RL-ABE: A Revocable Lattice Attribute Based Encryption Scheme Based on R-LWE Problem in Cloud Storage

Siyu Zhao, Rui Jiang, and Bharat Bhargava, *Fellow, IEEE*

Abstract—In this article, we propose a revocable lattice-based CP-ABE (Ciphertext-Policy Attribute-Based Encryption) scheme (RL-ABE), which is suitable to be applied in the cloud storage. The RL-ABE scheme can resist quantum algorithm attack and ensure fine-grained access control to the users' rights in achieving shared data. In addition, our scheme can realize attribute revocation, which can expediently renew users' attributes to grant or revoke their access rights. Then, we formally prove the security of our scheme based on the hardness of Ring Learning with Error problem(R-LWE) to resist quantum algorithm attack, and prove our scheme can solve security threatens to withstand collusion attacks. Finally, the performance analysis shows the high efficiency of our scheme compared with other related schemes.

Index Terms—Ciphertext-policy attribute-based encryption, attribute revocation, lattice-based cryptosystem, ring learning with error problem

1 Introduction

The development of network technology improves the speed of information transmission and the storage space, which promotes the development of cloud computing. The cloud computing provides convenience for users to share their data, thus saves the cost of local data management. For example, each user can use Baidu SkyDrive to upload videos, text files, torrents or other resources to share with other people. Cloud storage plays an important role in daily life. However, some data may be highly sensitive such as E-healthy records in the hospital. To ensure the security of cloud storage, many encryption schemes have been proposed.

Based on the notion of Identity-Based Encryption (IBE) [1], Sahai and Waters introduced the Attribute-Based Encryption (ABE) [2] as a new style of IBE. In the ABE scheme, each user owns a set of attributes, which can represent users' identity. Data owners can generate the ciphertext labels with a set of attributes and users can get their secret keys from the Key Generate Center (KGC) according to their attributes. Only if the attributes in secret key match the attributes in the ciphertext, can the user decrypt the ciphertext and achieve the shared data. The ABE scheme can make fine-grained access control.

ABE can be classified into two types: Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [3] and Key-Policy Attribute-Based Encryption (KP-ABE) [4]. In CP-ABE schemes, data owners can decide their access policies and apply policies to encrypt their messages. Besides, the KGC manages attributes and embed users' attributes in their secret keys. Only if the attributes in the secret key satisfy the requirement of access policy, can the user decrypt the ciphertext successfully. Since data owners can directly control their access policies of shared data, CP-ABE is regarded as one of the most promising schemes.

Attribute revocation is a necessary requirement of ABE schemes since users' attributes change a lot and their data access rights are dynamic. In some schemes [5], [6], KGC can accomplish effective user revocation by making a revocation list and revoking the access right of users on the list directly. However, the two schemes cannot make fine-grained revocation. In scheme [7], the authors proposed a method that assigned an expiration time to each attributes. However, this method cannot ensure high efficiency. Many schemes [8], [9], [10], [11], [12], [13], [14], [15] make attribute revocation by re-encrypting related components of ciphertexts and secret keys. With this kind of approach, attribute revocation may achieve high efficiency with low computation burden and storage cost. In the scheme [8], the authors separated users into different groups to manage their secret keys and apply re-encryption method to make revocation. However, the scheme could not resist collusion attacks. In the scheme [9], the authors improved the security of user group management by proposing attributes groups and identifying each user uniquely. Liu *et al*. proposed a secure data sharing scheme [10] that could support data sharing for group users. The scheme [11] could realize efficient attribute revocation. However, the above three schemes cannot resist collusion attacks. The scheme [12] can resist collusion attacks and many other attacks, which ensures the security of the revocation. However, it is not efficient enough for it's computation

- *S. Zhao is with the School of Information Science and Engineering, Southeast University, Nanjing, Jiangsu 210096, China. E-mail: 865961756@qq.com.*
- *R. Jiang is with the School of Cyber Science and Engineering, Southeast University, Nanjing, Jiangsu 210096, China. E-mail: r.jiang@seu.edu.cn.*
- *B. Bhargava is with the Department of Computer Science, Purdue University, West Lafayette, IN USA. E-mail: bbshail@purdue.edu.*

Manuscript received 3 Apr. 2019; revised 24 Jan. 2020; accepted 7 Feb. 2020. Date of publication 11 Feb. 2020; date of current version 8 Apr. 2022.
(Corresponding author: Rui Jiang.)
Digital Object Identifier no. 10.1109/TSC.2020.2973256

cost. The scheme [13] was designed to improve the efficiency. Li *et al.* proposed scheme [14] to ensure the security of revocation. However, there's no guarantee of efficiency. In scheme [15], the authors applied the group mangers to control the revocation, and made the scheme to resist collusion attacks and ensure high efficiency.

Unfortunately, almost all ABE schemes are based on bilinear pairing algorithm which is on the hardness of Diffie-Hellman Problem or Discrete Logarithm Problem. There are not any mature and efficient CP-ABE schemes that are constructed on other cryptographic assumptions. With the development of post-quantum, bilinear pairing algorithm, which is based on the hardness of Diffie-Hellman Problem or Discrete Logarithm Problem, is proven not able to ensure the security of encryption in the near future [16], which means the bilinear pairing algorithm becomes insecure in the presence of large-scale quantum computers and fails to protect secret data on quantum algorithm attack. Lattice problems, which include Shortest Vector Problem (SVP), Closest Vector Problem (CVP) and Learning with Error (LWE), are known to be hard on the worst case even under quantum situation. Since lattice problems can resist post-quantum attack and all known attacks, the encryption schemes based on lattice problem, namely lattice based encryption, can effectively ensure the security of sensitive data in cloud storage to resist quantum algorithm attack. Lattice based encryption also holds the advantages of asymptotic efficiency, conceptual simplicity and security proofs based on worst-case hardness, and has received extensive attention.

Ajtai *et al.* first introduced lattice based encryption [17]. In their scheme, the authors proved the time to attack the algorithm equals to the time to break the SVP problem, which ensured the security of data. However, their scheme was low efficient, poor practical and had a probability that making error in decryption. Goldreich *et al.* proposed the GGH scheme [18]. In their scheme, the authors put forward an idea about realizing the trapdoor through lattice, which was widely adopted by the other lattice based encryption schemes. GGH scheme could also achieve high efficiency. However, it lacked strict security proof and the ciphertext may leak some information in plaintext. Micciancio proposed a HNF scheme to improve the security of GGH [19]. However, the scheme decreased the efficient because of the high storage cost. Based on the LWE problem, Gentry *et al.* built and standardized the trapdoor functions in lattice based encryption [20]. These trapdoor functions were widely applied in lattice based encryption schemes due to their simple expression. The security of these trapdoor functions has been strictly proved.

