Ad Hoc & Sensor Wireless Networks, Vol. 37, pp. 117–143
Reprints available directly from the publisher
Photocopying permitted by license only

A Multi-Authority Key-Policy ABE Scheme from Lattices in Mobile Ad Hoc Networks

LIHUA LIU[1,2,*], SHANGPING WANG[1] AND QIAO YAN[3]

[1]*Shaanxi Key Laboratory for Network Computing and Security Technology, Xi'an University of Technology, Xi'an, 710054, China*
[2]*School of Mathematics and Computer Science, Shaanxi SCI-TECH University, Shaanxi, Hanzhong 723001, China*
[3]*College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, Guangdong 518060 China)*

Received: January 4, 2017. Accepted: May 10, 2017.

Compared with traditional wired networks, due to the lack of a centralized infrastructure and cooperative algorithm, the security of mobile ad hoc networks (MANETs) is faced with great challenges. Generally, identity-based cryptography is used to build scalable secure systems in MANETs. But in traditional identity-based cryptography protocol, security certificate depends on a trusted third-party authority. The center authority often bears a heavier burden and a bigger risk in a single-authority public-key encryption scheme. Attribute-based encryption (ABE) is a type of public-key encryption with fine-grained access control, which can preferably support the distributed environment in MANETs. Aiming to solve the security of MANETs, a multi-authority key-policy ABE scheme is proposed in this paper, which is constructed from lattices. Lattice-based cryptography has the property of resistance quantum attack. Therefore, a multi-authority key-policy ABE system from lattices may be more secure in the post quantum era than a single-authority ABE system on bilinear mapping.

In new scheme, every attribute has its own authority, and the private key of each attribute under an LSSS access policy is generated by its own authority alone. The new scheme has the advantage of fine-grained access control, and also can support multi-authority attribute management. So it facilitates the practical private key management in MANETs. The security of the new scheme is proved in the selective-attribute attack model under learning with errors (LWE) assumption, and the security parameter selecting is discussed in detail.

*Corresponding author: QiaoYan, College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, Guangdong, China. yanq@szu.edu.cn.

Keywords: Mobile Ad Hoc Networks (MANETs); Attribute-based Encryption (ABE); Lattices

1 INTRODUCTION

Mobile Ad-hoc Networks (MANETs) have been widely concern in military communications, disaster relief, business and other fields, relying on its self-organizing, mobility and anti-destroying ability. The expansion of application fields must be promoted its safety requirements. Due to the lack of a centralized infrastructure, the traditional symmetric cryptography is not applicable in MANETs. Especially, in security-sensitive environments such as military and commercial applications, the security services in MANETs are faced with grand challenges [1].

The limitations of symmetric cryptography have triggered the research on public key solutions in MANETs. Identity (ID)-based cryptography, as a typical public key encryption technology, is used to building scalable secure systems in MANETs [2-3]. But in traditional ID-based cryptography, security mechanism depends on a trusted third-party authority (the Certificate Authority, CA).The security of CA has become the core of the whole network security. The CA often bears a heavier burden and a bigger risk in a single-authority public-key encryption scheme. Since maintaining a secure central server is a difficult problem incompletely distributed environment, threshold cryptography [3] was introduced into MANETs, which can support the distributed CA. A threshold secret sharing scheme allows multiple network nodes to share a system master key and collaboratively issue private key for other nodes. By using (k, n) threshold mechanism, distributed CA in MANETs could be realized effectively. Therefore, combining ID-based cryptography with threshold mechanism is a better way to satisfy the demand of security and distribution in MANETs.

Attribute-based encryption (ABE), as an extension of ID-based encryption, is with a fine-grained access control, which can flexible realize user access permissions in cryptography protocol. In ABE system, identity is a series of descriptive attributes, and system access permission is implemented by any monotone access policy based on AND-OR-gate. A special user can decrypt the cipher text only if the user's attributes satisfy access policy.

The advantage of the ABE system is very applicable to the distributed environment, relying on flexible date access policy on one-to-many encryption scene. However, the most of existing ABE schemes have been designed with single-authority. Attributes of user were managed by the single-authority, which would inevitably increase its workload and reduce its efficiency. For this reason, a multi-authority ABE scheme [4] was proposed by Chase in 2009, in which a trusted central authority supervised multiple sub-attribute authority. Every sub-attribute authority was responsible for issuing

its private key sand maintaining its attribute respectively. Recently, identity-based cryptology has been closely considered for strengthening the security of MANETs.

On the other hand, most of the ABE schemes were based on bilinear mapping technology. Regrettably, it was proven that bilinear mapping technology is not safe under quantum attack in 1997[5]. On this account, the progress of ABE was constrained in post-quantum era. Lattice-based cryptography seems to be the most promising candidate for post-quantum cryptography, so far there is no viable quantum algorithm to solve difficulty lattice problems. Lattice-based cryptography has simply operation and can provide higher security than the traditional public-key cryptography. Therefore, it is attractive for constructing the new ABE scheme form lattices, which seems to support more security services in MANETs.

Related Works: MANETs are a kind of wireless ad hoc network which strongly depend on wireless communication technologies, Wireless communication technologies have made great progress in recent years [6-13]. With the network migrating to cloud computing environments, the rate of network attacks is growing substantially [14-15].

Attribute-based encryption (ABE) [16-20] with fine-grained access control is widely used in public-key cryptography. ABE is an extension of identity-based access control. It can be extended into the attribute signature [21,22], attribute security protocols [23,24] and other research field [25,26]. Compared with the traditional cryptography, ABE seems to have more flexible logic relationship, as the attribute management could extend "one-to-one model" to "one-to-many model". And encryption policy of ABE can support complex access structures, such as threshold, the Boolean expression and so on.

In 2005, Sahai et al. [16] firstly introduced the notion of ABE at EUROCRYPT, as an extension of identity-based encryption, in which user credentials is described assets of attribute and the predicate is described as a formula about these attributes. Subsequently, in 2006, Goyal et al. [17] further clarified the notion of ABE. They proposed two complementary forms of ABE: Key-policy ABE(KP-ABE) and Cipher text-policy ABE(CP-ABE). They developed a Key-policy ABE for fine-grained sharing of encrypted data. In their cryptosystem, cipher text is labeled with sets of attribute and private keys are associated with access structures that control which cipher text a user is able to decrypt. In 2007, Boneh et al.[18] presented a CP-ABE, which could be secure against collusion attacks. Latterly, Waters [19] presented a new scheme for CP-ABE under concrete and non-interactive cryptographic assumptions in the standard model. In order to describe more flexible cipher text protection strategy, and express more complex logic relationships, the researchers proposed the access tree and some other complex access structure in the encryption scheme, and to achieve better results in literature [20].

However, the above encryption schemes are mainly based on bilinear pairing technology with the bilinear Diffie-Hellman assumption. The main drawbacks of these schemes are vulnerable to quantum attacks.

Currently, lattice-based cryptography is considered to be the most promising candidate for post-quantum cryptography, so far there is no viable quantum algorithm to solve difficulty lattice problems. Meanwhile, lattice-based cryptography has simply operation and provides higher security more than the traditional public-key cryptographic technology.

In 1996, Ajtai [27] firstly introduced the lattice problem to the field of cryptography applications, in which he discovered some connections between the worst-case complexity and average-case complexityof some lattice problems. Based on these results, Ajtai and Dwork [28] constructed a public-key cryptosystem, and its security could be proven using only the worst-case hardness of a certain version of SVP. Thereafter, until 2008, Gentry et al.[29] constructed a variety of "trapdoor" cryptographic tool assuming the worst-case hardness of standard lattice problems, and they applied it to digital signature schemes and identity-based encryption. Subsequently, the result was further optimized by Alwen and Peikert [30]. In 2012, Micciancio et al. [31,32] proposed new methods for generating and using "strong trapdoors" in cryptographic lattices, which are asymptotically optimal with very small hidden constants. The method was mainly used to generate one-way trapdoor function with learning with error (LWE) [33,34] hardness assumption. In the same year, Agrawal et al.[35] constructed "fuzzy" identity-based encryption from the hardness of the standard LWE problem, and the CPA and CCA secure variants of their construction was given. Zhang et al.[36] presented cipher text policy attribute based encryption from lattices. In 2013, Boyen [37] proposed an efficient key-policy ABE scheme on lattice. He introduced a broad lattice manipulation technique for expressive cryptography, and realized functional encryption with access structures on post-quantum hardness assumptions.

Recently, in 2014, Han et al.[42] proposed a general transformation from ABE to attribute-based encryption with keyword search and a concrete attribute private key-policy ABE scheme. Zhao et al.[43] proposed a new ABE scheme for circuits on lattice. Shraddha et al. [44] gave an enhancing flexibility CP-ABE scheme with multiple mediators. In 2016, Li et al.[45] constructed a concrete KP-ABE outsourcing scheme. Karati et al. [46] proposed a threshold-based ABE scheme without bilinear map and pointed out the new scheme was much more efficient and flexible others.

Our Contributions: Aiming to the distributed environment of mobile ad hoc networks, a multi-authority attribute-based encryption scheme with key-policy represented by LSSS from lattices is proposed. In the new scheme an attribute can have its own authority, and the private key of each attribute under an access policy is generated a lonely by its own attribute

authority, the private key is issued by its attribute authority. The new scheme is more practical for attribute management than the existing ABE scheme, especially for attributes belong to different fields. For example, an identity attribute is usually managed by public security department, while a professional title attribute may be managed by a company or university, etc. So in practice, let different authority to manage its attribute key is more reasonable, and our new scheme is exactly suitable for distributed environment in MANETs.

The new scheme can be applied to multi-user system, in which different user has multiple attributes, and different attribute is managed by its own authority, such as "personal medical electronic file system", "the sharing of company documents", and so on.

