A Ciphertext Policy Attribute-Based Encryption Scheme without Pairings*

Jiang Zhang and Zhenfeng Zhang

State Key Laboratory of Information Security,
Institute of Software, Chinese Academy of Sciences, Beijing, 100190, China
{zhangjiang,zfzhang}@is.iscas.ac.cn

Abstract. Sahai and Waters [34] proposed Attribute-Based Encryption (ABE) as a new paradigm of encryption algorithms that allow the sender to set a policy to describe who can read the secret data. In recent years, lots of attribute-based schemes appeared in literatures, but almost all the schemes, to the best of our knowledge, are constructed from pairings. In this work, we present a ciphertext policy attribute-based encryption (CP-ABE) scheme, which supports and-gates without pairings. Our scheme is defined on q-ary lattices, and has a very strong security proof based on worst-case hardness. More precisely, under the learning with errors (LWE) assumption, our CP-ABE scheme is secure against chosen plaintext attack in the selective access structure model. Though our scheme only encrypts one bit at a time, we point out that it can support multi-bit encryption by using a well-known technique. Besides, our result can be easily extended to ideal lattices for a better efficiency.

1 Introduction

Sahai and Waters [34] introduced the notion of attribute-based encryption as an extension of identity-based encryption (IBE), where users' secret keys are produced by a trust authority according to a set of attributes. In an ABE system, a user's secret keys, and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key.

Goyal, Pandey, Sahai and Waters [14] further extended the idea of ABE and introduced two variants: key policy attribute-based encryption (KP-ABE) and ciphertext policy attribute-based encryption (CP-ABE). In a KP-ABE system, the ciphertext is associated with a set of descriptive attributes, while the private key of a party is associated with an access policy which is defined over a set of attributes and specifies which type of ciphertexts the key can decrypt. A CP-ABE system can be seen as a complementary form to KP-ABE system, where the private keys are associated with a set of attributes, while a policy defined over a

* The work is supported by the National Natural Science Foundation of China under Grant No. 60873261, 61170278, and the National Basic Research Program (973) of China under Grant No. 2007CB311202.

C.-K. Wu, M. Yung, and D. Lin (Eds.): Inscrypt 2011, LNCS 7537, pp. 324–340, 2012.

set of attributes is attached to the ciphertext. A ciphertext can be decrypted by a party if the attributes associated with its private keys satisfy the ciphertext's policy.

Cheung and Newport [9] proposed the first CP-ABE system that supports and-gates, and proved its security under decision bilinear Diffie-Hellman (DBDH) assumption. Since then, there are many attribute-based encryptions that support various access structures. Such as and-gates schemes in [9,27,10], tree-based schemes in [13,19,16], and directly linear secret sharing scheme (LSSS) based constructions in [17,18,36].

All the schemes mentioned above are constructed from pairings, and there are no implications that an (efficient) ABE scheme can be constructed based on other cryptographic assumptions than pairings. Moreover, those pairing related assumptions are known to be vulnerable as we step into a post-quantum era. In contrast, lattice is an ideal choice to construct secure cryptographic schemes according to the following two facts:

- There is no known algorithm that can efficiently solve lattice hard problems even for quantum computers;
- Lattice based cryptographic constructions enjoy several potential advantages: asymptotic efficiency, conceptual simplicity and security proofs based on worst-case hardness.

Unfortunately, there are few attribute-based cryptographic constructions from lattices, though lattice cryptography has gained fruitful results in recent years.

The seminal work of Ajtai [5] brought lattice cryptography into our sight. He gave the first collision-resistant hash function on random lattices in 1996. Later in 2002, Micciancio [25] constructed a hash function on ideal lattices and proved its one-wayness. In 2006, Lyubashevsky and Micciancio [21], Peikert and Rosen [29] independently proved that the hash function in [25] is collision-resistant with some restriction on the domain. As for public encryption setting, in 2005, Regev [31] introduced the learning with error (LWE) problem, and proved that its average-case hardness could be reduced by a quantum algorithm to some standard lattice problems in the worst-case. He also proposed an elegant encryption scheme based on LWE. Later, plenty of constructions based on LWE were proposed (e.g.,[30,32]). In 2009, Peikert [28] gave a classic reduction for LWE problem under an extension hard problem on lattices. In 2008, Gentry, Peikert and Vaikuntanathan [11] gave a famous algorithm that could efficiently sample elements from the distribution (i.e., $D_{\mathbf{\Lambda},s,\mathbf{c}}$, see section 3.1). They also gave a digital signature scheme on lattices which was proved to be secure in the random oracle model. Some other signature schemes on lattices have appeared in literatures (e.g., [22,20,12]). Based on the sample algorithm in [11] and the LWE assumption in [31], many IBE and Hierarchical IBE schemes have been proposed (e.g.,[1,2,8]).

More recently, two schemes [3,4] were posted on eprint.iacr.org. Agrawal et al. [3] constructed a fuzzy identity based encryption from lattices. Their construction employed the technique in [1] together with Shamir secret-sharing scheme. If we consider each identity "bit" in their scheme as an attribute, then we obtain

a KP-ABE that supports threshold gate policy. They also pointed out that it was difficult to generalize their construction to support more expressive policies. In addition, Agrawal, Freeman and Vaikuntanathan constructed a functional encryption for inner product predicates based on the LWE assumption. They utilized the technique in [1], and also presented a new technique that could transform the ciphertext lattice into a lattice that matches the key lattice (while two lattices are already matched once they are generated in [1]). Their scheme can also be viewed as a ABE scheme that supports inner product policy.

Our contribution. In this paper, we investigate ciphertext policy attribute-based encryption (CP-ABE), which supports and-gates on positive and negative attributes. In this setting, each attribute is associated with two types of attributes, namely positive attribute and negative attribute. And if a user has attribute i, we say he has positive attribute i. Otherwise, we say he has negative attribute i. Actually, positive attribute i and negative attribute i are two different attributes, and denoted by i^+ and i^- respectively. Each user in this system has one and only one of the two attributes, since a user either has attribute i or doesn't. For instance, for a real attribute system which has four attributes $\{att_1, att_2, att_3, att_4\}$, we extend these four attributes into $\{att_1^+, att_1^-, att_2^+, att_2^-, att_3^+, att_3^-, att_4^+, att_4^-\}$ in our system. If a user has attributes $\{att_1, att_3\}$ in the real world, we implicitly define his attributes set as $\{att_1^+, att_2^-, att_3^+, att_4^-\}$. Moreover, all access structures are organized by and-gates in this setting. E.g., a user can decrypt a ciphertext if he has all the positive attributes and doesn't have any negative attributes, which are specified in the ciphertext's policy. For instance, a ciphertext encrypted under access structure $W = (att_1^+$ and att_2^- and $att_3^+)$ can only be decrypted by those who have attributes att_1, att_3 and doesn't have attributes att_2, and we don't care about whether he has att_4.

We propose a ciphertext policy attribute-based encryption that supports and-gates on positive and negative attributes. The basic idea of our construction is that, in the positive and negative setting, each user in this system has an "identity" (i.e., the set of his positive and negative attributes), which is unique in the sense of attribute sets, thus we can use this "identity" to do some things as we do in IBE systems. Specifically, we associate each (positive or negative) attribute with a matrix, actually a matrix uniquely defines a lattice by a well-known definition in lattice cryptography [5]. Thus a user's "identity" uniquely defines a set of lattices. When we generate secret keys for a user with attribute set S, we use his lattices set determined by S to share a public vector, which is used for encryption, by utilizing a trapdoor (i.e., short basis) of these lattices, and the secret key for each attribute in S is a short vector in a lattice (strictly, a coset defined by the lattice) determined by the attribute. As two users with different attribute sets have different "identities", they share the same public vector in two different methods (i.e., in two different lattice sets). The security of this method is guaranteed by Inhomogeneous Small Integer Solution (ISIS) problem [26], which was shown to be as hard as some lattice hard problems. For details see section 4.