The LWE problem is the most common applied problem in lattice based encryption. Lots of schemes rely on the average case hardness of the LWE problem to ensure their security. Regev proposed the LWE problem and an efficient scheme [21] to resist chosen plaintext attack (CPA) and chosen ciphertext attack (CCA). However, the schemes based on the LWE problem may have big storage cost [22], which leads to the computation complexity exceeds the square of the security parameter. Therefore, schemes based on the LWE problem are low efficient, which makes the LWE problem hard to be applied to practice. Wang *et al*. proposed a scheme [23] which can both achieve dynamic and anonymity properties on the base of the LWE problem. Lin *et al.* proposed a traitor tracing scheme [24] based on the LWE problem. Kim *et al.* proposed a collusion-resistance scheme [25] and made a strict proof of the security of the scheme. Stehle *et al.* proposed the Ring Learning With Error problem(R-LWE) [26], then Lyubashevsky *et al.* perfected the definition of R-LWE problem [27]. Their researches changed the range of value to a ring, which is different from the LWE problem. Therefore, the schemes based on R-LWE can decrease the storage cost, which increases the efficiency of schemes based on the LWE problem [28]. In the scheme [29], the authors proposed an anonymous system based on R-LWE problem which could broadcast the messages. Poppelmann proposed a scheme [30] which could ensure high efficiency by reducing the storage cost of ciphertexts. In the scheme [31], the authors replaced the Gaussian noise distribution in the R-LWE problem with a unique binary distribution to increase the efficiency of the performance. Wang *et al.* proposed an IBE scheme [32] based on the R-LWE problem which could resist chosen ciphertext attack.

Despite the advantages of CP-ABE and lattice based encryption, to the best of our knowledge, few contributions have been made to merge two algorithms into one so as to realize fine-grained access control and quantum algorithm attack resistance [33], [34], [35], [36], [37], [38]. Zhang *et al.* proposed a lattice CP-ABE scheme [33], which could only support access policy expressed by and gate tree. The scheme [34] can only support gate tree policy and can only encrypt one bit of message at one time. Also, in their scheme, the authors just simply applied attribute keys to output user's secret keys, which made it impossible for the user to revoke his attributes. The scheme [35] applies R-LWE problem to construct all components of ciphertexts and secret keys, which largely decreases the coefficient of error in the decryption phase and increases the failure probability of decryption. Also, the access policy in this scheme is not flexible enough. The scheme [36] costs too much in computation since whole components of secret keys need to be calculated for all combination of attributes. The scheme [37] also has the same problem as the shame [36]. More recently, Li *et al.* proposed a lattice-based CP-ABPRE scheme [38] for Cloud Sharing, in which the authors converted the access policy embedded in the ciphertext by proxy re-encryption. However, the scheme [38] cannot deal with attributes revocation. Most important, the above schemes cannot realize attributes revocation.

1.1 Contributions

In this paper, we propose a revocable lattice attribute-based encryption scheme (RL-ABE) based on R-LWE problem. The contributions of our scheme are as follows:

1) Our RL-ABE scheme can resist the quantum algorithm attack and collusion attack. In our scheme, we first construct some trapdoor functions to generate public/secret key pairs of attributes and secret values, then apply R-LWE problem to merge the CP-ABE structure and propose the whole RL-ABE scheme, which can keep the security of plaintext and secret values in ciphertexts. Later, we make formal proof to ensure the security against quantum algorithm attack.

Besides, our scheme can resist collusion attack among the revoked users, legal users and outside attackers by embedding unique secret value of each user in the secret key components.

2) Our scheme can realize fine-grained access control. Since the lattice based encryption schemes cannot realize fine-grained access control on users' access rights, in this paper, we apply the structure of CP-ABE to distribute attributes to the users and embed attribute policies in the ciphertexts. Only attributes satisfy the access policy, can the users decrypt ciphertexts successfully. Hence, our RL-ABE scheme can flexibly control users' access rights to realize fine-grained access control.

3) Our scheme can realize effective and secure attribute revocation to the users. In our scheme, we distribute the update components to replace relative attribute values and renew users' attributes to dynamic control on users' access rights, which cannot be accomplished by other lattice CP-ABE schemes. Also, the attribute revocation in our scheme can be proved to ensure both effectiveness and security.

2 Preliminaries

2.1 Lattice

Definition 1 (Lattice) [21]. *Let $\{f_1, f_2, \ldots, f_n\}$ be a set of linear independent vectors, where $f_i \in R_p, 1 \leq i \leq n$. The lattice is the set of all integer combinations of the basis of lattice $\{f_1, f_2, \ldots, f_n\}$:$L(f_1, \ldots, f_n)$=$\{\sum_i x_i f_i, x_i \in Z\} \in R_p$.*

Definition 2 [21]. *Let p be a prime, $A \in R_p^m$ and $u \in R_p$. Then $\Lambda(A)$ =$\{u \in R_p | \exists \mathrm{e} \in \mathrm{Z_p^m} \Rightarrow Ae = u \pmod p\}$, $\Lambda^{\perp}(A) = \{e \in Z_p^m | Ae = 0 \pmod p\}$, $\Lambda^u(A) = \{e \in Z_p^m | Ae = u (\bmod p)\}$.*

2.2 Gaussian Distribution on Lattices

Definition 3 (Discrete Gaussian Distribution) [21]. *For any $c > 0$, the Gaussian function centered at $t \in R_p$ with parameter c is $\rho_{c,l}(x) = \exp(-\pi\|x - l\|^2/c^2), x \in R_p$. For a n-dimensional lattice Λ, define $\rho_{c,l}(\Lambda) = \sum_{x\in\Lambda} \rho_{c,l}(x)$, the discrete gaussian distribution on lattices is defined as: $D_{\Lambda,c,l}(x) = \frac{\rho_{c,l}(x)}{\rho_{c,l}(\Lambda)}, x \in \Lambda$.*

Definition 4 (Continuous Gaussian Probability Distribution) [27]. *Let $r > 0$, D_c is the continuous Gaussian probability distribution D_c of width c, given the density $\rho_{c,l}(x) \cdot c^{-n}$.*

Definition 5 (Smooth Parameter) [27]. *For a lattice $\Lambda(A)$ and a positive real $\varepsilon > 0$, the smooth parameter $\mu_\varepsilon(\Lambda)$ is defined as the smallest c such that $\rho_{\frac{1}{c}}(\Lambda^{\perp} \backslash \{0\}) \leq \varepsilon$.*

2.3 Trapdoor Functions [20]

$\mathbf{TrapGen(n, m, p)} \rightarrow \mathbf{(A, T)}$: The function randomly chooses a matrix $A \in R_p^m$, which has n rows and m columns. The function also outputs $T \in \Lambda^{\perp}(A)$=$\{Ae = 0 \pmod p | e \in Z_p^m\}$, where T is the lattices that consists of the integer vectors orthogonal to A.