Organization: The rest of this paper is organized as follows. In section 2 we give the algorithmic definition for the Key-Policy encryption scheme. In section 3 we describe the new scheme. The correctness and security of our construction are given in section 4. Finally, we conclude the paper in section 5.

2 PRELIMINARIES

2.1 Notation

By convention, $\mathbb{Z}$ denote the set of the integers, and $\mathbb{R}$ denote the set of real numbers. For any integer q, $\mathbb{Z}_q^{n\times m}$ denote a $n \times m$ matrix with entries in $\mathbb{Z}_q$, $[n]$ denote the set of positive integers $\{1,2,...,n\}$, and $\Lambda \in \mathbb{R}^m$ denote a m-dimensional lattice. Vectors are specified to be in column form and be denoted by bold lower-case letters, e.g. $\mathbf{X}$. The i-th element of vector $\mathbf{X}$ is defined as x_i. Similarly, denote matrices as bold capital letters, e.g. $\mathbf{M}$, and the i-th vector of a matrix $\mathbf{M}$ is defined as $\mathbf{M}_i$. The norm of a matrix $\mathbf{M}$ is defined as $\|\mathbf{M}\|_2$, the Gram-Schmidt orthogonal basis of $\mathbf{M}$ is defined as $\mathbf{M}$.

2.2 Key-Policy Attribute-based Encryption

2.2.1 Algorithms Definition

Here we give a new definition of the key-policy ABE, which is suitable for our purpose, and is based on the frame work of Goyal et al.[7].

A key-policy attribute-based encryption scheme consists of the following four PPT algorithms:

KP - ABE.Setup$(\lambda) \rightarrow (Pub, Msk)$: The system setup algorithm takes a security parameter λ as input. It outputs the public parameters *Pub* and the corresponding master key *Msk*.

KP - ABE.Extract$(Pub, \mathbf{B}_{\rho(i)}, (\mathbf{M}, \rho)) \rightarrow Key_{\rho(i)}$: The key extraction algorithm takes as input the public parameters *Pub*, the master key *Msk*, and an access policy ($\mathbf{M}$, ρ), where *Pub* and $\mathbf{B}_{\rho(i)}$ is corresponding to the

attribute$\rho(i)$ on the policy(**M**, ρ). It outputs decryption keys $Key_{\rho(i)}$ of each attribute $\rho(i)$ on the access policy (**M**, ρ).

KP - ABE.Encrypt$(Msg, Attrib, Pub) \rightarrow C_{tx}$: The encryption algorithm takes as input a message bit $Msg \in \{0,1\}$, the public parameters *Pub*, and a set of attributes *Attrib*. It outputs the cipher text C_{tx}.

KP - ABE.Decrypt$(Pub, Key, C_{tx}) \rightarrow b$:The decryption algorithm takes as input the public parameters *Pub*, the decryption keys *Key*, and the cipher text C_{tx}, where *Key* is a set of $Key_{\rho(i)}$ when the attribute $\rho(i)$ belonging to *Attrib* (by use to create C_{tx}).It outputs the bit *b* when the set of attribute *Attrib* satisfy the access policy (**M**, ρ). Otherwise, decryption fails.

Definition 1. *A KP-ABE scheme is said to be correct, if all attribute subsets Attrib* satisfy access policy* (**M**, ρ) *(i.e. Attrib* is authorized), it is true for Decrypt*(*Pub, Key,* C_{tx})=*Msg*, *when any pair* (*Pub, Msk*) *is generated by Setup*(λ)*, and any the decryption key* $Key_{\rho(i)}$ *is outputted from Extract*(*Pub,* $B_{\rho(i)}$, (**M**, ρ)) *and any cipher text* C_{tx} *is outputted from Encrypt*(*Msg, Attrib, Pub*).

2.2.2 Selective Security Definition

We define the selective-security model for key-policy ABE systems as given by Boyen [37] in the following game between an adversary and a challenger.

Target: The adversary $\mathcal{A}$ declares the attributes *Attrib**, which will wish to be challenged.

Setup: The challenger $\mathcal{B}$ obtains the public parameters *Pub* and corresponding master key *Msk* by invoking the system setup algorithm, and gives the public parameters *Pub* to the adversary $\mathcal{A}$.

Queries: The adversary $\mathcal{A}$ issues adaptive private keys *Key* queries by submitting attribute *i* to the challenger $\mathcal{B}$, where *i* is an attribute on its policy (**M**, ρ), as long as *Attrib** does not satisfy the policy (**M**, ρ).

Challenge: The adversary $\mathcal{A}$ gives a sign in readiness for accepting a challenge, and specify a message *Msg* to encrypt. The challenger $\mathcal{B}$ encrypts the message *Msg* for the challenge attributes *Attrib**. And then the challenger $\mathcal{B}$ flips a random coin $r = \{0,1\}$. If $r = 1$, the cipher text is send to the adversary $\mathcal{A}$. Otherwise, if $r = 0$, a random element of the cipher text space is send to the adversary A.

Queries: The adversary $\mathcal{A}$ may do additional key queries, this is a continuation of the earlier query phase.

Guess: The adversary $\mathcal{A}$ must submit a guess r' of r. The adversary's advantage in this game is defined as $|\Pr[r' = r] - \frac{1}{2}|$.

Definition 2. *A key-policy attribute-based encryption system is selectively secure if all PPT adversaries have at most a negligible advantage in this security game, where the adversary's advantage is defined as* $\text{Adv} = |\Pr[r' = r] - \frac{1}{2}|$.

3 A MULTI-AUTHORITY KEY-POLICY ABE SCHEME FROM LATTICE

In this section, we construct a multi-authority key-policy ABE scheme from lattice, the key-extract algorithm will generate the corresponding key for every attribute under an access policy represented by LSSS, and each of the attribute in the universe attribute set $\mathcal{U}$ is managed by its own attribute authority, the attribute authority is responsible for key generating of an attribute. And we suppose that each attribute $u_k (u_k \in \mathcal{U})$ has its own attribute authority, denoted as local authority $Auth^{(k)}$, and there is a central authority to generate some public parameters.

A new lattice-based key-policy ABE scheme consists of the following four algorithms:

- ***KP - ABE.Setup***$(\lambda) \rightarrow (pub, Msk)$: This algorithm takes a security parameter λ as input, do:
  1. The central authority selects three public parameters n, m and q, and publishes them, where $n > \Omega(\lambda)$ be a security dimension, $m > 5n \log q$ be a lattice base dimension, and $q > 2$ be a prime modulus. (The details is refer to the proposition 1[29], definition 4[23] in Appendix A.)
  2. For each attribute $u_k (u_k \in \mathcal{U})$,the local authority $Auth^{(k)}$ invokes the algorithm $TrapGen(n, m, q, \sigma)$[25] to create a uniformly random $n \times m$ matrix $\mathbf{A}_{u_k} \in \mathbb{Z}_q^{n \times m}$ with a full-rank *m-vector* set $\mathbf{B}_{u_k} \subseteq \Lambda_q^{\perp}(\mathbf{A}_{u_k})$ which satisfies the low-norm condition $\left\|\tilde{\mathbf{B}}_{u_k}\right\| \leq m \cdot \omega\left(\sqrt{\log m}\right)$, where σ is a Gaussian deviation parameter with $\Lambda(\mathbf{A}_{u_k})$. The local authority$Auth^{(k)}$ sends the matrix $\mathbf{A}_{u_k} \in \mathbb{Z}_q^{n \times m}$ to the central authority, and keeps $\mathbf{B}_{u_k} \subseteq \Lambda_q^{\perp}(\mathbf{A}_{u_k})$ as secret.
  3. The central authority selects a common uniformly random vector $\mathbf{u} \in \mathbb{Z}_q^n$ and a uniformly random integer $s \in \mathbb{Z}_q$, and publishes them as public parameters.
  4. Finally the central authority outputs the system public parameters *Pub*,

$$Pub = \{\mathbf{A}_{u_k}, \mathbf{u}, s\}_{u_k \in \mathcal{U}} .$$

And the secret key $Msk = \{\mathbf{B}_{u_k}\}_{u_k \in \mathcal{U}}$ is kept secretly by the local attribute authority separately.

- ***KP - ABE.Extract***$(Pub, \mathbf{B}_{\rho(i)}, (\mathbf{M}, \rho)) \rightarrow Key_{\rho(i)}$: This algorithm inputs the public parameters *Pub*, the master key *Msk*, an access policy ($\mathbf{M}$, ρ), and $\mathbf{B}\rho(i)$ is corresponding to the secret key of attribute $\rho(i)$ with the policy ($\mathbf{M}$, ρ), and the maximum attribute bound of policy ($\mathbf{M}$, ρ) is denoted by l, do:
  1. For the LSSS access policy ($\mathbf{M}$, ρ) on the universe attribute set $\mathcal{U}$, where $\mathbf{M}$ is a $l \times \theta$ matrix, called the share-generating matrix, and ρ is a function which maps the row number of matrix $\mathbf{M}$ to the universe attribute set $\mathcal{U}$, i.e. $\rho : [l] \rightarrow \mathcal{U}$, the *i-th* row of $\mathbf{M}$ will be assigned to a attribute $\rho(i) \in \mathcal{U}$.
  2. Construct a new vector $\mathbf{v} = (s, v_2, v_3, \cdots, v_\theta)^T$ where $v_2, \cdots, v_\theta \in \mathbb{Z}_q$ are randomly chosen, and computes the matrix multiplication $\mathbf{M} \cdot \mathbf{v}$, denotes the result by

$$(\lambda_1, \cdots, \lambda_l)^T := \mathbf{M} \cdot \mathbf{v} .$$

  3. Construct a new vector $\mathbf{w} = (0, w_2, \cdots, w_\theta)^T$, where $w_2, \cdots, w_\theta \in \mathbb{Z}_q$ are randomly chosen, and computes the matrix multiplication $\mathbf{M} \cdot \mathbf{w}$, denotes the result by

