$ defined as $(\mathcal{D}_{\mathbb{Z}^m,\sigma})^m$ conditioned on the resulting matrix being $\mathbb{Z}_q$-invertible [2]. $\mathcal{D}_{\mathbb{Z}^m,\sigma}$ is the discrete Gaussian distribution over $\mathbb{Z}^m$ with parameter $\sigma = \sqrt{n\log q}\cdot\omega(\sqrt{\log m})$.

Algorithm **SampleR**(1^m):

- The algorithm returns a $\mathbb{Z}_q$-invertible matrix $R \in \mathbb{Z}^{m\times m}$ sampled from $\mathcal{D}_{m\times m}$.

Algorithm **BasisDel**(A, R, T_A, σ):

- Inputs: A rank n matrix A in $\mathbb{Z}_q^{n\times m}$, a $\mathbb{Z}_q$-invertible matrix R, a basis $T_A \in \mathbb{Z}_q^{m\times m}$ of $\Lambda_q^{\perp}(A)$ and a gaussian parameter $\sigma \in \mathbb{R}_{>0}$.
- Outputs: Let $B = AR^{-1} \in \mathbb{Z}_q^{n\times m}$. The algorithm outputs a basis T_B of $\Lambda_q^{\perp}(B)$.

Algorithm **SampleRwithBasis**(A):

- Input: A rank n matrix A in $\mathbb{Z}_q^{n\times m}$.
- Outputs: A matrix $R \in \mathbb{Z}^{m\times m}$, which is sampled from a distribution statistically close to $\mathcal{D}_{m\times m}$, and a basis T_B where $B = AR^{-1} \in \mathbb{Z}_q^{n\times m}$.

Throughout this construction, we fix the order of matrices multiplication in $\prod_{v_{i,j}\in L} R_{i,j}$ for some attribute list L according to the reverse order of L. We will choose a matrix $R_{i,j} \in \mathbb{Z}_q^{m\times m}$ for each value $v_{i,j}$, where $i \in [N], j \in [N_i]$.

4.1 Description

Setup(1^n)**:** Takes a security parameter n as input, and the authority generates a uniformly random matrix $A \in \mathbb{Z}_q^{n\times m}$ with a short basis $T_A \in \mathbb{Z}_q^{m\times m}$ for $\Lambda_q^{\perp}(A)$ by using **TrapGen**(q, n). Choose matrices $R_{i,j} \in \mathbb{Z}_q^{m\times m}$ for $i \in [N], j \in [N_i]$ according to the distribution $\mathcal{D}_{m\times m}$ by using **SampleR**(1^m) and a uniformly random vector $u \in \mathbb{Z}_q^n$. Now, set the public parameter PP and the master key MK as:

$$PP = (A, \{R_{i,j}\}_{i\in[N],j\in[N_i]}, u) \quad MK = (T_A).$$

KeyGen(PP, MK, L)**:** Take the the public parameter PP, the master key MK and a attribute list $L = (L_1, L_2, \ldots, L_N)$ as inputs, where $L_i = v_{i,j}$ be the value for $i \in [N]$ and $j \in N_i$. The authority sets $F_L = A(\prod_{v_{i,j}\in L} R_{i,j})^{-1}$. Now invoke **BasisDel**$(A, \prod_{v_{i,j}\in L} R_{i,j}, T_A, \sigma)$ to generate a basis T_L for lattice $\Lambda_q^{\top}(F_L)$, and then sample the private key e_L as:

$$e_L \leftarrow \textbf{SamplePre}(F_L, T_L, u, \sigma).$$

Encrypt(PP, b, W)**:** Take the public parameter PP, a message bit $b \in \{0,1\}$ and a policy $W = (W_1, \ldots, W_N)$ as inputs, do the following:

- Set $F_W = A(\prod_{v_{i,j}\in W} R_{i,j})^{-1}$.
- Choose a uniformly random $s \in \mathbb{Z}_q^n$.
- Choose noise vectors $x \in \mathbb{Z}_q$ and $y \in \mathbb{Z}_q^m$ according to the distribution $\bar{\Psi}_\alpha$.
- Set $c_0 \leftarrow u^{\top}s + x + b\lfloor\frac{q}{2}\rfloor$, $c_1 \leftarrow F_W^{\top}s + y \in \mathbb{Z}_q^m$ and the ciphertext $C = (W, c_0, c_1)$.