$\mathbf{SampleD(\Lambda, , c, l)}$: The function is a randomized nearest-plane algorithm that samples from discrete Gaussian $D_{\Lambda,c,l}$. Input a m-dimensional lattice Λ, a parameter $c > 0$ and a center l, in which $c \in Z_p$, $l \in R_p$, the algorithm tries to output the nearest vector in the lattice Λ from center l. In this function, let $v_m = 0$ and $l_m = l$, where m is the number of iterations. Then we can output $l_i' = \frac{<l_i, b_i>}{<b_i, b_i>}$, $c_i = \frac{c}{\|b_i\|}$ and choose a z_i from D_{Z,c_i,l_i}, in which b_i is the ith basis of Λ. Then let $l_{i-1} = l_i - z_i b_i \in Z_p^m$ and $v_{i-1} = v_i + z_i b_i \in Z_p^m$, the function outputs v_0.

$\mathbf{SamplePre(A, T, c, u)} \rightarrow \mathbf{e}$: For $\{Ae = u (\bmod p) | \ e \in Z_p^m\}$, $u \in R_p$, since there is a map $e + \Lambda^{\perp} \rightarrow Ae (\bmod p)$, when we find a l that $Al = u (\bmod p)$, the conditional distribution of e is exactly $l + D_{\Lambda^{\perp},c,-l}$. Therefore, we can sample a v from $SampleD(\Lambda^{\perp}, c, -l)$ and output a small enough $e = l + v$. Since e is small enough, it is hard to find accurate e.

2.4 Ring Learning With Error problem(R-LWE) [27]

For any real $\alpha > 0$, Φ_α is defined as the distribution obtained by sampling from a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$, $\Phi_\alpha(y) = \sum_{k=-\infty}^{+\infty} \frac{1}{\alpha}\exp(-\pi(\frac{y-k}{\alpha})^2)$,$y \in [0, 1)$. For any probability distribution Φ_α, an discrete distribution φ over Z_p can be generated with the random variable $\lfloor p \cdot X_\Phi \rfloor$, in which X_Φ has distribution Φ_α.

Let $v, u_i \in R_p, \chi_i \in \varphi, 1 \leq i \leq m$,$a_i$, χ_i are chosen independently. Giving a list of equations $c_i = {u_i}^T \cdot v + \chi_i$,$1 \leq i \leq m$, the R-LWE problem donates recovering secret value s from these equations. This problem has been proven to be security from existing attacks. For $U = [u_1|u_2| \ldots |u_m] \in R_p^m$,$C_0 = (C_{0,1}, C_{0,2}, \ldots, C_{0,m})$, $\chi = (\chi_1, \chi_2, \ldots, \chi_m) \in R_p^m$, the R-LWE problem can also be donated as $C_0 = U^T v + \chi$.

Definition 6 ($BDD_{\Lambda,\mathbf{d}}$) [27]. *Let Λ be a lattice, $\lambda_1(\Lambda) = \min_{0\neq X\in\Lambda}\|X\|$ be the smallest norm of nonzero vector in Λ and $d < \lambda_1(\Lambda)/2$, the $BDD_{\Lambda,\mathbf{d}}$ problem is: given a z of form $z = y + x$, $y \in \Lambda$ and $\|x\| \leq d$, find y.*

Lemma 1 [20]. *For any prime $p = poly(n)$ and $m \geq 5n \cdot \lesssim^p$, there exists a probabilistic polynomial-time algorithm that inputs m, n, p and outputs matrix $A \in R_p^m$ and full rank matrix $T_A \in \Lambda^{\perp}(A)$. The distribution of A is statistically close to uniform over R_p^m.*

Lemma 2 [20]. *For matrix $A \in R_p^m$ and a fixed $u \in R_p$, there exists an $e \in Z_p^m$ that $Ae = u$. Take full rank matrix $T_A \in \Lambda^{\perp}(A)$ and a real $c \geq \|T_A\| \cdot \omega(\sqrt{\lg^m})$ as input, there exists an algorithm that outputs $e \sim D_{\Lambda^u(A),c}$ as conditional distribution.*

Lemma 3 [21]. *Let $\alpha \in (0, 1)$ be some real and p be a prime such that $\alpha p > 2\sqrt{n}$. Assume there exists an efficient algorithm that can solve the R-LWE problem with Φ_α, then there exists an efficient quantum algorithm for solving the worst case of SVP and CVP problem.*

Lemma 4 [27]. *Let $\phi \in R_p$ such that $\phi \cdot R_p$ is coprime with $< p >$, then the function $\phi : R_p \rightarrow R_p$ define as $\phi(\alpha_i) = \phi \cdot \alpha_i$ induces a isomorphism from R_p to R_p.*

Lemma 5 [27]. *Let Λ be a lattice, σ be an isomorphism mapping R_p to the lattice Λ and $r \geq \sqrt{2} \cdot \mu_\varepsilon(\Lambda)$ for some negligible ε, for z is distributed by $D_{\Lambda,r}$, χ is distributed by $D_{r'}$ with $r' \geq r\|x\|$, then the distribution of $z \cdot x + \chi$ is within negligible statistical distance of Gaussian distribution D_r where $r_i^2 = r^2 \cdot |\sigma_i(x)|^2 + (r')^2$.*

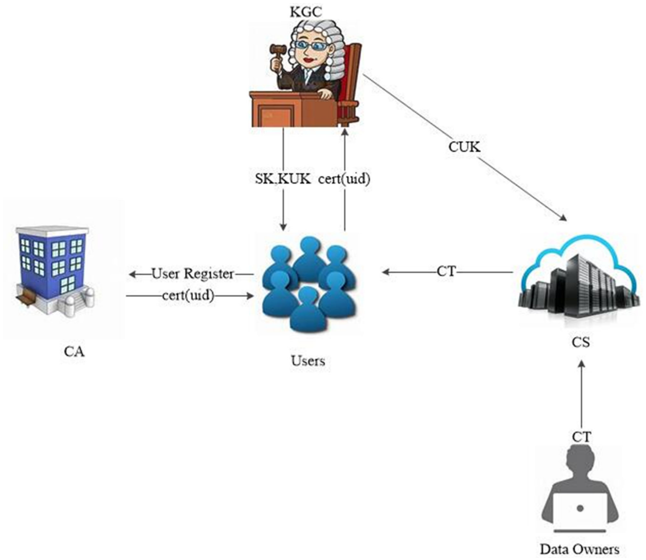

Fig. 1. System model.