$$(\omega_1, \cdots, \omega_l)^T := \mathbf{M} \cdot \mathbf{w} .$$

  And denote,

$$\mathbf{s}_i := [\lambda_i + \omega_i, 0, \cdots, 0]^T, \quad i \in [l] .$$

  4. For each attribute $\rho(i)$, the authority $Auth_{\rho(i)}^{(k)}$ invokes the algorithm $SamplePre(\mathbf{A}_{\rho(i)}, \mathbf{B}_{\rho(i)}, \mathbf{s}_i, \sigma_i)$ [29] to generate $\xi_{\rho(i)} \in \mathbb{Z}_q^m$ such that $\mathbf{A}_{\rho(i)} \xi_{\rho(i)} \mathbb{A} \mathbf{s}_i$, where the distribution of $\xi_{\rho(i)}$ is statistically close to $D_{\Lambda_{\rho(i)}, \sigma_i, \mathbf{s}_i}$, and σ_i is Gaussian distribution parameter which satisfies $\sigma_i \geq \left\| \mathbf{B}_{\rho(i)} \right\| \cdot \omega\left(\sqrt{\log m}\right)$).
  5. Similarly, the authority $Auth_{\rho(i)}^{(k)}$ invokes the algorithm $SamplePre(\mathbf{A}_{\rho(i)}, \mathbf{B}_{\rho(i)}, \mathbf{u}, \sigma_i)$ to generate $\eta_{\rho(i)} \in \mathbb{Z}_q^m$ such that $\mathbf{A}_{\rho(i)} \eta_{\rho(i)} \mathbb{A} \mathbf{u}$, where the distribution of $\eta_{\rho(i)}$ is statistically close to

$D_{\rho(i),\sigma_i,\mathbf{u}}$, and Gaussian distribution parameter σ_i is the same as above.

6. Output the decryption keys $Key_{\rho(i)}$ of the attribute $\rho(i)$ for the policy ($\mathbf{M}$, ρ), where

$$Key_{\rho(i)} = \{\xi_{\rho(i)}, \eta_{\rho(i)}\}, \quad i \in [l].$$

- ***KP - ABE.Encrypt***$\left(Msg, Attrib, Pub\right) \rightarrow C_{tx}$: This algorithm inputs a message bit $Msg \in \{0,1\}$, a subset of attributes $Attrib = \{u_{i_1}, u_{i_2}, ..., u_{i_t}\}$, and the public parameters *Pub*, do:
  1. Select a uniformly random n-vector $\mathbf{x} \in \mathbb{Z}_q^n$.
  2. Select a low-norm Gaussian noise scalar $\chi_1 \leftarrow \bar{\Psi}_\alpha$ and compute

$$C_1 = \mathbf{x}^T(\mathbf{u} + \begin{bmatrix} s \\ 0 \\ \vdots \\ 0 \end{bmatrix}) + \chi_1 + \left\lfloor \frac{q}{2} \right\rfloor Msg \mod q$$

  3. Select a low-norm Gaussian noise vector $\chi_2 \leftarrow (\bar{\Psi}_\alpha)^{tm}$, and compute

$$C_2 = \mathbf{x}^T[\mathbf{A}_{u_{i_1}}, \mathbf{A}_{u_{i_2}}, ..., \mathbf{A}_{u_{i_t}}] + \boldsymbol{\zeta}_2 \mod q,$$

  4. Output the cipher text C_{tx} for the list *Attrib*,

$$C_{tx} = \{C_1, C_2 \mathbb{N} Attrib\}.$$

- ***KP - ABE.Decrypt***$(Pub, Key, C_{tx}) \rightarrow b$: This algorithm inputs the public parameters *Pub*, the decryption key *Key* and the cipher text $C_{tx} = \{C_1, C_2 \mathbb{N} Attrib\}$, the key is a collection of some attribute key under a access policy ($\mathbf{M}$, ρ),and those attributes are a subset of *Attrib*, and those attributes should satisfy the access policy ($\mathbf{M}$, ρ), do:
  1. As a subset of *Attrib* that corresponding to the key satisfies the policy ($\mathbf{M}$, ρ) (i.e. *Attrib* be an authorized set), it is easy to find a linear combination of some rows of $\mathbf{M}$ that yields $[1,0,\cdots,0] \in \mathbb{Z}^\theta$, the rows are those corresponding to attributes in the subset. That is, there is l-vector $\mathbf{g}' = \left[g'_{\rho(1)}, \cdots, g'_{\rho(l)}\right]$ satisfies

$$\left[g'_{\rho(1)},\cdots,g'_{\rho(l)}\right]\cdot\mathbf{M}=\left[1,0,\cdots,0\right]_{1\times\theta}.$$

From the above analysis, denote by

$$J=\{j \mid g'_{\rho(j)}\neq 0,\ j\in[l]\},$$

$$\rho(J)=\{\rho(j) \mid j\in J\}.$$

Then

$$\rho(J)\subseteq Attrib=\{u_{i_1},u_{i_2},...,u_{i_t}\}.$$

2. In order to describe the above relationship clearly, here define a 1-1 mapping function $\varphi: J\rightarrow[t]$ such that

$$\rho(j)=u_{i_{\varphi(j)}},\ j\in J,\ \varphi(j)\in[t].$$

Thus there is an inverse mapping φ^{-1} such that

$$u_{i_j}=\rho(\varphi^{-1}(j)).$$

3. For every $j \in J$, using the corresponding decryption keys $Key_{\rho\nu\varphi^{-1}(j))}=\{\xi_{\rho\nu\varphi^{-1}(j))},\eta_{\rho\nu\varphi^{-1}(j))}\}$ of attribute $\rho(\varphi^{-1}(j))$ under the policy (**M**, ρ), compute

$$v\hat{=}C_1-C_2\left[\mathbf{d}_1,\cdots,\mathbf{d}_t\right]^T-\frac{1}{\sum_{j\in J}g'_{\rho(\varphi^{-1}(j))}}C_2\left[\mathbf{e}_1,\cdots,\mathbf{e}_t\right]^T \bmod q,$$

where

$$\mathbf{d}_j=\begin{cases}g'_{\rho(\varphi^{-1}(j))}\eta^T_{\rho(\varphi^{-1}(j))}, & j\in J\\ \mathbf{0}, & j\notin J\end{cases},\quad \mathbf{e}_j=\begin{cases}g'_{\rho(\varphi^{-1}(j))}\eta^T_{\rho(\varphi^{-1}(j))}, & j\in J\\ \mathbf{0}, & j\notin J\end{cases}.$$

And let v be an integer in $\left[-\left\lfloor\frac{q}{2}\right\rfloor,\left\lfloor\frac{q}{2}\right\rfloor\right]$.

4. Output the decrypted message bit b as

$$b=\begin{cases}0 & |v|\le\left\lfloor\frac{q}{4}\right\rfloor\\ 1 & |v|\ge\left\lfloor\frac{q}{4}\right\rfloor\end{cases}.$$

4. CORRECTNESS AND SECURITY

4.1 Correctness

In order to ensure decryption successfully, there exists a suitable vector **g** to satisfy $\mathbf{g}^{\mathrm{T}}\cdot\mathbf{M}=[1,0,\cdots,0]$, and the secret key $Key_{\rho(\varphi^{-1}(j))}=\{\zeta_{\rho(\varphi^{-1}(j))},\eta_{\rho(\varphi^{-1}(j))}\}$ to satisfy the policy (**M**, ρ).The following we will discuss decryption process.

$$\varepsilon\triangleq C_1-C_2\left[\mathbf{d}_1,\cdots,\mathbf{d}_l\right]^T-\frac{1}{\sum_{j\in J}g'_{\rho(\varphi^{-1}(j))}}C_2\left[\mathbf{e}_1,\cdots,\mathbf{e}_l\right]^T$$

$$=C_1-C_2\left[g'_{\rho(\varphi^{-1}(1))}\zeta^T_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))}\right]^T$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}C_2\left[g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\eta^T_{\rho(\varphi^{-1}(l))}\right]^T$$

$$=C_1-\mathbf{x}^T\left[\mathbf{A}_{\rho(\varphi^{-1}(1))},\cdots,\mathbf{A}_{\rho(\varphi^{-1}(l))}\right]\left[g'_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))}\right]^T$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\mathbf{x}^T\left[g'_{\rho(\varphi^{-1}(1))}\mathbf{A}_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\mathbf{A}_{\rho(\varphi^{-1}(l))}\right]$$

$$\left[\eta^T_{\rho(\varphi^{-1}(1))},\cdots,\eta^T_{\rho(\varphi^{-1}(l))}\right]^T$$

$$-\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))}\right]^T$$

$$-\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(l))}\right]^T$$

$$=C_1-\mathbf{x}^T\left[g'_{\rho(\varphi^{-1}(1))}\mathbf{A}_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}\mathbf{A}_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))}\right]$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\mathbf{x}^T$$

$$\left[g'_{\rho(\varphi^{-1}(1))}\mathbf{A}_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))} + \quad \cdots + \quad g'_{\rho(\varphi^{-1}(l))}\mathbf{A}_{\rho(\varphi^{-1}(l))}\eta^T_{\rho(\varphi^{-1}(l))} \right]$$

$$-\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))} \right]^T$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\eta^T_{\rho(\varphi^{-1}(l))} \right]^T$$

$$= C_1 - \mathbf{x}^T\left[g'_{\rho(\varphi^{-1}(1))}\mathbf{s}_1 + \quad \cdots + \quad g'_{\rho(\varphi^{-1}(l))}\mathbf{s}_l \right]$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\mathbf{x}^T\left[g'_{\rho(\varphi^{-1}(1))}\mathbf{u} + \quad \cdots + \quad g'_{\rho(\varphi^{-1}(l))}\mathbf{u} \right]$$

$$-\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))} \right]^T$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\eta^T_{\rho(\varphi^{-1}(l))} \right]^T$$

$$= C_1 - \mathbf{x}^T[s,0,\cdots,0]^T - \mathbf{x}^T\mathbf{u} - \chi_2\left[g'_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))} \right]^T$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\eta^T_{\rho(\varphi^{-1}(l))} \right]^T$$

$$= \left\lfloor \frac{q}{2} \right\rfloor Msg + \chi_1 - \chi_2\left[g'_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))} \right]^T$$

$$-\frac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))},\cdots, g'_{\rho(\varphi^{-1}(l))}\eta^T_{\rho(\varphi^{-1}(l))} \right]^T$$