Decrypt(PP, C, e_L)**:** Let C be encrypted under policy W. If $L \models W$, do the following:

- Compute $w \leftarrow c_0 - e_L^{\top}c_1 \in \mathbb{Z}_q$.
- If $|w - \lfloor\frac{q}{2}\rfloor| < \lfloor\frac{q}{4}\rfloor$ in $\mathbb{Z}$, output 1, otherwise, output 0.

If we view the lattice IBE scheme in [2] as a lattice ABE supporting And-gates on two-valued attributes (*i.e.*, 1 or 0), the above construction extends it to a lattice ABE supporting And-gates on multi-valued attributes.

4.2 Analysis of the Construction

When $L \models W$, we have the following equation

$$w = c_0 - e_L^{\top}c_1 = b\lfloor\frac{q}{2}\rfloor + x - e_L^{\top}y.$$

For more details about the discussion of the error term and the concrete setting of the security parameters, we refer the reader to previous literature [2]. Now, we show that the second construction is secure in the standard model under the learning with errors assumption.

Theorem 4. *The advantage of an adversary in the selective game is negligible under the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE assumption in our above construction.*

Proof. We prove this theorem along the line in [2]. Suppose there exists a PPT adversary, $\mathcal{A}$, that can attack our scheme in the Selective model with advantage ϵ. We build a simulator $\mathcal{B}$ that can decide the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem with advantage ϵ. The simulator $\mathcal{B}$ uses the adversary $\mathcal{A}$ to distinguish the LWE oracle $\mathcal{O}$. First $\mathcal{B}$ queries the LWE oracle $\mathcal{O}$ for $m+1$ times and receives fresh pairs $(\mathrm{u}_k, \mathrm{v}_k) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $k = 0, 1, 2, \ldots, m$, then $\mathcal{B}$ proceeds as follows:

- **Init:** $\mathcal{A}$ announces to $\mathcal{B}$ the challenge access structure $W^* = (W_1^*, W_2^*, \ldots, W_N^*)$.
- **Setup:** $\mathcal{B}$ prepares the public parameters as follows.
  - Set u to be u_0 and construct a matrix A_0 by letting the k-th column of A to be u_k for $k = 1, 2, \ldots, m$ from the LWE pairs.

– Let $i \in [N], j \in [N_i]$, for each $v_{i,j} = W_i^*$ (denote such $v_{i,j}$ by v_{i,j_i^*}), sample random matrices R_{i,j_i^*} by using algorithm **SampleR**(1^m). So we get $R_{1,j_1^*}, \ldots, R_{N,j_N^*}$.

– Set $A = A_0 R_{N,j_N^*} \ldots R_{1,j_1^*}$. Let $F_i = A(R_{1,j_1^*})^{-1} \ldots (R_{i-1,j_{i-1}^*})^{-1}$ for $i = 1, \ldots, N$ ($F_1 = A$ for $i = 1$). For each F_i, $\mathcal{B}$ invokes **SampleRwithBasis**(F_i) for $N_i - 1$ times to get matrices $R_{i,j}$ and basis $T_{i,j}$ for $\Lambda_q^{\perp}(F_i(R_{i,j})^{-1})$, where $j \in [N_i], j \neq j_i^*$. Give the parameters $(A, u, \{R_{i,j}\}_{i \in [N], j \in [N_i]})$ to $\mathcal{A}$.

$\mathcal{B}$ retains $T_{i,j}$ for $\Lambda_q^{\perp}(F_i(R_{i,j})^{-1})$, where $i \in [N], j \in [N_i], j \neq j_i^*$. Notice that these parameters have the correct distributions.