TABLE 1
Symbol Explanation

n	a security parameter of our scheme
p	a large prime
m	a parameter in the scheme to run trapdoor function
S	the set of attributes in our scheme
i	the order of one user in all the users of the system
j	the order of one attribute in all the attributes of the system
J	the set of attributes contained in the ciphertext
b	a $n * \eta$ bits of plaintext wrote as a matrix with n rows and η columns
b'	a $n * \eta$ bits decrypted plaintext
$b_{\lambda,\gamma}$	a one bit plaintext on the λ row and γ column of b
S'	The set of attributes need to be revoked

3 Construction of Our Scheme

3.1 System Model

In our scheme, there are five entities: Certificate Authority (CA), Key Generate Center (KGC), Cloud Server (CS), Data Owner and Users, which is illustrated in Fig. 1.

The CA is a global trusted authority in the system. At first, each user need to make register by sending their identity message to the CA. Once confirms the legality of the users, the CA sends corresponding certificates to the users and proves users' identities.

The KGC is an authority that manages users' attributes and secret keys. After receiving the certificates from the users, the KGC assigns the corresponding attributes to the users, and generates users' secret keys. The KGC can also make attributes revocation and renew users' secret keys.

The CS can share a large space to store the ciphertexts of data owners. When the KGC runs attributes revocation, the CS can also receive messages from the KGC to output new ciphertexts.

The data owners can decide access policies by their own. They embed the access policies in their messages to make encryption, then upload the ciphertexts to the CS.

Users can download the ciphertexts from the CS. Only if their attributes satisfy the access policies in the ciphertexts, can they apply their secret keys to decrypt the ciphertexts successfully.

3.2 Threat Model

In our RL-ABE scheme, we define the threat model in terms of the honest but curious CS, trusted KGC, legal users, revoked users and online intruders. First, the CS is honest but curious, which means that it will always execute the instructions correctly but may be curious about the content of the ciphertexts. Second, trusted KGC means that the KGC will always execute the requirements of all entities in the scheme correctly and not curious about the content of the messages.

Third, legal users are the users who have the access right to decrypt ciphertexts. Fourth, revoked users are the users whose attributes are revoked and try to decrypt the ciphertexts they have no right to access to. Finally, the online intruders are the outside attackers who have no secret keys and try to decrypt the ciphertexts. In this paper, the revoked users may collude with legal users or exchange information with each other, and the online intruders may collude with legal users.

3.3 Notation

The explanation of the symbols in our RL-ABE scheme will be shown in the Table 1.

3.4 Details of Our RL-ABE Scheme

In this section, we propose the detail construction of our RL-ABE scheme, which include the five phases: System Initialization, Secret Key Generation, Data Encryption, Data Decryption and Attribute Revocation.

3.4.1 System Initialization

In System Initialization phase, there are four steps which are CASetup, KGCSetup, TrapdoorSetup, and TrapdoorSetup2.

CASetup. Each user sends his identity information to the CA. After making sure that user's identity is legal, CA randomly chooses a $uid \in R_p$ as the unique identity number and outputs the certificate $cert(uid)$.

KGCSetup. The Key Generate Center sets a set of attributes $\{att_1, att_2, \ldots\ldots, att_{|S|}\}$, where $|S|$ is the number of attributes in the scheme. The KGC randomly chooses $g_j, f_j \in Z_p$ for each att_j, then randomly chooses a $u \in R_p^{\eta}$, a $VK_0 \in Z_p$ and outputs $PK_0 = VK_0 \cdot u$, then selects parameter $m \geq 5n \cdot \log p$ Note that m must be an integer multiple of $|S|$, namely $m = \eta|S|$.

TrapdoorSetup. The CA outputs a security parameter n as power of 2 and a large prime $p = 1(\bmod 2n)$, publishes $f(x) = x^n + 1$, ring $R = Z[x]/ < f(x) >$, $R_p = Z_p[x]/ < f(x) >$, a Discrete Gaussian distribution Φ_α with $\alpha \in (0,1)$ and $\alpha p > 2\sqrt{n}$, and a Hash function $H()$ which maps $x \in R_p$ to $H(x) \in Z_p$.

The KGC applies the trapdoor function $TrapGen(n,m,p)$ to generate matrix $A_j \in R_p^m$ and outputs $T_j \in \Lambda(A_j)$, and $PK_j = f_j^{-1} A_j \in R_p^m$ for each att_j. Then, the KGC uses the trapdoor function $TrapGen(n,m,p)$ to generate a matrix $U = [U_1|U_2|\ldots|U_{|S|}] \in R_p^m$ and corresponding full rank matrix $T_U \in \Lambda^{\perp}(U)$, in which each $U_j \in R_p^{\eta}$ is corresponding to the attribute att_j.

TrapdoorSetup2. The KGC randomly chooses a $c \in Z_p$ with the limitation $c \geq \|T_j\| \cdot \omega(\sqrt{\log m})$, and applies the trapdoor function $SamplePre(A_j, T_j, c, U_j)$ to output a $r_j \in Z_p^{m\times\eta}$ so that $A_j \cdot r_j = U_j (\bmod p)$, then the KGC generates $U_i = [U_1'|U_2'|\ldots|U_{|S|}'] \in R_p^m$ and T_{U_i} according to users' attributes $U_j' = U_j, j \in S_i \cap J$, $U_j' = 0 \in R_p^{\eta}, j \notin S_i \cap J$, then applies the trapdoor function $SamplePre(U_i, T_{U_i}, c, u)$ to generate $e = (e_1, e_2, \ldots, e_{|S|})$ with the limitation $c \geq \|T_U\| \cdot \omega(\sqrt{\log m})$.

3.4.2 Secret Key Generation

In Secret Key Generation phase, there is only KeyGen step as follows:

KeyGen. Users send their $cert(uid)$ to the KGC to make registrations. For user i, the KGC manages his/hers attributes, then randomly chooses a $t_i \in Z_p$ to generate $\{SK_{j,1} = H(uid)^{-1} \cdot g_j \cdot r_j \cdot t_i, j \in S_i\}$, in which S_i is the set of attributes the user i own. Then, the KGC outputs $SK_{j,2} = H(uid) g_j^{-1} f_j e_j \cdot VK_0 t_i^{-1}, j \in S_i$, combines the two components to get $SK = \{SK_{j,1}, SK_{j,2}\}$.