The above proof is due to the following conditions,

$$[g'_{\rho(\varphi^{-1}(1))}\mathbf{s}_1 + \ldots + g'_{\rho(\varphi^{-1}(l))}\mathbf{s}_l] = \sum_{j=1}^{l} g'_{\rho(\varphi^{-1}(j))\,\rho(\varphi^{-1}(j))}$$

$$= \sum_{j=1}^{l} g'_{\rho(\varphi^{-1}(j))}[\lambda_{\rho(\varphi^{-1}(j))} + \omega_{\rho(\varphi^{-1}(j))}, 0, \cdots, 0]^T \quad ,$$

$$= [\sum_{j=1}^{l} g'_{\rho(\varphi^{-1}(j))}(\lambda_{\rho(\varphi^{-1}(j))} + \omega_{\rho(\varphi^{-1}(j))}), 0, \cdots, 0]^T = [s, 0, \cdots, 0]^T$$

Also because of ,

$$\begin{aligned}&\left[g'_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\right]\left[\lambda_{\rho(\varphi^{-1}(1))},\cdots,\lambda_{\rho(\varphi^{-1}(l))}\right]^T\\&=\left[g'_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\right]\cdot\mathbf{M}\cdot\mathbf{v}^T\\&=[1,0,\cdots,0]_{1\times l}\left[s,v_2,\cdots,v_l\right]^T=s,\end{aligned}$$

$$\begin{aligned}&\left[g'_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\right]\left[\omega_{\rho(\varphi^{-1}(1))},\cdots,\omega_{\rho(\varphi^{-1}(l))}\right]^T\\&=\left[g'_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\right]\cdot\mathbf{M}\cdot\mathbf{w}^T\\&=[1,0,\cdots,0]_{1\times l}\left[0,w_2,\cdots,w_\theta\right]^T=0.\end{aligned}$$

Thus, let $|\varepsilon|\le\frac{q}{5}$ with overwhelming probability to be decrypted,

$$|\varepsilon|\triangleq\left|\begin{array}{l}\chi_1-\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\xi^T_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\xi^T_{\rho(\varphi^{-1}(l))}\right]^T\\-\dfrac{1}{g'_{\rho(\varphi^{-1}(1))}+\cdots+g'_{\rho(\varphi^{-1}(l))}}\chi_2\left[g'_{\rho(\varphi^{-1}(1))}\eta^T_{\rho(\varphi^{-1}(1))},\cdots,g'_{\rho(\varphi^{-1}(l))}\eta^T_{\rho(\varphi^{-1}(l))}\right]^T\end{array}\right|\le\frac{q}{5}.$$

4.2 Parameter Analysis

We will analyze the crucial system parameters in order to insure new scheme's correctness in this subsection. In new scheme, the security parameter is defined as λ, and the maximum of attribute bound with policy is defined as l, the rest of the parameters are set under the following constraints:

1. For LWE hardness assumption, Gaussian noise distribution $\chi_i=\bar{\Psi}^m_\alpha$, with Gaussian parameter satisfies $\alpha\ge2\sqrt{m}/q$. According to Regev's[43] proof, the norm of χ_i satisfy $O\left(\alpha q\sqrt{m}\right)\le2m.$ (See **Proposition 2**[33])
2. For the algorithm $TrapGen(n,m,q,\sigma)$, we need $n=\Omega(\lambda)$, prime $q>2$, lattice base dimension $m\ge5n\log q$, standard deviation of discrete Gaussian distribution $\sigma=\frac{1}{\sqrt{2\pi}}\cdot\alpha.$ If it satisfy to the dimension constraints of m, the output lattice from *TarapGen* algorithm[15] whose norm length is not more than $m\cdot\omega\left(\sqrt{\log m}\right).$ (See **Proposition** 1[29])

3. For Gaussian sample algorithm $SamplePre(\mathbf{A},\mathbf{B},\mathbf{u},\sigma)$, for any prime $q = poly(n) \geq 2$ and $m \geq 5n\log q$, we need $\sigma \geq \left\|\tilde{\mathbf{B}}\right\| \cdot \omega\left(\sqrt{\log m}\right)$, so that the norm length of extraction private key $key_i = \{\xi_i, \eta_i\}$ satisfy $\| \xi_i \| \leq \sigma\sqrt{m}$, $\| \eta_i \| \leq \sigma\sqrt{m}$ with overwhelming probability. (See **Lemma** 2 [29]).

Next, we discuss

$$
\begin{aligned}
|\varepsilon| &\triangleq |\chi_1 - \chi_2 \left[g'_{\rho(\varphi^{-1}(1))} \xi^T_{\rho(\varphi^{-1}(1))}, \cdots, g'_{\rho(\varphi^{-1}(l))} \xi^T_{\rho(\varphi^{-1}(l))} \right]^T \\
&\quad - \frac{1}{g'_{\rho(\varphi^{-1}(1))} + \cdots + g'_{\rho(\varphi^{-1}(l))}} \chi_2 \left[g'_{\rho(\varphi^{-1}(1))} \eta^T_{\rho(\varphi^{-1}(1))} \cdots, g'_{\rho(\varphi^{-1}(l))} \eta^T_{\rho(\varphi^{-1}(l))} \right]^T | \\
&\leq |\chi_1| + |\chi_2 \left[g'_{\rho(\varphi^{-1}(1))} \xi^T_{\rho(\varphi^{-1}(1))}, \cdots, g'_{\rho(\varphi^{-1}(l))} \xi^T_{\rho(\varphi^{-1}(l))} \right]^T \\
&\quad - \frac{1}{g'_{\rho(\varphi^{-1}(1))} + \cdots + g'_{\rho(\varphi^{-1}(l))}} \chi_2 \left[g'_{\rho(\varphi^{-1}(1))} \eta^T_{\rho(\varphi^{-1}(1))}, \cdots, g'_{\rho(\varphi^{-1}(l))} \eta^T_{\rho(\varphi^{-1}(l))} \right]^T | \\
&\leq |\chi_1| + |\sum_{j=1}^{l} g'_{\rho(\varphi^{-1}(j))} \xi^T_{\rho(\varphi^{-1}(j))} \chi_2| + |\sum_{j=1}^{l} \frac{g'_{\rho(\varphi^{-1}(j))}}{g'_{\rho(\varphi^{-1}(1))} + \cdots + g'_{\rho(\varphi^{-1}(j))}} \eta^T_{\rho(\varphi^{-1}(j))} \chi_2| \\
&\leq |\chi_1| + |\sum_{j=1}^{l} g'_{\rho(\varphi^{-1}(j))} \xi^T_{\rho(\varphi^{-1}(j))} \chi_2| + |\sum_{j=1}^{l} g'_{\rho(\varphi^{-1}(j))} \eta^T_{\rho(\varphi^{-1}(j))} \cdot \chi_2|
\end{aligned}
$$

$$
\begin{aligned}
&\leq (q\alpha \cdot \omega(\sqrt{\log m}) + 1/2) + 2l(m^{1.5} \cdot \omega(\sqrt{\log m})(q\alpha \cdot \omega(\sqrt{\log m}) + \sqrt{m}/2)) \\
&\leq (q\alpha \cdot \omega(\sqrt{\log m}) + \sqrt{m}/2)(1 + 2l(m^{1.5} \cdot \omega(\sqrt{\log m})) \\
&\leq q\alpha(\omega(\sqrt{\log m}) + 1)(1 + 2l(m^{1.5} \cdot \omega(\sqrt{\log m}))
\end{aligned}
$$

If $|\varepsilon| \leq \frac{q}{5}$ holds, then α need satisfy

$$
\alpha \leq \frac{1}{5}[(\omega(\sqrt{\log m}) + 1)(1 + 2l(m^{1.5} \cdot \omega(\sqrt{\log m}))]^{-1}
$$

According to $q\alpha \geq \sqrt{m}/2$, we can deduce

$$q \geq \frac{5}{2}\sqrt{m}[(\omega(\sqrt{\log m})+1)(1+l(m^{1.5}\cdot\omega(\sqrt{\log m}))]$$

If $|\varepsilon| \leq \frac{q}{5}$ holds, our scheme is correct. Thus we set n, m, σ, q, α as follows:

- The lattice dimension $m \geq 5n\log q$ and attributes upper bound l with the policy.
- The noise parameter of discrete Gaussian distribution $\alpha \leq \frac{1}{5}[(\omega(\sqrt{\log m})+1)(1+2l(m^{1.5}\cdot\omega(\sqrt{\log m}))]^{-1}$, and q be a prime $q \geq \frac{5}{2}\sqrt{m}[(\omega(\sqrt{\log m})+1)(1+l(m^{1.5}\cdot\omega(\sqrt{\log m}))]$, satisfying condition (1) above.
- $m = n^{1.5} \geq 5n\log q$, satisfying condition (2) above.
- $\sigma = \frac{1}{\sqrt{2\pi}}\cdot\alpha$, satisfying condition (3) above.