To the best of our knowledge, our construction is the first CP-ABE scheme without pairings. Though our construction seems to be not much efficient, it gives light to the possibility of constructing attribute schemes under other hard problem assumptions (e.g., lattice problems), instead of the pairing-related assumptions. Our scheme has a very strong security proof based on worst-case hardness. More precisely, under the learning with errors (LWE) assumption, our CP-ABE scheme is secure against chosen plaintext attack in the selective access structure model.

Our basic construction only encrypts one bit at a time, but as we show later, one can obtain a multi-bit encryption with a small ciphertext expansion (respect to the one bit setting) by using a well-known technique [1]. We also point out that our result can be easily extended to ideal lattices for a better efficiency.

2 Preliminaries

2.1 Notation

The set of real numbers (integers) is denoted by $\mathbb{R}$ ($\mathbb{Z}$, resp.). The function log denotes the natural logarithm. Vectors are in column form and denoted by bold lower-case letters (e.g., $\mathbf{x}$). We view a matrix simply as the set of its column vectors and denoted by bold capital letters (e.g., $\mathbf{X}$).

Denote l_2 and l_∞ norm by $\|\cdot\|$ and $\|\cdot\|_\infty$ respectively. Define the norm of a matrix $\mathbf{X}$ as the norm of its longest column (i.e., $\|\mathbf{X}\| = \max_i \|\mathbf{x}_i\|$). If the columns of $\mathbf{X} = \{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$ are linearly independent, let $\widetilde{\mathbf{X}} = \{\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_k\}$ denote the Gram-Schmidt orthogonalization of vectors $\mathbf{x}_1, \ldots, \mathbf{x}_k$ taken in that order. For $\mathbf{X} \in \mathbb{R}^{n \times m}$ and $\mathbf{Y} \in \mathbb{R}^{n \times m'}$, $[\mathbf{X}\|\mathbf{Y}] \in \mathbb{R}^{n \times (m+m')}$ denotes the concatenation of the columns of $\mathbf{X}$ followed by the columns of $\mathbf{Y}$. And for $\mathbf{X} \in \mathbb{R}^{n \times m}$ and $\mathbf{Y} \in \mathbb{R}^{n' \times m}$, $[\mathbf{X}; \mathbf{Y}] \in \mathbb{R}^{(n+n') \times m}$ is the concatenation of the rows of $\mathbf{X}$ followed by the rows of $\mathbf{Y}$. If S is an attribute set and W is an access structure, $S \vdash W$ means that S satisfies W.

The natural security parameter throughout the paper is n, and all other quantities are implicitly functions of n. Let $poly(n)$ denote an unspecified function $f(n) = O(n^c)$ for some constant c. We use standard notation O, ω to classify the growth of functions. If $f(n) = O(g(n) \cdot \log^c n)$, we denote $f(n) = \tilde{O}(g(n))$. We say a function $f(n)$ is negligible if for every $c > 0$, there exists a N such that $f(n) < 1/n^c$ for all $n > N$. We use $negl(n)$ to denote a negligible function of n, and we say a probability is overwhelming if it is $1 - negl(n)$.

2.2 Ciphertext Policy Attribute-Based Encryption

A ciphertext policy attribute-based encryption (CP-ABE) scheme $\mathcal{ABE} = \{$`Setup`, `KeyGen`, `Enc`, `Dec`$\}$ consists of four algorithms:

- `Setup`$(\lambda, \mathcal{R})$. Given a security parameter λ and an attribute set $\mathcal{R}$, the algorithm returns a public key pk and a master key msk. The public key is used for encryption. The master key, held by the central authority, is used to generate users' secret keys.

- $\texttt{KeyGen}(msk, S)$. The algorithm takes as input the master key msk and an attribute set $S \subseteq \mathcal{R}$, returns a secret key sk_S.
- $\texttt{Enc}(pk, W, M)$ Given the public key pk, an access structure W, and a message M, $\texttt{Enc}$ returns the ciphertext C.
- $\texttt{Dec}(sk_S, C)$ The algorithm takes a secret key sk_S and a ciphertext C as input, it first checks whether the attribute set of sk_S satisfies the access structure W in C. If not, the algorithm returns $\perp$. Otherwise, it decrypts C and returns the result.

For correctness, we require that, for any message $M \in \{0,1\}^*$, access structure W, attribute $S \subseteq \mathcal{R}$ that $S \vdash W$, $\texttt{Dec}(\texttt{ENC}(pk, W, M), sk_S) = M$ holds with overwhelming probability.

Here, we review the security model for CP-ABE in [9,15], in which the attacker specifies the challenge access structure before the setup phase. The formal description of this model is given below:

Init. The adversary chooses the challenge access structure W^* and gives it to the challenger.

Setup. The challenger runs the Setup algorithm, gives pk to the adversary and keeps the master key msk secret.

Key Generation Query: The adversary can adaptively make a number of key generation queries on attribute sets S except that he is not allowed to query an attribute set S that satisfies W^*.

Challenge. At some time, the adversary outputs two messages M_0, M_1, and $|M_0| = |M_1|$. The challenger randomly chooses one bit $b \in \{0,1\}$, computes $C^* = \texttt{Enc}(pk, W^*, M_b)$, and returns C^* to the adversary.

Guess. The adversary makes more key generation queries on any attribute set S with a restriction that S doesn't satisfy W^*. Finally, the adversary will output a bit b'.

The advantage of an adversary $\mathcal{A}$ in the above IND-sCPA game is defined as

$$\texttt{Adv}^{\text{ind-scpa}}_{\mathcal{ABE},\mathcal{A}}(\lambda) = |\Pr[b = b'] - \frac{1}{2}|$$

Definition 1. *A CP-ABE scheme $\mathcal{ABE}$ is said to be secure against selective chosen plaintext attack (sCPA) if the advantage $\texttt{Adv}^{ind\text{-}scpa}_{\mathcal{ABE},\mathcal{A}}(\lambda)$ is a negligible function in λ for all polynomial time adversary $\mathcal{A}$.*

3 Lattices

Let $\mathbb{R}^n$ be the n-dimensional Euclidean space. A lattice in $\mathbb{R}^n$ is the set

$$\mathcal{L}(\mathbf{b}_i, \ldots, \mathbf{b}_m) = \left\{ \sum_{i=1}^{m} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}$$

of all integral combinations of m linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{R}^n$. The integers m and n are called the rank and dimension of the lattice, respectively. The sequence of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$ is called a lattice basis and it is conveniently represented as a matrix

$$\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_m] \in \mathbb{R}^{n \times m}.$$

The dual lattice of $\mathbf{\Lambda}$, denoted $\mathbf{\Lambda}^*$, is defined to be

$$\mathbf{\Lambda}^* = \left\{ \mathbf{x} \in \mathbb{R}^n : \ \forall \ \mathbf{v} \in \mathbf{\Lambda}, \ \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z} \right\}$$

Let $\mathcal{B}_m(\mathbf{0}, r) = \{\mathbf{x} \in \mathbb{R}^m : \|\mathbf{x}\| < r\}$ be the m-dimensional open ball of radius r centered in $\mathbf{0}$. For any m-dimensional lattice $\mathbf{\Lambda}$, the ith minimum $\lambda_i(\mathbf{\Lambda})$ is the shortest radius r such that $\mathcal{B}_m(\mathbf{0}, r)$ contains i linearly independent lattice vectors. Formally,

$$\lambda_i(\mathbf{\Lambda}) = \inf\{r : dim(span(\mathbf{\Lambda} \cap \mathcal{B}_m(\mathbf{0}, r))) \geq i\}.$$

For any rank n lattice $\mathbf{\Lambda}$, $\lambda_1(\mathbf{\Lambda}), \ldots, \lambda_n(\mathbf{\Lambda})$ are constants, and $\lambda_1(\mathbf{\Lambda})$ is the length of the shortest vector in $\mathbf{\Lambda}$.

There are some well-known standard hard problems related to λ_i on lattices, and SIVP is one of those problems.