3.4.3 Data Encryption

In Data Encryption phase, there is only Encryption step as follows:

Encryption. Let $b = (b_1, \ldots, b_\eta)$, where $b_\lambda = (b_{\lambda,1}, \ldots, b_{\lambda,\gamma}, \ldots, b_{\lambda,n})^T$, in which $b_{\lambda,\gamma}$ is 0 or 1, $1 \leq \lambda \leq \eta$,$1 \leq \gamma \leq n$. The data owner decides an access policy A of valid attributes by defining a linear secret sharing matrix $L \in Z_p^{n\times m}$, in which the jth column corresponding to the att_j. Then the data owner decides the $s \in Z_p$ as the secret value of the linear secret sharing matrix, and sets $v = (s, d_1, \ldots, d_{n-1}) \in Z_p^n$, where $d_1, \ldots, d_{n-1} \in Z_p$ are randomly chosen. Note that there exists a set of constant number $\{\omega_1, \omega_2, \ldots, \omega_{|S_i \cap J|}\}$ that satisfy $\sum_{j\in S_i\cap J} \omega_j L_j = (1, 0, 0, \ldots, 0)$ if $S_i \cap J$ satisfy the requirement of access policy A. Then the data owner randomly chooses $a \in R_p$, $\chi \in \Phi_\alpha^\eta$ and $\chi_j \in \Phi_\alpha$. Besides, we multiply b with $[\frac{p}{2}]$, so that the value of $b_{\lambda,\gamma}$ is enlarged and the extraction accuracy can be improved with the existence of χ. The ciphertext CT can be written as: $CT = \{C_0 = VK_0 \cdot u \cdot a \cdot s + \chi + b[\frac{p}{2}], C_{j,1} = L_j^T \cdot v, C_{j,2} = f_j^{-1} A_j a + \chi_j, j \in J\}$, where the C_0 is the encrypted plaintext, and $C_{j,1}, C_{j,2}$ are attributes related ciphertext components. Note that the data owner encrypts the $n * \eta$ bits plaintext b to $n * \eta$ bits message C_0 at one time. Finally, data owner uploads the ciphertext CT to the cloud.

3.4.4 Data Decryption

In Data Decryption phase, there are three steps which are TokenGen, One-bit Decryption, and Multi-bit Decryption.

TokenGen. To decrypt the ciphertexts in the cloud, users first need to download the ciphertexts CT, then calculate the token of each attribute $j \in S_i \cap J$, $TK_j = C_{j,2} \cdot SK_{j,1} = (f_j^{-1} A_j a + \chi_{j,2}) \cdot H(uid)^{-1} g_j r_j t_i$. Token TK_j indicates that users have attribute j. Then users can use their tokens to decrypt the ciphertexts.

One-Bit Decryption. For legal users who try to decrypt the ciphertexts CT, they can make bit by bit decryption:

$$
\begin{aligned}
b_{\lambda,\gamma}' &= [C_0]_{\lambda,\gamma} - \left[\left(\sum_{j\in S_i\cap J} C_{j,1}\omega_j\right)\left(\sum_{j\in S_i\cap J} TK_j \cdot SK_{j,2}\right)\right]_{\lambda,\gamma} \\
&= [VK_0 \cdot u \cdot a \cdot s + \chi]_{\lambda,\gamma} + b_{\lambda,\gamma}\left[\frac{p}{2}\right] - \left[\left(\sum_{j\in S_i\cap J} L_j^T \omega_j\right) \cdot v \cdot H(uid)^{-1} \cdot \right. \\
&\left.\left(\sum_{j\in S_i\cap J} (f_j^{-1} A_j a + \chi_{j,2}) \cdot g_j r_j t_i \cdot H(uid) \cdot g_j^{-1} f_j e_j\right) \cdot VK_0 t_i^{-1}\right]_{\lambda,\gamma} \\
&= [VK_0 \cdot u \cdot a \cdot s]_{\lambda,\gamma} + b_{\lambda,\gamma}\left[\frac{p}{2}\right] - \left[VK_0 \cdot a \cdot s\left(\sum_{j\in S_i\cap J} A_j r_j e_j\right)\right. \\
&\left. + \chi - VK_0 \cdot s\left(\sum_{j\in S_i\cap J} \chi_{j,2} r_j e_j\right)\right]_{\lambda,\gamma} \\
&= [VK_0 \cdot u \cdot a \cdot s]_{\lambda,\gamma} + b_{\lambda,\gamma}\left[\frac{p}{2}\right] - \left[VK_0 \cdot a \cdot s\left(\sum_{j\in S_i\cap J} u_j e_j\right) + \chi - \chi'\right]_{\lambda,\gamma} \\
&= [VK_0 \cdot u \cdot a \cdot s + \chi'']_{\lambda,\gamma} + b_{\lambda,\gamma}\left[\frac{p}{2}\right] - [VK_0 \cdot a \cdot su]_{\lambda,\gamma} \\
&= \chi_{\lambda,\gamma}'' + b_{\lambda,\gamma}\left[\frac{p}{2}\right].
\end{aligned}
$$

If $b_{\lambda,\gamma}' < [\frac{p}{4}]$, $b_{\lambda,\gamma} = 0$; else, $b_{\lambda,\gamma} = 1$.

Note that $\chi' = VK_0 \cdot s(\sum_{j\in S_i\cap J} \chi_{j,2} r_j e_j)$ and $\chi'' = \chi - \chi'$ in this equation.

Multi-Bit Decryption. The legal user can decrypt the $n * \eta$ bits ciphertext C_0 together by computing under the one bit decryption process as follows:

$$
b' = C_0 - \begin{bmatrix} \omega_1 & \ldots & \omega_j & \ldots & \omega_{|J|} \end{bmatrix} \cdot \begin{bmatrix} C_{1,1} \\ \ldots \\ C_{j,1} \\ \ldots \\ C_{|J|,1} \end{bmatrix}
\cdot \begin{bmatrix} TK_1 & \ldots & TK_j & \ldots TK_{|J|} \end{bmatrix} \cdot \begin{bmatrix} SK_{1,2} \\ \ldots \\ SK_{j,2} \\ \ldots \\ SK_{|J|,2} \end{bmatrix},
$$

and finally get the $n * \eta$ bits plaintext message b' together.