For the above parameters, it is not only satisfying the condition algorithm we used, but also can decrypt cipher text correctly with overwhelming probability.

4.3 Security

In this subsection, we will prove the following theorem regarding the selective-security model for the key-policy ABE systems from lattices.

Theorem 1. *On the selective-security model, if there exists a PPT (probabilistic polynomial-time) algorithm $\mathcal{A}$ in attacking against the above scheme with non-negligible advantage $\varepsilon > 0$, there exists a PPT $\mathcal{B}$ that can solve the decision $(\mathbb{Z}_q, n, \chi)$-LWE problem with non-negligible advantage $\varepsilon/2$, where $\alpha = O(poly(n))$.*

Proof. By used the prowess of $\mathcal{A}$ we will construct a PPT simulating algorithm $\mathcal{B}$ decide $(\mathbb{Z}_q, n, \chi)$- LWE problem with non-negligible advantage. The reduction proceeds as follows.

Instance. The challenger $\mathcal{B}$ request oracle $\mathcal{O}$ and obtains LWE samples that we denote as,

$$[(\mathbf{w}_0, v_0)] \in (\mathbb{Z}_q^n \times \mathbb{Z}_q)$$

$$\left[(\mathbf{w}_1^1, v_1^1), \cdots, (\mathbf{w}_1^m, v_1^m)\right] \in (\mathbb{Z}_q^n \times \mathbb{Z}_q)^m$$

$$\left[(\mathbf{w}_2^1, v_2^1), \cdots, (\mathbf{w}_2^m, v_2^m)\right] \in (\mathbb{Z}_q^n \times \mathbb{Z}_q)^m$$

$$\vdots$$

$$\left[(\mathbf{w}_l^1, v_l^1), \cdots, (\mathbf{w}_l^m, v_l^m)\right] \in (\mathbb{Z}_q^n \times \mathbb{Z}_q)^m$$

Target. The adversary $\mathcal{A}$ announces a target challenge *Attrib**.

Setup. The challenger $\mathcal{B}$ prepares the public parameter as follows.

If attribute $u_i \in Attrib^*$, set the matrix $\mathbf{A}_{u_i} = [\mathbf{w}_i^1 | \ldots | \mathbf{w}_i^m]$, where $\mathbf{w}_i$ derive from the LWE samples of index *i*.

If attribute $u_i \notin Attrib^*$, the challenger $\mathcal{B}$ first selects integers $q = q(\lambda)$, error rate $\alpha = \alpha(\lambda)$, and sampling rate $\sigma = \sigma(\lambda)$, and generates $(\mathbf{A}_{u_i}, \mathbf{B}_{u_i}) \leftarrow \text{TrapGen}(n, m, q, \sigma)$.

The challenger $\mathcal{B}$ sets $\mathbf{u} = \mathbf{w}_0 - [s, 0, \cdots, 0]^T (\mathbf{u} \in \mathbb{Z}_q^n)$, where $\mathbf{w}_0$ is from LWE sample of index 0, and $s \in \mathbb{Z}_q$ is selected randomly and uniformly.

The challenger $\mathcal{B}$ returns the public parameter *Pub* to the adversary $\mathcal{A}$,

$$Pub = \{\{\mathbf{A}_{u_i}\}_{u_i \in Attrib^*}, \mathbf{u}, s, q, \alpha, \sigma\}.$$

Queries. The adversary $\mathcal{A}$ is allowed to issue adaptive queries for a secret key $Key_{\rho(i)}$ by submitting attribute $\rho(i)$ to the challenger $\mathcal{B}$, where $\rho(i)$ is an attribute on its choice policy ($\mathbf{M}$, ρ), as long as the target attribute list *Attrib** does not satisfy the policy ($\mathbf{M}$, ρ). The challenger $\mathcal{B}$ constructs and returns a secret key $Key_{\rho(i)}$ for each query policy ($\mathbf{M}$, ρ) as follows.

As in the real scheme, the challenger $\mathcal{B}$ constructs a LSSS matrix $\mathbf{M} \in \mathbb{Z}^{l \times \theta}$ on the access policy. Let $\kappa \triangleq \{\rho(i_1), \rho(i_2), .., \rho(i_{num_0}) \,|\, 1 \le k \le num_0, 1 \le i_k \le l\}$ denote the set of attribute on choice policy ($\mathbf{M}$, ρ), compute the user private key $Key_{\rho(i_k)}$ for each attribute $\rho(i_k)$ on the query policy ($\mathbf{M}$, ρ) as follows:

Compute $(\xi_{\rho(i_1)}, \xi_{\rho(i_2)}, \cdots, \xi_{\rho(i_{num_0})})^T$ by using sample algorithm, satisfy

$$[\mathbf{A}_{\rho(i_1)}, \mathbf{A}_{\rho(i_1)}, \cdots, \mathbf{A}_{\rho(i_{num_0})}] \begin{pmatrix} \xi_{\rho(i_1)} \\ \xi_{\rho(i_2)} \\ \vdots \\ \xi_{\rho(i_{num_0})} \end{pmatrix} = \begin{pmatrix} s \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Notability, in this step have to ensure the challenge attribute subset *Attrib** do not satisfy the query policy $(\mathbf{M}, \rho)$, so here must exist at least one $\rho(i_k) \in \kappa$ and $\rho(i_k) \notin Attrib^*$, thus the challenger $\mathcal{B}$ can use $\mathbf{B}_{\rho(i_k)}$, which is a short base on orthogonal lattice $\Lambda^{\perp}\left(\mathbf{A}_{\rho(i_k)}\right)$, to compute a short base $\mathbf{T}_B$ on $[\mathbf{A}_{\rho(i_1)}, \cdots, \mathbf{A}_{\rho(i_j)}, \cdots, \mathbf{A}_{\rho(i_{num_0})}]$ by invoking algorithm $GenExtBasis(\mathbf{B}_{\rho(i_k)}, [\mathbf{A}_{\rho(i_1)}, \cdots, \mathbf{A}_{\rho(i_k)}, \cdots, \mathbf{A}_{\rho(i_{num_0})}])$. Lastly, the challenger $\mathcal{B}$ compute a short vector $(\xi_{\rho(i_1)}, \cdots, \xi_{\rho(i_{num_0})})$ satisfy the above equation by using $SamplePreimage([\mathbf{A}_{\rho(i_1)}, \cdots, \mathbf{A}_{\rho(i_k)}, \cdots, \mathbf{A}_{\rho(i_{num_0})}], \mathbf{T}_B, (s, 0, \cdots, 0)^T, \sigma)$.

Similarly the challenger $\mathcal{B}$ can get $\eta_{\rho(i_k)}$ by using sample algorithm $SamplePreimage(\mathbf{A}_{\rho(i_k)}, \mathbf{B}_{\rho(i_k)}, \mathbf{u}, \sigma)$, satisfy

$$\mathbf{A}_{\rho(i_k)} \eta_{\rho(i_k)} = \left(\mathbf{w}_0 - \begin{bmatrix} s \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) = \mathbf{u}$$

Thus the challenger B sends the private key pair $(\xi_{\rho(i_k)}, \eta_{\rho(i_k)})$ to each attribute $\rho(i_k) \notin Attrib^*$ in attribute list κ on the query policy $(\mathbf{M}, \rho)$.

Challenge. The adversary $\mathcal{A}$ gives a sign in readiness for accepting a challenge, and specifies a message $Msg^* \in \{0,1\}$ to encrypt. The challenger $\mathcal{B}$ encrypts the message *Msg** for the challenge attributes *Attrib**. Let $\phi = |Attrib^*|$, then the challenger $\mathcal{B}$ responds with a cipher text $C_{tx}{}^* = (c_1^*, c_2^*)$ assembled form the LWE instance, as follow:

Let $c_1^* = v_0 + \left\lfloor \frac{q}{2} \right\rfloor Msg^*$.

Let $c_2^* = \left[v_1^1, \cdots, v_1^m, \cdots, v_\phi^1, \cdots, v_\phi^m \right]$.

Note that, if the oracle $\mathcal{O}$ is a pseudo-random LWE oracle $\mathcal{O}_{\mathbf{x}}$ with embedded secret $\mathbf{x} \in \mathbb{Z}_q^n$, then

$$c_1^* = v_0 + \left\lfloor \frac{q}{2} \right\rfloor \cdot Msg^* = \mathbf{x}^T \mathbf{w}_0 + \chi_1 + \left\lfloor \frac{q}{2} \right\rfloor \cdot Msg^*$$

$$= \mathbf{x}^T \left(\begin{bmatrix} s \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) + \mathbf{x}^T \left(\mathbf{w}_0 - \begin{bmatrix} s \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) + \chi_1 + \left\lfloor \frac{q}{2} \right\rfloor \cdot Msg^*$$

$$= \mathbf{x}^T \begin{bmatrix} s \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \mathbf{x}^T \mathbf{u} + \chi_1 + \left\lfloor \frac{q}{2} \right\rfloor \cdot Msg^*$$

$$c_2^* = [v_1^1, ..., v_1^m, ..., v_\phi^1, ..., v_\phi^m]$$

When $u_i \in Attrib^*$, and v_i comes from the genuine LWE oracle $\mathcal{O}_{\mathbf{x}}$, then $[v_i^1, ..., v_i^m] = \mathbf{x}^T [\mathbf{w}_i^1 | ... | \mathbf{w}_i^m] + \chi_m = \mathbf{x}^T \cdot \mathbf{A}_{u_i} + \chi_2$. The distribution of $c_2^* = [v_1^1, ..., v_1^m, ..., v_\phi^1, ..., v_\phi^m]$ and $\mathbf{x}^T [\mathbf{A}_{u_1}, \mathbf{A}_{u_2}, \cdots, \mathbf{A}_{u_\phi}] + \chi_2 \bmod q$ is indistinguishable.