Definition 2 (Shortest Independent Vector Problem, SIVP). *Given a basis* $\mathbf{B}$ *of an* n*-dimensional lattice* $\mathbf{\Lambda} = \mathcal{L}(\mathbf{B})$*, the goal of a* $SIVP_\gamma$ *problem is to find a set of* n *linearly independent lattice vectors* $\mathbf{S} = \{\mathbf{s}_1, \ldots, \mathbf{s}_n\} \subset \mathbf{\Lambda}$*, such that* $\|\mathbf{S}\| \leq \gamma(n) \cdot \lambda_n(\mathbf{\Lambda})$*, where* $\gamma = \gamma(n)$ *is the approximation factor as a function of the dimension.*

Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ for some positive integers n, m, q, we consider two kinds of full-rank m-dimensional integer lattices defined by $\mathbf{A}$:

$$\mathbf{\Lambda}_q^{\perp}(\mathbf{A}) = \left\{ \mathbf{e} \in \mathbb{Z}^m \ \ s.t. \ \mathbf{Ae} = 0 \ (\bmod q) \right\}$$

$$\mathbf{\Lambda}_q(\mathbf{A}) = \left\{ \mathbf{y} \in \mathbb{Z}^m \ \ s.t. \ \exists \mathbf{s} \in \mathbb{Z}^n, \ \mathbf{A^T s} = \mathbf{y} \ (\bmod q) \right\}$$

The two lattices defined above are dual when properly scaled, as $\mathbf{\Lambda}_q^{\perp}(\mathbf{A}) = q\mathbf{\Lambda}_q(\mathbf{A})^*$ and $\mathbf{\Lambda}_q(\mathbf{A}) = q\mathbf{\Lambda}_q^{\perp}(\mathbf{A})^*$.

For any fixed $\mathbf{u}$, define the coset of $\mathbf{\Lambda}_q^{\perp}(\mathbf{A})$ as

$$\mathbf{\Lambda}_q^{\mathbf{u}}(\mathbf{A}) = \left\{ \mathbf{e} \in \mathbb{Z}^m \ \ s.t. \ \mathbf{Ae} = \mathbf{u} \ (\bmod q) \right\}.$$

The following hard-on-average problem was first proposed by Ajtai [5], and then was formalized by Micciancio and Regev in [26].

Definition 3 (Small Integer Solution Problem). *The Small Integer Solution (SIS) problem in l_2 norm is: Given an integer q, a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a real β, find a non-zero integer vector $\boldsymbol{e} \in \mathbb{Z}^m$ such that $\mathbf{Ae} = \mathbf{0}$ (mod q) and $\|\boldsymbol{e}\| \leq \beta$. Equivalently, the SIS problem asks to find a vector $\mathbf{e} \in \boldsymbol{\Lambda}_q^{\perp}(\mathbf{A})\backslash\{\mathbf{0}\}$ with $\|\mathbf{e}\| \leq \beta$.*

Micciancio and Regev also defined a variant problem, called ISIS problem, which is to find a short solution to a random inhomogeneous system.

Definition 4 (Inhomogeneous Small Integer Solution Problem). *The Inhomogeneous Small Integer Solution (ISIS) problem in l_2 norm is: Given an integer q, a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a syndrome $\mathbf{u} \in \mathbb{Z}_q^n$, and a real β, find a non-zero integer vector $\mathbf{e} \in \mathbb{Z}^m$ such that $\mathbf{Ae} = \mathbf{u}$ (mod q) and $\|\mathbf{e}\| \leq \beta$. The average-case problem $ISIS_{q,m,\beta}$ is defined similarly, where $\mathbf{A}$ and $\mathbf{u}$ are uniformly random and independent.*

The SIS and ISIS problems were shown to be as hard as certain worst-case lattice problems in [11].

Proposition 1 ([11]). *For any poly-bounded $m, \beta = poly(n)$ and any prime $q \geq \beta\omega(\sqrt{n\log n})$, the average-case problems $SIS_{q,m,\beta}$ and $ISIS_{q,m,\beta}$ are as hard as approximating the SIVP problem in the worst case to within certain $\gamma = \beta \cdot \widetilde{O}(\sqrt{n})$ factors.*

3.1 Discrete Gaussians

For any $s > 0$, define the Gaussian function on $\boldsymbol{\Lambda} \subset \mathbb{Z}^n$ centered at $\mathbf{c}$ with parameter s:

$$\forall \mathbf{x} \in \boldsymbol{\Lambda},\ \rho_{s,\mathbf{c}}(\mathbf{x}) = \exp\Big(-\pi\frac{\|\mathbf{x}-\mathbf{c}\|^2}{s^2}\Big).$$

Let $\rho_{s,\mathbf{c}}(\boldsymbol{\Lambda}) = \sum_{\mathbf{x}\in\boldsymbol{\Lambda}} \rho_{s,\mathbf{c}}(\mathbf{x})$. Define the discrete Gaussian distribution over $\boldsymbol{\Lambda}$ with center $\mathbf{c}$, and parameter s as:

$$\forall \mathbf{y} \in \boldsymbol{\Lambda}, D_{\boldsymbol{\Lambda},s,c}(\mathbf{y}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{y})}{\rho_{s,\mathbf{c}}(\boldsymbol{\Lambda})}.$$

The subscripts s and $\mathbf{c}$ are taken to be 1 and $\mathbf{0}$ (respectively) when omitted.

Micciancio and Regev [26] proposed a lattice quantity called smoothing parameter:

Definition 5 ([26]). *For any n-dimensional lattice $\boldsymbol{\Lambda}$ and positive real $\epsilon > 0$, the smoothing parameter η_ϵ is the smallest real $s > 0$ such that $\rho_{1/s}(\boldsymbol{\Lambda}^*\backslash\{\mathbf{0}\}) \leq \epsilon$.*

3.2 Learning with Errors

The learning with errors problem on lattices was proposed by Regev [31]. The hardness of the problem can be reduced by a quantum algorithm to some standard lattices problems (i.e., SIVP) in the worst case. For any $\alpha \in \mathbb{R}^+$, Ψ_α is

defined to be the distribution on $\mathbb{T}$ of a normal variable with mean 0 and standard $\alpha/\sqrt{2\pi}$, reduced modulo 1.

$$\forall r \in [0,1),\ \Psi_\alpha(r) := \sum_{k=-\infty}^{\infty} \frac{1}{\alpha} \cdot \exp(-\pi(\frac{r-k}{\alpha})^2).$$

For any probability distribution $\phi : \mathbb{T} \to \mathbb{R}^+$ and some integer $q \geq 1$, the discrete distribution $\bar{\phi}$ over $\mathbb{Z}_q$ is the random variable $\lfloor q \cdot X_\phi \rceil \bmod q$, where X_ϕ has distribution ϕ. By the standard tail inequality: a normal variable with variance σ^2 is within distance $t \cdot \sigma$ of its mean, except with probability at most $\frac{1}{t}\exp(-t^2/2)$. We have that, for any $m = poly(n)$ independent variables $\mathbf{e} = (e_1, \ldots, e_m)$ from $\bar{\Psi}_\alpha$ over $\mathbb{Z}_q$, $\|\mathbf{e}\| \leq \alpha q\sqrt{m}\omega(\sqrt{\log m})$ with overwhelming probability, since each $\|e_i\| \leq \alpha q\omega(\sqrt{\log m})$ holds with probability negligible to 1.

For $q \geq 2$ and some probability distribution χ over $\mathbb{Z}_q$, an integer $n \in \mathbb{Z}^+$ and a vector $\mathbf{s} \in \mathbb{Z}_q^n$, define $A_{\mathbf{s},\chi} \subseteq \mathbb{Z}_q^n \times \mathbb{Z}_q$ as the distribution of variable $(\mathbf{a}, \mathbf{a^T s}+x)$, where $\mathbf{a}$ and x are informally chosen from $\mathbb{Z}_q^n$ and χ respectively, and all operations are performed in $\mathbb{Z}_q$. For any m independent samples $(\mathbf{a}_1, y_1), \ldots, (\mathbf{a}_m, y_m)$ from $A_{\mathbf{s},\chi}$, we simply denote it by $(\mathbf{A}, \mathbf{y}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$, where $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m)$ and $\mathbf{y} = (y_1, \ldots, y_m)^T$.