3.4.5 Attribute Revocation

In Attribute Revocation phase, there are three steps which are UpdateGen, KeyUpdate, and CTUpdate.

UpdateGen. For attributes $j \in S'$ need to be revoked, the KGC randomly chooses a $g_j' \in Z_p$, then outputs $KUK_{j,1} = (g_j' - g_j) r_j H(uid)^{-1} t_i$, $KUK_{j,2} = H(uid)((g_j')^{-1} f_j' - g_j^{-1} f_j) e_j \cdot VK_0 t_i^{-1}$,$j \in S_i \cap S'$ for the user i who has these attributes. Also, the KGC outputs $CUK_j = ((f_j')^{-1} - f_j^{-1}) A_j a + \chi_{j,2}'$, $j \in J \cap S'$.

KeyUpdate. The KGC sends $KUK_{j,1}$ and $KUK_{j,2}$ to the user i, then the user calculates $SK_{j,1}' = SK_{j,1} + KUK_{j,1}$ and $SK_{j,2}' = SK_{j,2} + KUK_{j,2}$,$j \in S'$ to update his secret keys as $SK = \{SK_{j,1}', SK_{j,2}', j \in S' \cap S_i, SK_{j,1}, SK_{j,2}, j \in \overline{S'} \cap S_i\}$.

CTUpdate. The KGC sends $CUK_j, j \in J \cap S'$ to the CS, then the CS outputs $C_{j,2}' = C_{j,2} + CUK_j$ to update the ciphertexts as $CT = \{C_0, C_{j,1}, C_{j,2}, j \in J \cap \overline{S'}, C_{j,2}', j \in J \cap S'\}$.

3.5 Correctness

Theorem 1. *The RL-ABE scheme is correct.*

Proof. According to the Lemma 1, since we select $m \geq 5n \cdot \log p$, the trapdoor function $TrapGen(n, m, p)$ with the input m, n, p can output matrix $A \in R_p^m$ that is statistically close to uniform over R_p^m. Therefore, the security of trapdoor function $TrapGen(n, m, p)$ can be ensured.

According to the Lemma 2, since we select $c \geq \|T\| \cdot \omega(\sqrt{\log m})$, with the matrix $A_j, U \in R_p^m$ and fixed $u \in R_p$ as input, the trapdoor function can output $e \sim D_{\Lambda^u(A),c}$ as conditional distribution that $Ae = u$. Therefore, the security of trapdoor functions $SamplePre(A_j, T_j, c, u)$ and $SamplePre\ (U, T_U, c, u)$ can be ensured.

According to the Lemma 3, with $\alpha \in (0, 1)$ and p be a prime, since we select $\alpha p > 2\sqrt{n}$, if there exists an efficient algorithm that can solve the R-LWE problem with Φ_α, then there exists an efficient quantum algorithm for solving the worst case of SVP and CVP problem. Since the SVP and CVP problem can resist quantum algorithm attack, the hardness of R-LWE can be ensured. Therefore, the correctness of the trapdoor functions and security for our secret key generation phase can be ensured.

Since users have $SK_{j,2} = H(uid)g_j^{-1} f_j e_j \cdot VK_0 t_i^{-1}$, token TK_j to each attribute j, and $CT = \{C_0 = VK_0 \cdot u \cdot a \cdot s + \chi + b[\frac{p}{2}], C_{j,1} = L_j^T \cdot v, C_{j,2} = f_j^{-1} A_j a + \chi_j, j \in J\}$, they can finish one-bit decryption as shown in the Section 3.4.4. Finally, users can make correct multi-bit decryption as follows:

$$b' = C_0 - \begin{bmatrix} \omega_1 & \dots & \omega_j & \dots & \omega_{|J|} \end{bmatrix} \cdot \begin{bmatrix} C_{1,1} \\ \dots \\ C_{j,1} \\ \dots \\ C_{|J|,1} \end{bmatrix}$$

$$\cdot \begin{bmatrix} TK_1 & \dots & TK_j & \dots & TK_{|J|} \end{bmatrix} \cdot \begin{bmatrix} SK_{1,2} \\ \dots \\ SK_{j,2} \\ \dots \\ SK_{|J|,2} \end{bmatrix}$$

$$= VK_0 \cdot u \cdot a \cdot s + \chi + b\left[\frac{p}{2}\right] - \left(\sum_{j \in S_i \cap J} L_j^T \omega_j \right) \cdot v \cdot H(uid)^{-1} \cdot$$

$$\left(\sum_{j \in S_i \cap J} (f_j^{-1} A_j a + \chi_{j,2}) g_j r_j t_i \cdot H(uid) g_j^{-1} f_j e_j \right) VK_0 \cdot t_i^{-1}$$

$$= VK_0 \cdot u \cdot a \cdot s + \chi + b\left[\frac{p}{2}\right] - VK_0 \cdot u \cdot a \cdot s - \chi'$$

$$= b\left[\frac{p}{2}\right] + \chi''$$

Note that $\chi' = VK_0 \cdot s(\sum_{j \in S_i \cap J} \chi_{j,2} r_j e_j)$ and $\chi'' = \chi - \chi'$ in this equation.

In addition, the correctness of Attribute Revocation for our RL-ABE scheme can be proved in Theorem 4. □

The Theorem 1 proves that our RL-ABE scheme is correct in all the phases. In all, the correctness of our scheme can be ensured.

4 Security Analysis

4.1 Formal Proof

In this section, we formally prove that our RL-ABE scheme can resist quantum algorithm attack and collusion attack to ensure the security in the post-quantum environment.