So that above encryption simulation is perfect.

Continuation. $\mathcal{A}$ is allowed continuing making further private key extraction queries, after having obtained the challenge ciphertext.

Decision. $\mathcal{A}$ eventually emits a guess, whether $C_{tx}^* = (c_1^*, c_2^*)$ was actually a valid encryption of $Msg^* \in \{0,1\}$ as requested.

If the guess is correct, then the challenger $\mathcal{B}$ answer the LWE sample is from a genuine LWE oracle $\mathcal{O}_{\mathbf{x}}$, otherwise it is from a random oracle $\mathcal{O}_{\$}$.

If the adversary succeeds in guessing *Msg** with probability at least $\frac{1}{2} + \varepsilon$, then B will correctly guess the nature of the LWE oracle with probability at least $\frac{1}{2} + \frac{\varepsilon}{2}$.

4.4 Efficiency Analysis

In order to explain the efficiency of the new scheme, we compare the new scheme with those schemes in other references ([35-37,43]) in terms of space efficiency and time efficiency, as illustrated in Table 1 and Table 2.

In table 1, we compare the size of public key, master key, private key and ciphertext with other ABE schemes form lattices on difference police (i.e. ciphertext-policy or key-policy). We let n be the security parameter, m be the dimension of the output lattice, l be the upper limit of all attributes, $|Attrib|$ be the number of attributes that must be satisfied with the access policy ($|Attrib| < l$). The new scheme is construed on key-policy ABE form lattices. Table 1 shows that, in terms of space efficiency, the new scheme is equivalent to literature [37], and is better than literature [36] and literature [43].

In table 2, we compare the time efficiency of encryption algorithm and decryption algorithm with other schemes. Here, we mainly consider the number of addition and multiplication operation in algorithms. In literature [36], d is defined as the minimum number of default attributes. That is, a system

Scheme	classification	Public key	Master key	Private key	Ciphertext
literature [35]	Fuzzy-IBE	$O(2lmn)$	$O(2lmm)$	$O(lm)$	$O(lm)$
literature [36]	CP-ABE	$O((l+d)mn)$	$O(mm)$	$O(2lm)$	$O(2lm)$
literature [37]	KP-ABE	$O(lmn)$	$O(lmm)$	$O((l+1)m)$	$O((l+1)m)$
literature [43]	KP-ABE	$O(2lmn)$	$O(2lmm)$	$O(2(l+r)m)$	$O(lm)$
Our scheme	KP-ABE	$O(lmn)$	$O(lmm)$	$O(2lm)$	$O(lm)$

TABLE 1
Compare on space efficiency

Time efficiency (time)	Encryption	Decryption
literature [35]	$O(lmn)^2$	$O(nl^2m^2)$
literature [36]	$O(2(l+d)mn^2)$	$O(2m(l+d)^2n^2)$
literature [37]	$O((l+1)mn^2)$	$O(n(\|Attrib\|+1)^2m^2)$
literature [43]	$O(2lmn)^2$	$O(2n(l+r)^2m^2)$
Our scheme	$O(\|Attrib\|mn^2)$	$O(2n\|Attrib\|^2m^2)$

Notes:
l : The upper limit of all attributes
d : The minimum number of default attributes, a system user has at least $d+1$ attributes ($d \le l$)
r : The number of gates in circuits

TABLE 2
Compare on time efficiency

user has at least $d+1$ attributes ($d \le l$). In literature [43], r is defined as the number of gates in circuits. In new scheme, we define a new mapping function to reduce the computation of the decryption algorithm. So, comparing on time efficiency of decryption algorithm, the new scheme is better than other schemes in literatures [35,36] and [43].

5. CONCLUSIONS

We present a multi-authority key-policy ABE from lattices in this paper, in which the private key of an attribute under an access policy is computed in a different method. In the new scheme each attribute can have its own authority, and the private key of each attribute under an access policy is created by the attribute authority alone. The new scheme is more practical for key management than the existing ABE scheme, especially for attributes belong to different networks nodes. So in practice, our new scheme is exactly suitable for distributed environment in MANETs.

In the next step, a revocable and keyword-searchable ABE scheme from lattices is worth studying. Moreover, we plan to extend the proposed framework to heterogeneous wireless networks [47,48]. In addition, using recent advances of big data [49] in the security issue can be an interesting research direction.

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China under grants 61572019 and 61672358, Shaanxi Provincial Natural Science Foundation under grants 2016JZ001, and Research Foundation of Education Department of Shaanxi Province of China under grants 2013JK1142. Thanks also go to the anonymous reviewers for their useful comments.

REFERENCE

[1] Gangwar, S. (2016).Security threats in mobile ad hoc networks-A survey. International Journal of Computer Science and Information Technologies, vol. 7, no. 1, pp.74–77.

[2] Ouada, F. S., Mawloud, O., Bouabdallah, A., Tari, A.(2016).Lightweight identity-based authentication protocol for wireless sensor networks. International Journal of Information and Computer Security,vol. 8, no. 2, pp.121–138.

[3] Deng, H., Agrawal, D.P.(2004).TIDS: Threshold and identity-based security scheme for wireless ad hoc networks. Ad Hoc Networks, vol. 2, no. 3, pp. 291–307.

[4] Chase, M. (2009). Multi-authority attribute based encryption.The 4th Theory of Cryptography Conference, Amsterdam, the Netherlands, pp. 515–534.

[5] Shor, P. W. (1997).Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.SIAM Review,vol. 26, no. 5, pp. 1484–1509.

[6] Liang, C. and Yu, F. R. (Firstquarter 2015). Wireless network virtualization: A survey, some research issues and challenges. IEEE Commun. Surveys Tutorials, vol 17, no. 1, pp. 358–380.

[7] Nan Zhao, F. Richard Yu, Ming Li, Qiao Yan, Victor C. M. Leung. (2016). Physical layer security issues in interference- alignment-based wireless networks. IEEE Communications Magazine, vol. 54, no. 8, pp. 162–168.

[8] Niu, J., Gao, Y., Qiu, M., and Ming, Z. (2012). Selecting proper wireless network interfaces for user experience enhancement with guaranteed probability. Journal of Parallel and Distributed Computing, vol. 72, no. 12, pp. 1565–1575.

[9] Zhang, S. and Liew, S. C. (2010). Applying physical-layer network coding in wireless networks. EURASIP Journal on Wireless Communications and Networking, 2010(1):1.

[10] Jinyi, Z., Shutao, X., Jiang, Y., Zheng, H., and Laizhong, C. (2013). Maximum multiflow in wireless network coding. IEICE Transactions on Communications, vol. 96, no. 7, pp. 1780–1790.

[11] Lin, X.-H., Kwok, Y.-K., Wang, H., and Xie, N. (2015). A game theoretic approach to balancing energy consumption in heterogeneous wireless sensor networks. Wireless Communications and Mobile Computing, vol. 15, no. 1, pp. 170–191.

[12] Qiu, M., Ming, Z., Li, J., Liu, J., Quan, G., and Zhu, Y. (2013). Informer homed routing fault tolerance mechanism for wireless sensor networks. Journal of Systems Architecture, vol. 59, no. 4, pp. 260–270.

[13] Lu, K., Chen, G., Feng, Y., Liu, G., and Mao, R. (2010). Approximation algorithm for minimizing relay node placement in wireless sensor networks. Science China Information Sciences, vol. 53, no. 11, pp. 2332–2342.

[14] Qiao Yan; Yu, F.,Jianqiang Li, Qingxiang Gong. (2016). Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. IEEE Communications Surveys & Tutorials. vol. 18, no. 1, pp. 602–622.

[15] Qiao Yan; Qingxiang Gong, and Fang-an Deng. (2016). Detection of DDoS Attacks Against Wireless SDN Controllers Based on the Fuzzy Synthetic Evaluation Decision-making Model. Ad Hoc & Sensor Wireless Networks, vol. 33, pp. 275–299.

[16] Sahai, A.,Waters, B. (2005). Fuzzy identity-based encryption.EUROCRYPT 2005, LNCS, vol.3494, Springer Berlin Heidelberg, pp. 557–557.

[17] Goyal, V.,Pandey, O., Sahai, A.,Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. The 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, pp. 89–98.

[18] Bethencourt, J.,Sahai, A.,Waters, B. (2007). Cipher text-policy attribute-based encryption. IEEE Symposium on Security and Privacy, Oakland, pp. 321–334.

[19] Waters, B. (2011). Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization.Public Key Cryptography, LNCS,vol. 6571,Springer Berlin Heidelberg, pp. 53–70.

[20] Okamoto, T.; Takashima, K. (2014). Efficient attribute-based signatures for non-monotone predicates in the standard model. IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 409–421.

[21] Li, W., Xue, K. P., Xue, Y. J., Hong, J. N. (2016). TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage. IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484–1496.

[22] Cheng, S., Nguyen, K., Wang, H.(2016). Policy-based signature scheme from lattices. Designs, Codes and Cryptography, vol. 81, no. 1, pp. 1–32

[23] Rahulamathavan, Y., Veluru, S., Han, J.,Li,F.,Rajarajan,M., Lu, R. (2016). User collision avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption. IEEE Transactions on Computers, vol. 65, no. 9, pp: 2939–2946.

[24] Rial, A. (2016). Blind attribute-based encryption and oblivious transfer with fine-grained access control. Designs, Codes and Cryptography, vol. 81, no. 2, pp. 179–223.

[25] Ruj, S., Stojmenovic, M., Nayak A. (2014). Decentralized access control with anonymous authentication of data stored in clouds.IEEE Transactions on Parallel & Distributed Systems, vol. 25, no. 2, pp. 384–394.

[26] Nkenyereye, L., Park, Y., Rhee, K. H. (2016). A secure billing protocol over attribute-based encryption in vehicular cloud computing. EURASIP Journal on Wireless Communications and Networking, 2016(1), pp. 1–12.