Learning with Errors (LWE). For an integer $q = q(n)$ and a distribution χ on $\mathbb{Z}_q$, we say that an algorithm solves $\mathrm{LWE}_{q,\chi}$ if, for any $\mathbf{s} \in Z_q^n$, given samples from $\mathrm{A}_{\mathbf{s},\chi}$ it outputs $\mathbf{s}$ with probability exponentially close to 1.

The decisional variant of the LWE problem is to distinguish samples chosen according to $\mathrm{A}_{\mathbf{s},\chi}$ for a uniformly random $\mathbf{s} \in \mathbb{Z}_q^n$ from samples chosen according to the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$. Regev [31] showed that for $q = poly(n)$ prime, LWE and its decisional version are polynomially equivalent. He proved that for certain modulus q and Gaussian error distribution χ, $\mathrm{LWE}_{q,\chi}$ is as hard as solving SIVP problems using a quantum algorithm.

Proposition 2 ([31]). *Let $\alpha = \alpha(n) \in (0,1)$ and let $q = q(n)$ be a prime such that $\alpha \cdot q > 2\sqrt{n}$. If there exists an efficient (possibly quantum) algorithm that solves $LWE_{q,\bar{\Psi}_\alpha}$, then there exists an efficient quantum algorithm for approximating SIVP in the l_2 norm, in the worst case, to within $\tilde{O}(n/\alpha)$ factors.*

3.3 Some Facts

Here, we list several facts about lattices in literatures.

Lemma 1 ([26]). *For any n-dimensional lattice $\mathbf{\Lambda}$, vector $\mathbf{c} \in \mathbb{R}^n$, and reals $0 < \epsilon < 1, s \geq \eta_\epsilon(\mathbf{\Lambda})$, we have*

$$\Pr_{\mathbf{x}\sim D_{\mathbf{\Lambda},s,\mathbf{c}}}[\|\mathbf{x}-\mathbf{c}\| > s\sqrt{n}] \leq \frac{1-\epsilon}{1+\epsilon} \cdot 2^{-n}.$$

For a lattice $\mathbf{\Lambda}$, define the Gram-Schmidt minimum as $\tilde{bl}(\mathbf{\Lambda}) = \min_{\mathbf{B}} \|\tilde{\mathbf{B}}\|$, where the minimum is taken over all (ordered) bases $\mathbf{B}$ of $\mathbf{\Lambda}$.

Lemma 2 ([11]). *For any n-dimensional lattice* $\mathbf{\Lambda}$ *and real* $\epsilon > 0$*, we have* $\eta_\epsilon(\mathbf{\Lambda}) \leq \tilde{bl}(\mathbf{\Lambda}) \cdot \sqrt{(\log(2n(1+1/\epsilon))/\pi}$*. Then for any* $\omega(\sqrt{\log n})$ *function, there is a negligible* $\epsilon(n)$ *for which* $\eta_\epsilon(\mathbf{\Lambda}) \leq \tilde{bl}(\mathbf{\Lambda}) \cdot \omega(\sqrt{\log n})$*.*

Proposition 3 ([11]). *There is a probabilistic polynomial-time algorithm that, given a basis* $\mathbf{B}$ *of an n-dimensional lattice* $\mathbf{\Lambda} = \mathcal{L}(\mathbf{B})$*, a parameter* $s \geq \|\widetilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log n})$*, and a center* $\mathbf{c} \in \mathbb{R}^n$*, outputs a sample from a distribution that is statistically close to* $D_{\mathbf{\Lambda},s,\mathbf{c}}$*.*

We refer to the algorithm of Proposition 3 as $\texttt{SampleGaussian}(\mathbf{B}, s, \mathbf{c})$, which takes a basis $\mathbf{B}$ for a lattice $\mathbf{\Lambda} \subset \mathbb{R}^m$, a positive real $s \geq \|\widetilde{\mathbf{B}}\| \cdot \omega(\sqrt{\log m})$, and a vector $\mathbf{c} \in \mathbb{R}^m$ as input, outputs a random vector $\mathbf{x} \in \mathbf{\Lambda}$ drawn from a distribution statistically close to $D_{\mathbf{\Lambda},s,\mathbf{c}}$.

Proposition 4 ([11]). *Let* n *and* q *be a positive integers with* q *prime, and let* $m \geq 2n \log q$*. Then for all but a* $2q^{-n}$ *fraction of all* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *and for any* $s \geq \omega(\sqrt{\log m})$*, the distribution of the syndrome* $\mathbf{u} = \mathbf{Ae} \mod q$ *is statistically close to uniform over* $\mathbb{Z}_q^n$*, where* $\mathbf{e} \backsim D_{\mathbb{Z}^m,s}$*.*

Gentry, Peikert and Vaikuntanathan [11] showed that, for any $\mathbf{u} \in \mathbb{Z}_q^n$, $\mathbf{t} \in \mathbb{Z}^m$ such that $\mathbf{At} = \mathbf{u} \mod q$, the conditional distribution of $\mathbf{e} \backsim D_{\mathbb{Z}^m,s}$ given $\mathbf{Ae} = \mathbf{u} \mod q$ is exactly $\mathbf{t} + D_{\mathbf{\Lambda}_q^\perp(\mathbf{A}),s,-\mathbf{t}}$. Furthermore, there is an algorithm $\texttt{SamplePre}(\mathbf{A}, \mathbf{T_A}, s, \mathbf{u})$, that takes input a short basis $\mathbf{T_A}$ for $\mathbf{\Lambda}_q^\perp(\mathbf{A})$, a real $s \geq \|\widetilde{\mathbf{T}}_\mathbf{A}\| \cdot \omega(\sqrt{\log m})$, and a vector $\mathbf{u} \in \mathbb{Z}^n$, outputs a vector $\mathbf{e} \backsim D_{\mathbb{Z}^m,s}$ condition on $\mathbf{Ae} = \mathbf{u}$.

Proposition 5 ([6]). *For any* $\delta_0 > 0$*, there is a probabilistic polynomial-time algorithm that, on input a security parameter* n*, an odd prime* q*=poly(*n*), and integer* $m \geq (5 + 3\delta_0)n \log q$*, outputs a statistically* $(mq^{-\delta_0 n/2})$*-close to uniform matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *and a basis* $\mathbf{T_A} \subset \mathbf{\Lambda}_q^\perp(\mathbf{A})$ *such that with overwhelming probability* $\|\mathbf{T_A}\| \leq O(n \log q)$ *and* $\|\widetilde{\mathbf{T}}_\mathbf{A}\| \leq O(\sqrt{n \log q})$*.*

For concreteness, we use $\texttt{TrapGen}(n, m, q)$ to denote the algorithm in Proposition 5. Note that if we let $\delta_0 = \frac{1}{3}$, we can choose $m \geq \lceil 6n \log q \rceil$.

Lemma 3 ([1]). *Let* $\mathbf{e}$ *be some vector in* $\mathbb{Z}^m$ *and let* $\mathbf{y} \leftarrow \bar{\Psi}_\alpha^m$*. Then the quantity* $|\mathbf{e}^T\mathbf{y}|$ *treated as an integer in* $[0, q-1]$ *satisfies*

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

with all but negligible probability in m*. In particularly, if* $x \leftarrow \bar{\Psi}_\alpha$ *is treated as an integer in* $[0, q-1]$ *then* $|x| \leq q\alpha\omega(\sqrt{\log m}) + 1/2$ *with all but negligible probability in* m*.*

For convenience, we give the following lemma, which is implied by Theorem 3.4 in [7].