Theorem 2. *Let $\alpha \in (0, 1)$, Λ be the lattice in our scheme, and $r \geq \sqrt{2}p \cdot \mu_\varepsilon(\Lambda)$ for some negligible ε, giving a discrete Gaussian distribution $D_{\Lambda,r}$, there is a polynomial time reduction from our RL-ABE scheme to $R - LWE_{p,\Phi_{\leq\alpha}}$ problem since the number field of our RL-ABE scheme meets the requirement, and the norm of error χ can ensure that $\|r_\gamma\| = \|\sqrt{r^2 \cdot |\sigma_\gamma(x)|^2 + (r')^2}\| \leq \alpha$, which can ensure the quantum algorithm attack resistance of our scheme.*

Proof. First, we demonstrate the number field of ciphertext in our RL-ABE scheme are identical to that of R-LWE problem [21]. For the ciphertext CT , in which one component is $C_0 = VK_0 \cdot u \cdot a \cdot s + \chi + b[\frac{p}{2}]$. For $u \in R_p^\eta$, $VK_0 \in Z_p$, $a \in R_p$, $s \in Z_p$ and $\chi \in \Phi_\alpha^\eta$, where $u = [u_1| \dots |u_\eta]$, $\chi = [\chi_1| \dots |\chi_\eta]$, and $u_\gamma \in R_p$, $\chi_\gamma \in \Phi_\alpha$, we can get a set of pairs $(\alpha_\gamma', \beta_\gamma')$ with $a_\gamma' = VK_0 \cdot u_\gamma$ and $\beta_\gamma' = a \cdot s \cdot VK_0 \cdot u_\gamma + \chi_\gamma$. Therefore, each pair has the expression $\beta_\gamma' = \alpha_\gamma' \cdot (a \cdot s) + \chi_\gamma$. Since $VK_0 \in Z_p$ and $u_\gamma \in R_p$, we have $\alpha_\gamma' \in R_p$. Since $a \in R_p$, $s \in Z_p$ and $\chi_\gamma \in \Phi_\alpha$, we have $a \cdot s \in R_p$ and $\beta_\gamma' \in R_p$. Hence, each pair $(\alpha_\gamma', \beta_\gamma')$, $a \cdot s$ and χ_γ meet the number field requirement of R-LWE problem [21].

Then we can try to reduce each pair $(\alpha_\gamma', \beta_\gamma')$ to $BDD_{\Lambda,d}$ problem. Since p is a prime, then $\phi \in R_p$ can ensure that $\phi \cdot R_p$ and $< p >$ are coprimes. Therefore, according to the Definition 6 and the Lemma 4, in a $BDD_{\Lambda,d}$ problem with $d = (\alpha/\sqrt{2} \cdot r)$ for $\alpha_i' \in R_p$, there exists a new sample $z_\gamma \in D_{\Lambda,r}$ such that $z_\gamma = \phi \cdot \alpha_\gamma$. Since $z_\gamma \in D_{\Lambda,r}$, $z_\gamma = y_\gamma + x_\gamma$ with $y_\gamma \in R_p$ and $x_\gamma \leftarrow D_{\alpha/\sqrt{2}}$, we can obtain $\beta_\gamma' = \alpha_\gamma' \cdot a \cdot s + \chi_\gamma' = (z_\gamma \cdot \phi^{-1}) \cdot a \cdot s + \chi_\gamma' = (y_\gamma \cdot \phi^{-1}) \cdot a \cdot s + (x_\gamma \cdot \phi^{-1}) \cdot a \cdot s + \chi_\gamma'$. Therefore, each pair $(\alpha_\gamma', \beta_\gamma')$ can be reduced to $BDD_{\Lambda,d}$ problem.

After substituting the value of α_γ' into β_γ', we can prove that β_γ' accord with the R-LWE problem. Since $y_\gamma \in R_p$, $\phi^{-1} \in R_p$ and $a \cdot s \in R_p$, we can get $(y_\gamma \cdot \phi^{-1}) \cdot a \cdot s \in R_p$. Also, since $a \cdot s \in R_p$, according to Lemma 4, we can have $\phi^{-1} a \cdot s \in D_{\Lambda,r}$. Therefore, since our RL-ABE scheme follow the condition $\|r'\| = \frac{\alpha}{\sqrt{2}} \geq r \cdot \frac{\alpha}{r \cdot \sqrt{2}} = r \cdot |\sigma_\gamma(x)|$ of the Lemma 5, we can obtain that $r_\gamma^2 = r^2 \cdot |\sigma_\gamma(x)|^2 + (r')^2 = r^2 d^2 + (\frac{\alpha}{\sqrt{2}})^2 \leq (r \cdot \frac{\alpha}{r\sqrt{2}})^2 + (\frac{\alpha}{\sqrt{2}})^2 = \frac{\alpha^2}{2} + \frac{\alpha^2}{2} = \alpha^2$, which means $\|r_\gamma\| \leq \alpha$. Therefore, we can know that $(x_\gamma \cdot \phi^{-1}) \cdot a \cdot s + \chi_\gamma' \leftarrow \Phi_\alpha$, which means $\beta_\gamma' = \alpha_\gamma' \cdot (a \cdot s) + \chi_\gamma$ accord with the construction of the R-LWE problem [21]. Since R-LWE problem has been proved to resist quantum algorithm attack [21], we can keep the confidential of $s' = a \cdot s$ under quantum algorithm attack even if the set of pairs $(a_\gamma', \beta_\gamma')$ have been published.

Then we can prove that the confidential of $b_\gamma[\frac{p}{2}]$ can be ensured by $C_{0,\gamma} = a_\gamma' \cdot (a \cdot s) + \chi_\gamma + b_\gamma[\frac{p}{2}]$. After the $b_\gamma[\frac{p}{2}]$ have been added in the expression, we can express the $C_{0,\gamma} = a_\gamma' \cdot (a \cdot s) + \chi_\gamma + b_\gamma[\frac{p}{2}]$ in the set of pairs $(a_\gamma', C_{0,\gamma})$. Since there's just $b_\gamma[\frac{p}{2}] \in R_p$ being added in to get the result $C_{0,\gamma} = \beta_\gamma' + b_\gamma[\frac{p}{2}] \in R_p$, $C_{0,\gamma}$ can still accord with the R-LWE problem. Therefore, we can see that the confidentiality of $s' = a \cdot s$ under quantum algorithm attack can still be ensured. Therefore, the value of the $b_\gamma[\frac{p}{2}]$ in each pair can be kept confidential under quantum algorithm attack, which means the value of b_γ will not be exposed.

Therefore, we can prove that the condition $b = (b_1, \ldots, b_\eta)$ can be ensured. Since $u = [u_1| \ldots |u_\eta]$ and each u_i in u is independent, each $a_\gamma{}' = VK_0 \cdot u_\gamma$ is independent. Also, since $\chi = [\chi_1| \ldots |\chi_\eta]$ and each χ_γ in χ is independent, each $\beta_\gamma{}' = \alpha_\gamma{}' \cdot (a \cdot s) + \chi_\gamma$ is also independent. Clearly, each b_γ in b is independent. Therefore, each $C_{0,\gamma}= \beta_\gamma{}' + b_\gamma[\frac{p}{2}]$ is also independent. Since each $C_{0,\gamma}$ in $C_0 = [C_{0,1}| \ldots |C_{0,\eta}]$ can ensure the security of b_γ, the contents of $b = (b_1, \ldots, b_\eta)$ will not be exposed, which shows that our scheme can keep security against quantum algorithm attack □

The Theorem 2 proves that our scheme can resist quantum algorithm attack. Since our scheme is based on the R-LWE problem which can resist quantum algorithm attack, our scheme can make a polynomial time reduction to the R-LWE problem, which can ensure the quantum algorithm attack resistance.