- **Phase 1:** $\mathcal{B}$ can use the trapdoor bases $T_{i,j}$ generated in the above stage to respond to private key queries. Assume that $\mathcal{A}$ queries a private key for L, where $L \not\models W^*$. There must exist some i such that $v_{i,j} \in L$ and $v_{i,j} \notin W^*$, and this means that $j \neq j_i^*$. We denote the smallest i by t. Then we have

$$\begin{aligned} F_L &= A(\prod_{v_{i,j} \in L} R_{i,j})^{-1} \\ &= A_0 R_{N,j_N^*} \ldots R_{1,j_1^*} (\prod_{v_{i,j} \in L} R_{i,j})^{-1} \\ &= A_0 R_{N,j_N^*} \ldots R_{t,j_t^*} \cdot (\prod_{v_{i,j} \in L, i \geq t} R_{i,j})^{-1} \\ &= A_0 R_{N,j_N^*} \ldots R_{t,j_t^*} \cdot (R_{t,j})^{-1} \cdot (\prod_{v_{i,j} \in L, i > t} R_{i,j})^{-1} \\ &= F_t \cdot (R_{t,j})^{-1} \cdot (\prod_{v_{i,j} \in L, i > t} R_{i,j})^{-1}. \end{aligned}$$

By construction, $\mathcal{B}$ knows a basis $T_{t,j}$ for $\Lambda_q^{\perp}(F_t(R_{t,j})^{-1})$ where $j \in [N_t], j \neq j_t^*$. Now $\mathcal{B}$ invokes **BasisDel**$(F_t \cdot (R_{t,j})^{-1}, \prod_{v_{i,j} \in L, i > t} R_{i,j}, T_{t,j}, \sigma)$ to generate a basis T_L for lattice $\Lambda_q^{\top}(F_L)$. $\mathcal{B}$ samples the private key e_L as

$$e_L \leftarrow \textbf{SamplePre}(F_L, T_L, u, \sigma),$$

and gives it to $\mathcal{A}$. Notice that the above values F_L and e_L have the correct forms.

- **Challenge:** $\mathcal{B}$ receives a message bit $b^* \in \{0, 1\}$ from $\mathcal{A}$. By construction, we have

$$\begin{aligned} F_{W^*} &= A(\prod_{v_{i,j} \in W^*} R_{i,j})^{-1} \\ &= A_0 R_{N,j_N^*} \ldots R_{1,j_1^*} (\prod_{v_{i,j} \in W^*} R_{i,j})^{-1} \\ &= A_0. \end{aligned}$$

$\mathcal{B}$ generates the challenge ciphertext that encrypted under the access structure W^* as follows.

– Set $\mathrm{v}^* = [\mathrm{v}_1, \mathrm{v}_2, \ldots, \mathrm{v}_m]^{\top} \in \mathbb{Z}_q^m$, $c_0^* = \mathrm{v}_0 + b^* \lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q$, and $c_1^* = \mathrm{v}^*$, where v_k from the LWE instances for $k = 0, 1, \ldots, m$.

– $\mathcal{B}$ chooses a random bit $r \in \{0, 1\}$. If $r = 0$, return $C^* = (W^*, c_0^*, c_1^*)$ to $\mathcal{A}$ as the challenge ciphertext. If $r = 1$, choose randomly $c_0 \in \mathbb{Z}_q$ and $c_1 \in \mathbb{Z}_q^m$ and return (W^*, c_0, c_1) to $\mathcal{A}$ as the challenge ciphertext.

It is easy to see that the above challenge ciphertext has the correct distribution. When $\mathcal{O} = \mathcal{O}_s$, by the setting of the public parameters, we have $F_{W^*} = A_0$ and $\mathrm{v}^* = A_0^{\top} s + y$ for some random noise vector $y \in \mathbb{Z}_q^m$ with distribution $\bar{\Psi}_\alpha$. Therefore, c_0^* and c_1^* have the correct forms. When $\mathcal{O} = \mathcal{O}_\$$, the challenge ciphertext is uniform in $\mathbb{Z}_q \times \mathbb{Z}_q^{2m}$.