[27] Ajtai, M. (1996). Generating hard instances of lattice problems. The 28th Annual ACM Symposium on Theory of Computing, ACM, New York, USA, pp. 99–108.

[28] Ajtai, M., Dwork, C. (1997). A public-key cryptosystem with worst-case/average-case equivalence. STOC'1997, ACM,El Paso, Texas, USA, pp. 284–293.

[29] Gentry, C. Peikert, C., Vaikuntanathan, V. (2008). Trapdoors for hard lattices and new cryptographic constructions. STOC2008, ACM, Victoria, British Columbia, Canada, pp. 197–206.

[30] J. Alwen, C. Peikert, Generating shorter bases for hard random lattices. The 26th International Symposium on Theoretical Aspects of Computer Science (STACS'2009), Springer, Freiburg, February 2009, pp.75–86.

[31] Micciancio, D., Peikert, C. (2012). Trapdoors for lattices: simpler, tighter, faster, and smaller.The 31th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2012, Springer Berlin Heidelberg, pp. 700–718.

[32] Micciancio, D. (2012).Inapproximability of the shortest vector problem: toward a deterministic reduction. Theory of Computing, vol. 8, no. 22, pp. 487–512.
[33] Regev, O.(2005). On lattices, learning with errors, random linear codes, and cryptography. The 37th Annual ACM Symposium on Theory of Computing, Baltimore, Maryland, USA, pp. 84–93.
[34] Brakerski, Z., Langlois, A., Peikert, C.,Regev, O., Stehle, D. (2013).Classical hardness of learning with errors. The 45th Annual ACM Symposium on Symposium on Theory of Computing, New York, USA,pp. 575–584.
[35] Agrawal, S.,Boyen, X.,Vaikuntanathan, V., Voulgaris, P.,Wee, H. (2012). Functional encryption forthreshold functions (or fuzzy IBE) from lattices.PKC 2012, LNCS, vol. 7293, Springer Berlin Heidelberg,pp. 280–297.
[36] Zhang, J., Zhang, Z., Ge, A. (2012). Ciphertext policy attribute-based encryption from lattices.The 7th ACM Symposium on Information, Computer and Communications Security, Seoul, Republic of Korea,pp.16–17.
[37] Boyen, X. (2013). Attribute-based functional encryption on lattices. TCC 2013, Theory of Cryptography, LNCS, vol. 7785, Springer Berlin Heidelberg, pp. 122–142.
[38] Peikert, C. (2009). Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. STOC2009, Bethesda, Maryland, pp. 333–342.
[39] Cash, D., Hofheinz, D., Kiltz, E., Peikert, C. (2010). Bonsai trees, or how to delegate a lattice basis. TACT 2010,Advances in Cryptology, EUROCRYPT 2010, LNCS, vol. 6110, pp. 523–552.
[40] Micciancio, D., Regev, O. (2004). Worst-case to average-case reductions based on Gaussian measures. The 45th Annual IEEE Symposium on Foundations of Computer Science, Rome, Italy, pp. 372–381.
[41] Beimel, A. (1996). Secure schemes for secret sharing and key distribution, PhD thesis, Department of Computer Science,Technion.
[42] Han, F., Qin, J., Zhao, H., Hu, J. (2014). A general transformation from KP-ABE to searchable encryption. Future Generation Computer Systems,vol. 30, no. 1, pp. 107–115.
[43] Zhao, J.,Gao, H. Y., Zhang, J. Q.(2014). Attribute-based encryption for circuits on lattices. Tsinghua Science and Technology,vol. 45, no. 5, pp. 479–499.
[44] Shraddha, R., Bharat, T. (2014). Enhancing flexibility for ABE through the use of cipher policy scheme with multiple mediators. FICTA2014, Bhubaneswar, Odisa, India, pp. 457–464.
[45] Li, C., Lang, B.,Wang, J. M. (2016).Outsourced KP-ABE with enhanced security. INTRUST 2014, Trusted systems, LNCS, vol. 9473, pp. 36–50.
[46] Karati, A., Amin, R., Biswas, G. P. (2016). Provably secure threshold-based ABE scheme without bilinear map. Arabian Journal for Science and Engineering, vol. 41, no. 8, pp. 3201–3213.
[47] Ma, L., Yu, F., Leung, V.C.M., Randhawa, T. (2004). A New Method to Support UMTS/WLAN Vertical Handover Using SCTP, IEEE Wireless Comm., vol. 11, no. 4, pp. 44–51, Aug. 2004.
[48] Yu, F., Krishnamurthy, V. (2007). Optimal Joint Session Admission Control in Integrated WLAN and CDMA Cellular Networks with Vertical Handoff, IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 126–139, Jan. 2007.
[49] He, Y., Yu, F. R., Zhao, N., Yin, H., Yao, H., Qiu, R.C. (2016). Big Data Analytics in Mobile Cellular Networks, IEEE Access, vol. 4, pp. 1985–1996, 2016.

APPENDIX A

A.1 Lattices and LWE Hardness Assumption

Definition 1. Let $\mathbf{B} = \left[\mathbf{b}_1 \middle| \cdots \middle| \mathbf{b}_m\right] \in \mathbb{R}^{m\times m}$ be a $m \times m$ matrix whose columns are linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_m \in \mathbb{R}^m$. The m-dimensional full-rank lattice Λ generated by **B** is infinite periodic set,

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{y} \in \mathbb{R}^m \quad \text{s.t.} \quad \exists \mathbf{s} = (s_1, s_2, ..., s_m) \in \mathbb{Z}^m, \mathbf{y} = \mathbf{Bs} = \sum_{i=1}^{m} s_i \mathbf{b}_i\}$$

Here, we are interested in integer lattices, i.e. infinite periodic subsets of $\mathbb{Z}^m$, that are invariant under translation by multiples of some integer q in each of the coordinates.

Definition 2. For q prime, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{u} \in \mathbb{Z}_q^n$, define:

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m \quad \text{s.t.} \quad \mathbf{Ae} = 0 \pmod{q}\}$$
$$\Lambda_q^{u}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m \quad \text{s.t.} \quad \mathbf{Ae} = \mathbf{u} \pmod{q}\}$$

Definition 3. Let $m \in \mathbb{Z}_{>0}$ be a positive integer and $\Lambda \in \mathbb{R}^m$ an m-dimensional lattice. For any vector $\mathbf{c} \in \mathbb{R}^m$ and any positive parameter $\sigma \in \mathbb{R}_{>o}$, we define:

$\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi \frac{\|\mathbf{x}-\mathbf{c}\|^2}{\sigma^2}\right)$: A Gaussian-shaped function on $\mathbb{R}^m$ with center **c** and parameter σ.

$\rho_{\sigma,\mathbf{c}}(\Lambda) = \sum_{\mathbf{x}\in} \rho_{\sigma,\mathbf{c}}(\mathbf{x})$: The discrete integral of $\rho_{\sigma,\mathbf{c}}$ over the lattice Λ.

$D_{\Lambda,\sigma,\mathbf{c}}$: The discrete Gaussian distribution over Λ with center **c** and parameter σ,

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

For notional convenience, $\rho_{\sigma,0}$ and $D_{\Lambda,\sigma,0}$ are abbreviated as ρ_σ and $D_{\Lambda,\sigma}$.

Gentry et al.[29] construct the following algorithm for sampling from the discrete Gaussian $D_{\Lambda,\sigma,\mathbf{c}}$, given a basis **B** for the m-dimensional lattice Λ with $\sigma \geq \|\tilde{\mathbf{B}}\| \cdot \omega\left(\sqrt{\log m}\right)$:

SampleGaussian (Λ,**B**,σ,**c**)[29]: On input lattice Λ, a basis **B** for Λ, a positive Gaussian parameter σ, and a center vector $\mathbf{c} \in \mathbb{R}^m$, it outputs a fresh random vector $\mathbf{x} \in \Lambda$ drawn from a distribution statistically close to $D_{\Lambda,\sigma,\mathbf{c}}$.

Proposition 1[19]. For any prime $q \geq 2$ and $m \geq 5n\log q$. There exists a probabilistic polynomial-time algorithm *TrapGen* that outputs a pair $(\mathbf{A} \in \mathbb{Z}_q^{n\times m}, \mathbf{B} \in \mathbb{Z}_q^{m\times m})$, such that Λ is statistically close to uniform and **B** is a basis for $\Lambda_q^{\perp}(\mathbf{A})$ with length $L = \left\|\tilde{\mathbf{B}}\right\| \leq m \cdot \omega\left(\sqrt{\log m}\right)$ with all but $n^{-\omega(1)}$ probability.

TrapGen(n,m,q,σ)[19]: On input a modulus q, a lattice dimension m, a constraint dimension n, and a Gaussian deviation parameter σ dimension Λ, it outputs **A** and **B** as above.

The main use of short lattice basis for our purposes is that they will allow us to sample short pre-images of a specific target under the linear map defined by the matrix associated with the lattice. The following algorithm is what allows us to perform this pre-image sampling. The shorter the lattice basis, the smaller a pre-image we shall be able to obtain.

SamplePre(**A**,**B**,**u**,σ)[19]: Let n,q,m be positive integers with $q \geq 2$, $m \geq 2n\log q$. On input a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ with 'short' trapdoor basis **B** for $\Lambda_q^{\perp}(\mathbf{A})$, a target image $\mathbf{u} \in \mathbb{Z}_q^n$ and a Gaussian parameter $\sigma \geq \left\|\tilde{\mathbf{B}}\right\| \cdot \omega\left(\sqrt{\log m}\right)$, outputs a sample $\mathbf{e} \in \mathbb{Z}^m$ from a distribution that is within negligible statistical distance $D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma}$.