Lemma 4. *There exists an algorithm that takes* $\mathbf{A}_1 \in \mathbb{Z}_q^{n\times m}, \ldots, \mathbf{A}_k \in \mathbb{Z}_q^{n\times m}$, *a basis* $\mathbf{S}_i$ *of* $\mathbf{\Lambda}_q^{\perp}(\mathbf{A}_i)$, *and a vector* $\mathbf{u} \in \mathbb{Z}_q^n$, *a real* $s \geq \|\tilde{\mathbf{S}}_i\| \cdot \omega(\sqrt{\log km})$ *as input, outputs a vector* $\mathbf{e} \sim D_{\mathbf{\Lambda}_q^{\mathbf{u}}(\mathbf{A}),s}$ *with overwhelming probability, where* $\mathbf{A} = [\mathbf{A}_1\| \ldots \|\mathbf{A}_k]$, *and each* $\mathbf{A}_i$ *is randomly chosen from* $\mathbb{Z}_q^{n\times m}$.

The algorithm first randomly chooses $\mathbf{e}_j$ from $D_{\mathbb{Z}^{m_j},s}$ for all $j \neq i$, then it computes $\mathbf{u}' = \mathbf{u} - \sum_{j\neq i} \mathbf{A}_j\mathbf{e}_j$. Finally, it computes $\mathbf{e}_i \leftarrow \mathtt{SamplePre}(\mathbf{A}_i, \mathbf{S}_i, s, \mathbf{u}')$ and outputs $\mathbf{e} = [\mathbf{e}_1; \ldots; \mathbf{e}_k]$.

For simplicity of notation, we denote the new algorithm by `SamplePre` as before.

4 A CP-ABE Scheme on Lattices

In this section, we present our CP-ABE scheme in which the access structures are and-gates on positive and negative attributes. Basically, each negative attribute is considered as a new attribute [9]. Namely, if a user has attribute set $S \subseteq \mathcal{R}$ in the real system, we consider all of his attributes in S as positive attributes, and the other attributes in $\mathcal{R}\backslash S$ are implicitly considered as his negative ones. Hence, each user in our system actually has $|\mathcal{R}|$ attributes. Without loss of generality, we denote $\mathcal{R} = \{1, \ldots, |\mathcal{R}|\}$.

Our construction is defined below, which is parameterized by modulus q, dimension m, Gaussian parameter s, and α that determines the error distribution χ. Usually, all these parameters are functions of security parameter n, and all of these will be instantiated later. All the additions here are performed in $\mathbb{Z}_q$.

`Setup`$(n, m, q, \mathcal{R})$: Given positive integers n, m, q, and an attribute set $\mathcal{R}$, first compute $(\mathbf{B}_0, \mathbf{T}_{\mathbf{B}_0}) \leftarrow \mathtt{TrapGen}(n, m, q)$. Then for each $i \in \mathcal{R}$, randomly choose $\mathbf{B}_{i^+} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{B}_{i^-} \leftarrow \mathbb{Z}_q^{n\times m}$. Next, randomly choose a vector $\mathbf{u} \leftarrow \mathbb{Z}_q^n$, and set public key $pk = (\mathbf{B}_0, \{\mathbf{B}_{i^+}, \mathbf{B}_{i^-}\}_{i\in\mathcal{R}}, \mathbf{u})$, and master secret key $msk = (pk, \mathbf{T}_{\mathbf{B}_0})$. Finally, return (pk, msk).

`KGen`(msk, S): Given the master secret key msk and a user's attribute set $S \subseteq \mathcal{R}$, for each $i \in \mathcal{R}$, if $i \in S$, define $\tilde{\mathbf{B}}_i = \mathbf{B}_{i^+}$, else define $\tilde{\mathbf{B}}_i = \mathbf{B}_{i^-}$. Then for each $i \in \mathcal{R}$, randomly choose $\mathbf{e}_i \leftarrow D_{\mathbb{Z}^m,s}$, and compute $\mathbf{y} = \mathbf{u} - \sum_{i\in R} \tilde{\mathbf{B}}_i\mathbf{e}_i$. Finally, compute $\mathbf{e}_0 \leftarrow \mathtt{SamplePre}(\mathbf{B}_0, \mathbf{T}_{\mathbf{B}_0}, s, \mathbf{y})$, and return secret key $\mathbf{sk}_S = [\mathbf{e}_0; \ldots; \mathbf{e}_{|\mathcal{R}|}]$.

Observe that, if let $\mathbf{D} = [\mathbf{B}_0\|\tilde{\mathbf{B}}_1\| \ldots \|\tilde{\mathbf{B}}_{|\mathcal{R}|}]$, we have $\mathbf{D} \cdot \mathbf{sk}_S = \mathbf{u}$.

`Enc`(pk, W, M): Given the public key $pk = (\{\mathbf{B}_{i^+}, \mathbf{B}_{i^-}\}_{i\in\mathcal{R}}, \mathbf{u})$, an access structure W, and a message bit $M \in \{0, 1\}$, denote $S^+(S^-)$ as the set of positive (negative) attributes in W, and $S' = S^+ \cup S^-$. Then for each $i \in S'$, if $i \in S^+$, define $\tilde{\mathbf{B}}_i = \mathbf{B}_{i^+}$, else, define $\tilde{\mathbf{B}}_i = \mathbf{B}_{i^-}$. Next, randomly choose $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and compute:

- $z = \mathbf{u}^T\mathbf{s} + x_z + M\lfloor\frac{q}{2}\rfloor$, where $x_z \leftarrow \chi$,
- $\mathbf{c}_0 = \mathbf{B}_0^T\mathbf{s} + \mathbf{x}_0$, where $\mathbf{x}_0 \leftarrow \chi^m$,
- $\mathbf{c}_i = \tilde{\mathbf{B}}_i^T\mathbf{s} + \mathbf{x}_i$ for each $i \in S'$, where $\mathbf{x}_i \leftarrow \chi^m$,
- $\mathbf{c}_{i^+} = \mathbf{B}_{i^+}^T\mathbf{s} + \mathbf{x}_{i^+}$ and $\mathbf{c}_{i^-} = \mathbf{B}_{i^-}^T\mathbf{s} + \mathbf{x}_{i^-}$ for each $i \in \mathcal{R}\backslash S'$, where $\mathbf{x}_{i^+}, \mathbf{x}_{i^-} \leftarrow \chi^m$.

Finally, return ciphertext $C = (W, z, \mathbf{c}_0, \{\mathbf{c}_i\}_{i\in S'}, \{\mathbf{c}_{i^+}, \mathbf{c}_{i^-}\}_{i\in\mathcal{R}\setminus S'})$.

Dec$(C, \mathbf{sk})$: Given the ciphertext C and the secret key $\mathbf{sk} = [\mathbf{e}_0; \ldots; \mathbf{e}_{|\mathcal{R}|}]$, let S be the attribute set associated to $\mathbf{sk}$, if S doesn't satisfy W, then return $\perp$. Otherwise $S \vdash W$. Define $S^+(S^-)$ as the set of positive (negative) attributes in W, and $S' = S^+ \cup S^-$. Obliviously, $S^+ \subset S$ and $S^- \cap S = \emptyset$. Parse C into $(W, z, \mathbf{c}_0, \{\mathbf{c}_i\}_{i\in S'}, \{\mathbf{c}_{i^+}, \mathbf{c}_{i^-}\}_{i\in\mathcal{R}\setminus S'})$. Then let $\mathbf{y}_i = \mathbf{c}_i$ for each $i \in S' \cup \{0\}$, and for each $i \in \mathcal{R}\setminus S'$, if $i \in S$, let $\mathbf{y}_i = \mathbf{c}_{i^+}$, else let $\mathbf{y}_i = \mathbf{c}_{i^-}$. Define $\mathbf{y} = [\mathbf{y}_0; \mathbf{y}_1; \ldots; \mathbf{y}_{|\mathcal{R}|}]$, and compute $a = \mathbf{sk}^T\mathbf{y} = \mathbf{u}^T\mathbf{s} + x'$, $b = z - a = x_z - x' + M\lfloor\frac{q}{2}\rfloor$. Finally, If $|b - \lfloor\frac{q}{2}\rfloor| \leq \lfloor\frac{q}{4}\rfloor$ in $\mathbb{Z}$, return 1, otherwise return 0.