- **Phase 2:** The simulator works as in **Phase 1**.

- **Guess:** $\mathcal{B}$ receives a guess r' for r from $\mathcal{A}$, and outputs r' as the answer to the LWE challenge.

Thus $\mathcal{B}$ has advantage ϵ to decide the $(\mathbb{Z}_q, n, \bar{\Psi}_\alpha)$-LWE problem. This completes the proof. □

5 Conclusions

We present two constructions for lattice ciphertext policy attribute based encryption scheme. The ciphertext policy that we achieved is AND-gates on multi-valued attributes. It is the future work for achieving access structure of more complexity.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (No. 61202493). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h) ibe in the standard model," in *Advances in Cryptology - Eurocrypt '10*, pp. 553–572. Springer-Verlag, 2010.

[2] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical ibe," in *Advances in Cryptology - Crypto '10*, pp. 98–115. Springer-Verlag, 2010.

[3] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee. "Fuzzy identity based encryption from lattices,". Cryptology ePrint Archive, http://eprint.iacr.org/2011/414, 2011.

[4] M. Ajtai, "Generating hard instances of the short basis problem," in *Automata, Languages and Programming*, pp. 1–9. Springer-Verlag, 1999.

[5] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," in *26th International Symposium on Theoretical Aspects of Computer Science STACS 2009*, pp. 75–86, 2009.

[6] N. Attrapadung and H. Imai, "Dual-policy attribute based encryption," in *Applied Cryptography and Network Security*, pp. 168–185. Springer-Verlag, 2009.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, pp. 321–334. IEEE, 2007.

[8] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology - Crypto '01*, pp. 213–229. Springer-Verlag, 2001.

[9] X. Boyen, "Attribute-based functional encryption on lattices," in *Theory of Cryptography*, pp. 122–142. Springer-Verlag, 2013.

[10] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Advances in Cryptology - Eurocrypt '10*, pp. 523–552. Springer-Verlag, 2010.

[11] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in *Information Security Practice and Experience*, pp. 13–23. Springer-Verlag, 2009.

[12] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th annual ACM symposium on Theory of computing*, pp. 197–206. ACM, 2008.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98. ACM, 2006.

[14] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology - Eurocrypt '10*, pp. 62–91. Springer-Verlag, 2010.

[15] Q. Li, H. Xiong, F. Zhang, and S. Zeng, "An expressive decentralizing kp-abe scheme with constant-size ciphertext," *International Journal of Network Security*, vol. 15, no. 3, pp. 161–170, 2013.

[16] C. Ling and N. Calvin, "Provably secure ciphertext policy abe," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 456–465. ACM, 2007.

[17] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pp. 84–93. ACM, 2005.

[18] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology - Eurocrypt '05*, pp. 457–473. Springer-Verlag, 2005.

[19] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology - Crypto '84*, pp. 47–53. Springer-Verlag, 1985.

[20] Y. Wang, K. Chen, Y. Long, and Z. Liu, "Accountable authority key policy attribute-based encryption," *Science China Information Sciences*, vol. 55, no. 7, pp. 1631–1638, 2012.

[21] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology - Eurocrypt '05*, pp. 114–127. Springer-Verlag, 2005.

[22] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography- PKC '11*, pp. 53–70. Springer-Verlag, 2011.

[23] J. Zhang, Z. Zhang, and A. Ge, "Ciphertext policy attribute-based encryption from lattices," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 16–17. ACM, 2012.

Yongtao Wang was born in 1980. He received his Ph.D. degree in Computer Science and Engineering from Shanghai Jiao Tong University, Shanghai, China, in 2011. He is currently a Research Assistant at China Information Technology Security Evaluation Center, Beijing, China. His research interests include information security and modern cryptography, etc.