Definition 4[23]. Consider a prime q, a positive integer n, and a distribution $\chi \in \mathbb{Z}_q$, all public. An $(\mathbb{Z}_q, n, \chi)$- LWE problem instance consists of access to an unspecified challenge oracle $\mathcal{O}$, being, either, a noisy pseudo-random sampler $\mathcal{O}_{\mathbf{x}}$ carrying some constant random secret key $\mathbf{x} \in \mathbb{Z}_q^n$, or, a truly sampler $\mathcal{O}_{\$}$, whose behaviors are respectively as follows:

$\mathcal{O}_{\mathbf{x}}$: Output noisy pseudo-random samples of the form $(\mathbf{w}_i, v_i) = (\mathbf{w}_i, \mathbf{w}_i^T\mathbf{x} + \chi_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where, $\mathbf{x} \in \mathbb{Z}_q^n$ is a uniformly distributed persistent secret key that is invariant across invocations, $\chi_i \in \mathbb{Z}_q$ is a freshly generated ephemeral additive noise component with distribute χ, and $\mathbf{w}_i \in \mathbb{Z}_q^n$ is a fresh uniformly distributed vector revealed as part of the output.

$\mathcal{O}_{\$}$: Output truly random samples $(\mathbf{w}_i, v_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, drawn in independently uniformly at random in the entire domain $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

The $(\mathbb{Z}_q, n, \chi)$-LWE problem statement, or LWE for short, allows an unspecified number of queries to be made to the challenge oracle $\mathcal{O}$, with no stated prior bound. We say that an algorithm *A* decides the $(\mathbb{Z}_q, n, \chi)$-LWE problem if $\left|\Pr[A^{\mathcal{O}_{\mathbf{x}}} = 1] - \Pr[A^{\mathcal{O}_{\$}} = 1]\right|$ is non-negligible for a random $\mathbf{x} \in \mathbb{Z}_q^n$.

It has been shown in literature[34] that there is a *poly*(n,q)-timereduction from search $(\mathbb{Z}_q, n, \chi)$-LWE to decision $(\mathbb{Z}_q, n, \chi)$-LWE.

The confidence in the hardness of the LWE problem stems in part of a result of Regev[23], which shows that the for certain noise distributions χ, the LWE problem is as hard as the worst-case SIVP and GapSVP under a quantum reduction. A classical reduction with related parameters was later obtained by Peikert[38].

Proposition 2[23]. For an $\alpha \in (0,1)$ and a prime $q > 2\sqrt{n}/\alpha$, let $\bar{\Psi}_\alpha$ denote the discrete dist ribution over $\mathbb{Z}_q$ of the random variable $\lfloor qX + \frac{1}{2} \rfloor \bmod q$ where the random variable X is a normal random variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$. Then, if there exists an efficient, possibly quantum algorithm for deciding the $(\mathbb{Z}_q, n, \chi)$-LWE, there exists a quantum polytime algorithm for approximating the SIVP and Gap-SVP problems, to within $\tilde{O}(n/\alpha)$ factors in the l_2 norm, in the worst case.

A.2 Delegate algorithm of a Lattice Basis

Cash et al.[29] described how an arborist may extend its control of a lattice to an arbitrary higher- dimensional extension, without any loss of quality in the resulting basis.

ExtBasis$\left(\mathbf{S}, \mathbf{A}' = \mathbf{A} \| \overline{\mathbf{A}}\right)$ [39] Given an arbitrary matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ whose columns generate the entire group $\mathbb{Z}_q^n$, an arbitrary basis $\mathbf{S} \in \mathbb{Z}^{m \times m}$ of $\Lambda^\perp(\mathbf{A})$, and an arbitrary $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n \times \bar{m}}$. Outputs a basis $\mathbf{S}'$ of $\Lambda^\perp(\mathbf{A}') \subseteq \mathbb{Z}^{m+\bar{m}}$, such that $\|\tilde{\mathbf{S}}\| = \|\tilde{\mathbf{S}}_0\|$. Moreover, the same holds even for any given permutation of the columns of $\mathbf{A}'$ (e.g., if columns of $\overline{\mathbf{A}}$ are both appended and extended to $\mathbf{A}$).

RandBasis ($\mathbf{S}$,r)[39]: Input m-dimension lattice $\Lambda^\perp(\mathbf{A})$, with a basis $\mathbf{S} \in \mathbb{Z}^{m \times m}$, and a parameter $r \geq \|\tilde{\mathbf{S}}\| \cdot \omega(\sqrt{\log n})$. . With overwhelming probability, output a short basis $\mathbf{S}'$ of lattice $\Lambda^\perp(\mathbf{A})$, such that $\|\mathbf{S}'\| \leq r \cdot \sqrt{m}$. Moreover, for any two bases $\mathbf{S}_0, \mathbf{S}_1$ of the same lattice and any $r \geq \max\{\|\tilde{\mathbf{S}}_0\|, \|\tilde{\mathbf{S}}_1\|\} \cdot \omega(\sqrt{\log n})$, the outputs of *RandBasis* ($\mathbf{S}_0$,r) and *RandBasis* ($\mathbf{S}_1$,r) are within *negl*(n) statistical distance.

A.3 Two Lemmas to Bound Norms

Next two lemmas will need to show that can guarantee decryption works correctly.

Lemma 1[40]. For any m-dimension lattice Λ, vector $\mathbf{c} \in R^m$, and real $\varepsilon \in (0,1), s > \eta_\varepsilon(\Lambda)$, we have

$$\Pr_{\substack{r \\ \mathbf{x} \sim D_{\Lambda,s,\mathbf{c}}}} \left[\|\mathbf{x} - \mathbf{c}\| > s\sqrt{n}\right] \leq \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-m}$$

The lemma sates that for large enough s, almost the elements chosen from $D_{\Delta,s,\mathbf{c}}$ are close to $\mathbf{c}$.

Lemma 2[29]. Let **e** be some vector in $\mathbb{Z}_m$ and let $\mathbf{y} \leftarrow \bar{\Psi}_\alpha^m$. Then the quantity $\left|\mathbf{e}^{\mathrm{T}}\mathbf{y}\right|$ treated as an integer in [0, q – 1] satisfies

$$\left|e^{\mathrm{T}}\mathbf{y}\right| \le \|\mathbf{e}\|(q\alpha\cdot\omega\left(\sqrt{\log m}\right)+\frac{\sqrt{m}}{2})$$

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 $|x| \le q\alpha\cdot\omega\left(\sqrt{\log m}\right)+1/2$ with all but negligible probability in m.

APPENDIX B

B.1 Access Structure and Linear Secret Sharing Scheme

Definition 5[41]. Let $\mathcal{U}$ be the attribute universe. An access structure on $\mathcal{U}$ is a collection $\mathbb{A}$ of non- empty sets of attributes, i.e. $\mathbb{A} \subseteq 2^{\mathcal{U}} \setminus \{\}$. The sets in $\mathbb{A}$ are called the authorized sets and the sets not in $\mathbb{A}$ are called the unauthorized sets. Additionally, an access structure is called monotone if $\forall B,C \in \mathbb{A}$: if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$.

Definition 6[41]. Let p be a prim and $\mathcal{U}$ be the attribute universe. A secret sharing scheme Π with domain of secrets $\mathbb{Z}_p$ realizing access structures on $\mathcal{U}$ is linear over $\mathbb{Z}_p$ if

1. The shares of a secret $s \in \mathbb{Z}_p$ for each attribute form a vector over $\mathbb{Z}_p$.
2. For each access structure $\mathbb{A}$ on $\mathcal{U}$, there exists a matrix $\mathbf{M} \in \mathbb{Z}_q^{l\times\theta}$, called the share-generating matrix, and a function on ρ, that labels the rows of **M** with attributes from $\mathcal{U}$, i.e. $\rho:[l]\to\mathcal{U}$, which satisfy the following:

During the generation of the shares, we consider the column vector $\vec{v} = \left(s, r_2, \cdots, r_\theta\right)^T$, where $r_2, \cdots, r_\theta \xleftarrow{\$} \mathbb{Z}_q$. Then the vector of l shares of the secret s according to Π is equal to $\mathbf{M}v = \left(\lambda_1, \lambda_2, \cdots \lambda_l\right) \in \mathbb{Z}_p^{l\times\theta}$. The share $\lambda_i = \left(\mathbf{M}v\right)_i$ is assigned to party ρ(i).

Every LSSS according to the above definition enjoys the linear reconstruction property. This means that if Π is an LSSS for the access structure $\mathbb{A}$, and then the following is true. Let $\mathcal{S} \in \mathbb{A}$ be any authorized set, and let $I \subset \{1,2,\cdots l\}$ be defined as $I = \{i : \rho(i) \in \mathcal{S}\}$. Then, there exist constants $\{k_i \in \mathbb{Z}_q\}$ for $i \in I$, such that, if $\{\lambda_i = (\mathbf{M}\vec{v})_i\}$ are valid shares of any secret s according to Π, then $\sum_{i\in I} k_i\lambda_i = s$. It was shown by Beimel[41], that these

constants $\{k_i\}$ can be found in time polynomial in the size of the share-generating matrix $\mathbf{M}$.

On the other hand, for unauthorized sets $\mathcal{S}' \notin \mathbb{A}$ no such constants $\{k_i\}$ exist. Moreover, in this case it is also true that if $I' = \{i \mid i \in [l] \wedge \rho(i) \in \mathcal{S}'\}$, there exists a vector $\vec{\omega} \in \mathbb{Z}_p^\theta$, such that its first component ω_1 is any non-zero element in $\mathbb{Z}_p$ and $\mathbf{M}_i \vec{\omega} = \mathbf{0}$ for all $i \in I'$, where $\mathbf{M}_i$ is i-th row of $\mathbf{M}$.