4.1 Parameters and Correctness

Let $\mathbf{D}$ be the matrix determined by the attribute set in $\mathbf{sk}$, thus $\mathbf{D}\cdot\mathbf{sk} = \mathbf{u}$. By the method we choose vector $\mathbf{y}$, we have $\mathbf{y} = \mathbf{D}^T\mathbf{s} + \mathbf{x}_y$, where $\mathbf{s} \in \mathbb{Z}_q^n, \mathbf{x}_y \in \chi^{m(|\mathcal{R}|+1)}$ are chosen in the encryption. Thus, $a = \mathbf{sk}^T\mathbf{y} = \mathbf{sk}^T(\mathbf{D}^T\mathbf{s} + \mathbf{x}_y) = \mathbf{u}^T\mathbf{s} + \mathbf{sk}^T\mathbf{x}_y = \mathbf{u}^T\mathbf{s} + x'$. And if $|x_z - x'| \leq q/5$ holds (with overwhelming probability), it is easy to check that our decryption algorithm always outputs plaintext M correctly.

Now we set the parameters to achieve our goal.

- For algorithm `TrapGen`, we need $m \geq \lceil 6n \log q \rceil$ (i.e., by Proposition 5).
- For the security proof and `SamplePre`, we need $s \geq \|\tilde{\mathbf{T}}_{\mathbf{B}_0}\| \cdot \omega(\sqrt{\log(m(|\mathcal{R}|+1))})$ (i.e., by Lemma 4).
- For the hardness of LWE, we need $\alpha q > 2\sqrt{n}$ (i.e., by Proposition 2).
- For the decryption algorithm works correctly, we need $|x_z - x'| \leq q/5$.

Note that $\|\tilde{\mathbf{T}}_{\mathbf{B}_0}\| \leq O(\sqrt{n \log q})$ by Proposition 5, $\|\mathbf{sk}\| \leq s\sqrt{m(|\mathcal{R}|+1)}$ by Lemma 1, $|x_z| \leq q\alpha\omega(\sqrt{\log m}) + 1/2$ and $|x'| \leq \|\mathbf{sk}\|q\alpha\omega(\sqrt{\log(m(|\mathcal{R}|+1))}) + \|\mathbf{sk}\|\sqrt{m(|\mathcal{R}|+1)}/2$ by Lemma 3. We obtain $|x_z - x'| \leq sq\alpha\sqrt{m(|\mathcal{R}|+1)} \cdot \omega(\sqrt{\log(m(|\mathcal{R}|+1))}) + sm(|\mathcal{R}|+1)$.

To satisfy all the conditions above, we assume δ is real such that $n^\delta > \lceil \log q \rceil$, and set m, s, q, α as below:

$$
\begin{aligned}
m &= 6n^{1+\delta} \\
s &= \sqrt{m}\omega(\sqrt{\log(m(|\mathcal{R}|+1))}) \\
q &= sm(|\mathcal{R}|+1) \cdot w(\sqrt{\log(m(|\mathcal{R}|+1))}) \\
\alpha &= (s\sqrt{m(|\mathcal{R}|+1)} \cdot \omega(\sqrt{\log(m(|\mathcal{R}|+1))}))^{-1}
\end{aligned}
$$

4.2 Security

Theorem 1. *Let m, s, q, α as above, and let $\chi = \bar{\Psi}_\alpha$. Then if $LWE_{q,\chi}$ is hard, our CP-ABE scheme is secure against selective chosen ciphertext attack (sCPA).*

In particularly, if there exists an adversary $\mathcal{A}$ that breaks the sCPA security of our scheme with advantage ϵ, then there exists an algorithm $\mathcal{B}$ solves $LWE_{q,\chi}$ with probability ϵ.

Proof. Suppose there exists a polynomial time adversary $\mathcal{A}$ that breaks the sCPA security of our CP-ABE scheme with advantage ϵ and makes at most q key generation queries. We construct an algorithm $\mathcal{B}$ that solves the LWE problem with probability negligible to ϵ.

Note that algorithm $\mathcal{B}$ has an oracle $\mathcal{O}(\cdot)$, and he wants to decide whether the samples output by $\mathcal{O}(\cdot)$ is from $\mathrm{A}_{\mathbf{s},\chi}$ or uniform. $\mathcal{B}$ runs adversary $\mathcal{A}$ and simulates $\mathcal{A}$'s view in the sCPA security experiment as follows:

Init. Adversary $\mathcal{A}$ chooses a challenge access structure W^* and gives it to $\mathcal{B}$. Let $S^+(S^-)$ be the set of positive (negative) attributes in W^*, and let $S' = S^+ \cup S^-$.

Setup. After receiving W^*, $\mathcal{B}$ compute:

- $\mathcal{B}$ obtains $(\mathbf{B}_0, \mathbf{v}_0) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$ and $(\mathbf{u}, v_u) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from $\mathcal{O}(\cdot)$.
- For each $i \in \mathcal{R}\backslash S'$, $\mathcal{B}$ obtains $(\mathbf{B}_{i^+}, \mathbf{v}_{i^+}), (\mathbf{B}_{i^-}, \mathbf{v}_{i^-}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$ from $\mathcal{O}(\cdot)$.
- For each $i \in S^+$, $\mathcal{B}$ obtains $(\mathbf{B}_{i^+}, \mathbf{v}_{i^+}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$ from $\mathcal{O}(\cdot)$, then compute $(\mathbf{B}_{i^-}, \mathbf{T}_{\mathbf{B}_{i^-}}) \leftarrow \mathtt{TrapGen}(n, m, q)$.
- For each $i \in S^-$, $\mathcal{B}$ obtains $(\mathbf{B}_{i^-}, \mathbf{v}_{i^-}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$ from $\mathcal{O}(\cdot)$, then compute $(\mathbf{B}_{i^+}, \mathbf{T}_{\mathbf{B}_{i^+}}) \leftarrow \mathtt{TrapGen}(n, m, q)$.

Finally, $\mathcal{B}$ sets $pk = (\mathbf{B}_0, \{\mathbf{B}_{i^+}, \mathbf{B}_{i^-}\}_{i\in R}, \mathbf{u})$, and keeps $(\{\mathbf{T}_{\mathbf{B}_{i^-}}, \mathbf{v}_{i^+}\}_{i\in S^+}$, $\{\mathbf{T}_{\mathbf{B}_{i^+}}, \mathbf{v}_{i^-}\}_{i\in S^-}$, $\{\mathbf{v}_{i^+}, \mathbf{v}_{i^-}\}_{i\in\mathcal{R}\backslash S'})$ secret.

Key Generation Queries. After receiving a query with attribute set $S \subseteq \mathcal{R}$. If $S \vdash W^*$, $\mathcal{B}$ simply outputs $\perp$. Otherwise, for each $i \in \mathcal{R}$, if $i \in S$, $\mathcal{B}$ lets $\tilde{\mathbf{B}}_i = \mathbf{B}_{i^+}$, else lets $\tilde{\mathbf{B}}_i = \mathbf{B}_{i^-}$. Since S doesn't satisfy W^*, namely $S^+ \cap S \neq S^+$ or $S^- \cap S \neq \emptyset$,

there must exists a $j \in \mathcal{R}$, such that $\tilde{\mathbf{B}}_j$ is generated by $\mathtt{TrapGen}$. Hence, $\mathcal{B}$ knows its trapdoor $\mathbf{T}_{\tilde{\mathbf{B}}_j}$. Let $\mathbf{D} = [\mathbf{B}_0 \| \tilde{\mathbf{B}}_1 \| \ldots \| \tilde{\mathbf{B}}_n \|]$, $\mathcal{B}$ computes $\mathbf{e}_S \leftarrow \mathtt{SamplePre}(\mathbf{D}, \mathbf{T}_{\tilde{\mathbf{B}}_j}, s, \mathbf{u})$, and returns $sk_S = \mathbf{e}_S$ to $\mathcal{A}$.

Challenge. When $\mathcal{A}$ submits $M_0, M_1 \in \{0,1\}$, $\mathcal{B}$ randomly chooses $b \in \{0,1\}$, and computes $z = v_u + M_b \lfloor \frac{q}{2} \rfloor$ and $\mathbf{c}_0 = \mathbf{v}_0$. For each $i \in S^+$, let $\mathbf{c}_i = \mathbf{v}_{i^+}$. For each $i \in S^-$, let $\mathbf{c}_i = \mathbf{v}_{i^-}$. For each $i \in \mathcal{R}\backslash S'$, let $\mathbf{c}_{i^+} = \mathbf{v}_{i^+}$ and $\mathbf{c}_{i^-} = \mathbf{v}_{i^-}$. Finally, $\mathcal{B}$ returns $C^* = (W, z, \mathbf{c}_0, \{\mathbf{c}_i\}_{i\in S'}, \{\mathbf{c}_{i^+}, \mathbf{c}_{i^-}\}_{i\in\mathcal{R}\backslash S'})$.

$\mathcal{A}$ can make more key generation queries on attribute set S that doesn't satisfy W^*. Eventually, $\mathcal{A}$ outputs a bit b' as a guess for b. if $b' = b$, $\mathcal{B}$ outputs 1, else outputs 0.

Note that $\mathcal{B}$ answers the key generation queries almost the same as the challenger does in the real game by Lemma 4. On one hand, if $\mathcal{O}(\cdot)$ is a LWE oracle for some $\mathbf{s}^*$, C^* is a valid ciphertext, thus the distribution of $\mathcal{A}$'s view is statistically close to that in the real game. On the other hand, if $\mathcal{O}(\cdot)$ is chosen from uniform, then the ciphertext z is uniform on $\mathbb{Z}_q$, thus the probability that $\mathcal{A}$ guesses the right b is exactly $1/2$. So if $\mathcal{A}$ can break our system, $\mathcal{B}$ can break the LWE assumption, which yields our claim.

5 Multi-bit Encryption

Note that, our basic construction only encrypts one bit at a time, but as many other encryption schemes based on LWE (e.g., [11,1]), it is secure to reuse the same random coin $\mathbf{s}$ to encrypt multiple message bits.

Basically, in the ciphertext there is only one element $z \in \mathbb{Z}_q$ that contains the message information (i.e., $z = \mathbf{u}^T\mathbf{s} + x_z + M\lfloor\frac{q}{2}\rfloor$). In order to encrypt N bits message, a matrix $\mathbf{U} = (\mathbf{u}_1, \ldots, \mathbf{u}_N) \in \mathbb{Z}_q^{n\times N}$ is chosen instead of a vector $\mathbf{u} \in \mathbb{Z}_q^n$ in the public key. And for the jth bit of message $(M_1, \ldots, M_N) \in \{0,1\}^N$, compute $z_j = \mathbf{u}_j^T\mathbf{s} + x_{zj} + M_j\lfloor\frac{q}{2}\rfloor$. For a user whose attributes satisfy a ciphertext's policy can decrypt the ciphertext, the key generation has to generate secret keys $sk_1, \ldots, sk_N$ for him, where each sk_j are independently produced as in our basic construction by using $\mathbf{u}_j$ instead of $\mathbf{u}$. For completeness, we present our multi-bit encryption in Table 1.

We claim that the multi-bit encryption is also secure under the LWE assumption. As in the security proof of our basic scheme, $(\mathbf{u}, v_u)$ are drawn from the oracle $\mathcal{O}(\cdot)$. Here, we can simply get a matrix $(\mathbf{U}, \mathbf{v}_U) \in \mathbb{Z}_q^{n\times N} \times \mathbb{Z}_q^N$ by independently drawing from the same oracle N times, and set $z_j = v_j + M_j\lfloor\frac{q}{2}\rfloor$ in the challenge ciphertext. Thus, we can simulate the security experiment perfectly as in the one bit setting.

Note that, the total ciphertext with this technique is 1 element of $\mathbb{Z}_q$ for each bit of messages, plus at least $m|\mathcal{R}|$ elements of $\mathbb{Z}_q$ regardless of the message length. Thus the ciphertext size is at least $N + m|\mathcal{R}|$ (at most $N + 2m|\mathcal{R}|$) elements of $\mathbb{Z}_q$.

6 On Ideal Lattices

In 2002, Micciancio constructed a hash function [25] based on a kind of special structure lattices which called cyclic lattices or ideal lattices. Since then, many works on ideal lattices have appeared (e.g., [23,33,24]). Usually, the schemes based on ideal lattices have asymptotical computation efficiency and require small storage. Using the known results showed below with some more subtle considerations, our result can be extended to the ideal lattices with a shorter key and ciphertext size.

Stehlé, Steinfeld, Tanaka and Xagawa [35] constructed an efficient public key encryption algorithm on ideal lattices. In their work, they gave an algorithm `TrapGen`, which can be considered as similar version of the one in Proposition 5 in the ideal lattice setting. Namely, the algorithm outputs a random vector $\mathbf{g} \in (\mathbb{Z}_q[x]/f)^m$, and a short basis for the lattice $rot_f(\mathbf{g})^\perp$, where f is a degree n polynomial $f \in \mathbb{Z}[x]$ and $rot_f(\mathbf{g})^\perp = \{\mathbf{b} \in (\mathbb{Z}[x]/f)^m | \langle \mathbf{b}, \mathbf{g}\rangle = 0 \mod q\}$. Recently, Lyubashevsky, Peikert and Regev [24] introduced Ring-LWE and gave a similar quantum reduction as for the classic LWE problem. They also showed that computational Ring-LWE can be reduced to decisional Ring-LWE.

Combining the above two facts and the results in Proposition 3, we can obtain a secure CP-ABE scheme on ideal lattices. For more details, please refer to [35,24].

Table 1. Multi-bit Encryption

$\texttt{Setup}(n, m, q, \mathcal{R})$	$(\mathbf{B}_0, \mathbf{T}_{\mathbf{B}_0}) \leftarrow \texttt{TrapGen}(n, m, q)$; Choose $\mathbf{U} = (\mathbf{u}_1, \ldots, \mathbf{u}_N) \leftarrow \mathbb{Z}_q^{n \times N}$; For each $i \in \mathcal{R}$, choose $\mathbf{B}_{i^+} \leftarrow \mathbb{Z}_q^{n \times m}$ and $\mathbf{B}_{i^-} \leftarrow \mathbb{Z}_q^{n \times m}$; $pk = (\{\mathbf{B}_{i^+}, \mathbf{B}_{i^-}\}_{i \in \mathcal{R}}, \mathbf{U})$, $msk = (pk, \mathbf{T}_{\mathbf{B}_0})$; Return (pk, msk).
$\texttt{KGen}(msk, S)$	For each $i \in \mathcal{R}$, if $i \in S$, $\tilde{\mathbf{B}}_i = \mathbf{B}_i^+$, else $\tilde{\mathbf{B}}_i = \mathbf{B}_i^-$; For each $j \in \{1, \ldots, N\}$ and $i \in \mathcal{R}$, choose $\mathbf{e}_{j,i} \leftarrow D_{\mathbb{Z}^m, s}$; Compute $\mathbf{y}_j = \mathbf{u}_j - \sum_{i \in \mathcal{R}} \tilde{\mathbf{B}}_i \mathbf{e}_{j,i}$, $\mathbf{e}_{j,0} \leftarrow \texttt{SamplePre}(\mathbf{B}_0, \mathbf{T}_{\mathbf{B}_0}, s, \mathbf{y}_j)$; Set $\mathbf{sk}_j = [\mathbf{e}_{j,0}; \ldots; \mathbf{e}_{j,\lvert\mathcal{R}\rvert}]$; Return $\mathbf{sk}_S = (\mathbf{sk}_0, \ldots, \mathbf{sk}_N)$.

$\texttt{Enc}(pk, W, M)$	// Denote $S^+(S^-)$ be the set of positive (negative) attributes in W.
	// Denote $S' = S^+ \cup S^-$ and $\bar{S}' = \mathcal{R} \backslash S'$.
	// $M = \{M_1, \ldots, M_N\} \in \{0,1\}^N$.
	Choose $\mathbf{s} \leftarrow \mathbb{Z}_q^n$;
	For each $j \in \{1, \ldots, N\}$, compute $z_j = \mathbf{u}_j^T \mathbf{s} + x_{zj} + M_j \lfloor \frac{q}{2} \rfloor$,
	where $x_{zj} \leftarrow \chi$;
	For each $i \in S^+$, compute $\mathbf{c}_i = \mathbf{B}_{i^+}{}^T \mathbf{s} + \mathbf{x}_{i^+}$, where $\mathbf{x}_{i^+} \leftarrow \chi^m$;
	For each $i \in S^-$, compute $\mathbf{c}_i = \mathbf{B}_{i^-}{}^T \mathbf{s} + \mathbf{x}_{i^-}$, where $\mathbf{x}_{i^-} \leftarrow \chi^m$;
	For each $i \in \bar{S}'$, compute $\mathbf{c}_{i^+} = \mathbf{B}_{i^+}^T \mathbf{s} + \mathbf{x}_{i^+}$ and
	$\mathbf{c}_{i^-} = \mathbf{B}_{i^-}^T \mathbf{s} + \mathbf{x}_{i^-}$, where $\mathbf{x}_{i^+}, \mathbf{x}_{i^-} \leftarrow \chi^m$;
	Finally, compute $\mathbf{c}_0 = \mathbf{B}_0^T \mathbf{s} + \mathbf{x}_0$, where $\mathbf{x}_0 \leftarrow \chi^m$;
	Return $C = (W, \{z_j\}_{j \in \{1,\ldots,N\}}, \mathbf{c}_0, \{\mathbf{c}_i\}_{i \in S'}, \{\mathbf{c}_{i^+}, \mathbf{c}_{i^-}\}_{i \in \bar{S}'})$.

$\texttt{Dec}(C, sk)$	// Denote S be the attribute set associated to sk.
	// Denote W be the access structure in C.
	// Denote $S^+(S^-)$ as the set of positive (negative) attributes in W.
	// Denote $S' = S^+ \cup S^-$ and $\bar{S}' = \mathcal{R} \backslash S'$.
	If S doesn't satisfy W, return $\perp$.
	Parse C into $(W, \{z_j\}_{j \in \{1,\ldots,N\}}, \mathbf{c}_0, \{\mathbf{c}_i\}_{i \in S'}, \{\mathbf{c}_{i^+}, \mathbf{c}_{i^-}\}_{i \in \bar{S}'})$;
	Parse $\mathbf{sk}$ into $(\mathbf{sk}_0; \ldots; \mathbf{sk}_N)$;
	For each $i \in S'$, let $\mathbf{y}_i = \mathbf{c}_i$;
	For each $i \in \bar{S}'$, if $i \in S$, let $\mathbf{y}_i = \mathbf{c}_{i^+}$, else $\mathbf{y}_i = \mathbf{c}_{i^-}$;
	Let $\mathbf{y} = [\mathbf{c}_0; \mathbf{y}_1; \ldots; \mathbf{y}_{\lvert\mathcal{R}\rvert}]$;
	For each $j \in \{1, \ldots, N\}$, compute $a_j = \mathbf{sk}_j^T \mathbf{y}, b_j = z_j - a_j$;
	If $\lvert b_j - \lfloor \frac{q}{2} \rfloor \rvert \leq \lfloor \frac{q}{4} \rfloor$ in $\mathbb{Z}$, let $M_j = 1$, else $M_j = 0$;
	Return $M = \{M_0, \ldots, M_N\}$.

7 Conclusion

In this paper, a selective secure ciphertext policy attribute-based encryption (CP-ABE) without pairings is proposed. To the best of our knowledge, it is the first CP-ABE scheme from lattices. The security of the proposed scheme is proved in standard model under the LWE assumption. Our constructions only support and-gate access policy, and it remains an open problem to obtain a CP-ABE scheme that can support more general access structure from lattices.

Acknowledgments. We thank Yanfei Guo, Wenhao Wang, Xiang Xie, Rui Zhang, and the anonymous reviewers for their helpful comments and suggestions.

References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient Lattice (H)IBE in the Standard Model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010)
2. Agrawal, S., Boneh, D., Boyen, X.: Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 98–115. Springer, Heidelberg (2010)
3. Agrawal, S., Boyen, X., Vaikuntanathan, V., Voulgaris, P., Wee, H.: Fuzzy identity based encryption from lattices. Cryptology ePrint Archive, Report 2011/414 (2011), `http://eprint.iacr.org/`
4. Agrawal, S., Freeman, D.M., Vaikuntanathan, V.: Functional encryption for inner product predicates from learning with errors. Cryptology ePrint Archive, Report 2011/410 (2011), `http://eprint.iacr.org/`
5. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC 1996, pp. 99–108. ACM, New York (1996)
6. Alwen, J., Peikert, C.: Generating shorter bases for hard random lattices. In: STACS, pp. 75–86 (2009)
7. Cash, D., Hofheinz, D., Kiltz, E.: How to delegate a lattice basis. Cryptology ePrint Archive, Report 2009/351 (2009), `http://eprint.iacr.org/`
8. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai Trees, or How to Delegate a Lattice Basis. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 523–552. Springer, Heidelberg (2010)
9. Cheung, L., Newport, C.: Provably secure ciphertext policy ABE. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 456–465. ACM, New York (2007)
10. Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M.: A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 13–23. Springer, Heidelberg (2009)
11. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008, pp. 197–206. ACM, New York (2008)
12. Dov Gordon, S., Katz, J., Vaikuntanathan, V.: A Group Signature Scheme from Lattice Assumptions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 395–412. Springer, Heidelberg (2010)
13. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded Ciphertext Policy Attribute Based Encryption. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 579–591. Springer, Heidelberg (2008)
14. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, pp. 89–98. ACM, New York (2006)
15. Herranz, J., Laguillaumie, F., Ràfols, C.: Constant Size Ciphertexts in Threshold Attribute-Based Encryption. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 19–34. Springer, Heidelberg (2010)
16. Ibraimi, L., Tang, Q., Hartel, P., Jonker, W.: Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 1–12. Springer, Heidelberg (2009)

17. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010)
18. Lewko, A., Waters, B.: Decentralizing Attribute-Based Encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011)
19. Liang, X., Cao, Z., Lin, H., Xing, D.: Provably secure and efficient bounded ciphertext policy attribute based encryption. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ASIACCS 2009, pp. 343–352. ACM, New York (2009)
20. Lyubashevsky, V.: Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 598–616. Springer, Heidelberg (2009)
21. Lyubashevsky, V., Micciancio, D.: Generalized Compact Knapsacks Are Collision Resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006, Part II. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (2006)
22. Lyubashevsky, V., Micciancio, D.: Asymptotically Efficient Lattice-Based Digital Signatures. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 37–54. Springer, Heidelberg (2008)
23. Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFT: A Modest Proposal for FFT Hashing. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 54–72. Springer, Heidelberg (2008)
24. Lyubashevsky, V., Peikert, C., Regev, O.: On Ideal Lattices and Learning with Errors over Rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010)
25. Micciancio, D.: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In: Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pp. 356–365 (2002)
26. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. SIAM J. Comput. 37, 267–302 (2007)
27. Nishide, T., Yoneyama, K., Ohta, K.: Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures. In: Bellovin, S.M., Gennaro, R., Keromytis, A., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 111–129. Springer, Heidelberg (2008)
28. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, pp. 333–342. ACM, New York (2009)
29. Peikert, C., Rosen, A.: Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 145–166. Springer, Heidelberg (2006)
30. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008, pp. 187–196. ACM, New York (2008)
31. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, STOC 2005, pp. 84–93. ACM, New York (2005)
32. Rosen, A., Segev, G.: Chosen-Ciphertext Security via Correlated Products. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 419–436. Springer, Heidelberg (2009)

33. Rückert, M.: Lattice-Based Blind Signatures. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 413–430. Springer, Heidelberg (2010)
34. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
35. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient Public Key Encryption Based on Ideal Lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 617–635. Springer, Heidelberg (2009)
36. Waters, B.: Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011)