Theorem 3. *Our RL-ABE scheme can resist the collusion attack between revoked users and legal users, the collusion attack between online intruders and legal users, and the collusion attack between revoked users.*

Proof. When generating the secret keys of users, the KGC randomly chooses a unique t_i for each user i, then binds it with some components $SK_{j,1} = H(uid)^{-1} g_j r_j t_i$, $SK_{j,2} = H(uid) g_j^{-1} f_j e_j VK_0 t_i^{-1}$ with user i's secret key. Besides, the KGC keeps each t_i in private. Therefore, even if one revoked user k achieves the valid secret key of user i, he/she cannot replace the t_i with t_k to get the valid secret key. Therefore, our RL-ABE scheme can resist the collusion attack between revoked users and legal users.

Also, the private and unique t_i, which is bound in components $SK_{j,1}$, $SK_{j,2}$ of each user i's secret keys, cannot be replaced even if the online intruders achieves the valid secret key of user i. Therefore, the online intruders cannot forge users' secret keys even if the intruders collude with legal users or intercept their message to achieve their secret keys. Therefore, our RL-ABE scheme can resist the collusion attack between online intruders and legal users.

There exists a $e_M = (e_1, e_2, \ldots, e_{|S|})$ corresponding to the attributes of each user i. The KGC uses the trapdoor function $SamplePre(U_M, T_{U_M}, c, u)$ to output different e_M and generates secret keys. Even if different users i and k try to union their attribute sets to satisfy the requirement of the access policy, since the matrix U and T_U are kept in secret, they cannot get the correct U_M to output the correct e_M corresponding to the union their attribute sets. Also, their own e_M are invalid. Therefore, two revoked users cannot collude together to union their attribute sets to output a valid secret key. Therefore, our RL-ABE scheme can resist the collusion attack between revoked users.

In all, our RL-ABE scheme can resist the collusion attack between revoked users and legal users, the collusion attack between online intruders and legal users, and the collusion attack between revoked users. □

TABLE 2
Security Comparison

	Collusion-resistance	Secure Attribute Revocation	Quantum algorithm-resistance
Scheme [11]	×	×	×
Scheme [25]	√	×	√
Scheme [33]	×	×	√
Scheme [34]	√	×	√
Scheme [35]	√	×	√
Scheme [36]	×	×	√
Our RL-ABE	√	√	√

The Theorem 3 shows that neither revoked users nor online intruders can threaten the security of our scheme even if they can achieve legal users' secret keys. Therefore, our RL-ABE scheme can resist collusion attacks among revoked users, legal users, and online intruders.

Theorem 4. *Our RL-ABE scheme can make correct, effective and secure attribute revocation.*

Proof. For the attribute j needs to be revoked, we will change their corresponding attribute parameters f_j, g_j to new values $f_j{}', g_j{}'$. Therefore, the corresponding secret key components will be renewed to $SK_{j,1}{}' = H(uid)^{-1} g_j{}' r_j t_i$, $SK_{j,2}{}' = H(uid)(g_j{}')^{-1} f_j{}' e_j VK_0 t_i^{-1}$ and the corresponding ciphertexts components will be renewed to $C_{j,2}{}' = (f_j{}')^{-1} A_j a + \chi_{j,2}{}'$. These components can successfully output the $TK_j{}' = C_{j,2}{}' \cdot SK_{j,1}{}' = ((f_j{}')^{-1} A_j a + \chi_{j,2}{}') H(uid)^{-1} g_j r_j t_i$, then users can calculate the result of $b' = C_0 - (\sum_{j \in J \cap S_i} C_{j,1} \omega_j)(\sum_{j \in J \cap S_i} TK_j \cdot SK_{j,2}) = VK_0 \cdot u \cdot a \cdot s + b[\frac{p}{2}] - VK_0 \cdot s (\sum_{j \in J \cap S_i} u_j e_j) a + \chi'$. Therefore, as long as the set of attributes satisfied the policy, our scheme can ensure the correctness of the decrypt. For the users who have the attribute j been revoked, they cannot output $TK_j{}' = C_{j,2}{}' \cdot SK_{j,1}{}'$, which ensure the effective of the attribute revocation of our scheme.

Besides, the key update components $KUK_{j,1} = (g_j{}' - g_j) r_j H(uid)^{-1} t_i$, $KUK_{j,2} = H(uid) \cdot ((g_j{}')^{-1} f_j{}' - g_j^{-1} f_j) \cdot e_j VK_0 t_i^{-1}$ are bound by t_i, which is uniquely granted to user i and kept secret by the KGC. Therefore, even if revoked users and online intruders can achieve other users' key update components, they cannot replace t_i to their own secret parameters and output their attribute secret key components, which means that the online intruding attacks or collusion attacks can be resisted. Therefore, our scheme can ensure secure attribute revocation.

In all, our RL-ABE scheme can ensure the correctness, effectiveness and security of attribute revocation. □

The Theorem 4 shows that our RL-ABE scheme can make correct and effective attribute revocation. The revocation period can also resist the online intruding attacks or collusion attacks, which ensure the security of attribute revocation in our scheme.

4.2 Security Comparison

In this section, we compare the security of our RL-ABE scheme with other schemes [11], [25], [33], [34], [35], [36] in Table 2. The comparison is under the security goals of

TABLE 3
Storage Cost

	KGC	User	Data Owner	CS
Scheme [11]	$(\lvert S\rvert + 2\lvert i\rvert + 3) \cdot \log p$	$(2\lvert K\rvert + \lvert S_i\rvert) \cdot \log p$	$(3\lvert K\rvert + (n+3)\lvert J\rvert + 3) \cdot \log p$	$(4\lvert J\rvert + 3 + k) \cdot \log p$
Scheme [25]	$((2mn + 2m^2)\lvert i\rvert + 5) \cdot \log p$	$2m^2 \log p$	$(2n + 2mn + 2m^2) \cdot \log p$	$\lvert i\rvert \cdot (mn + k) \cdot \log p$
Scheme [33]	$((2\lvert S\rvert + 1)mn + m^2 + kn)\cdot \log p$	$k(\lvert S\rvert + 1) \cdot \log p$	$(2\lvert J\rvert mn + n + k) \cdot \log p$	$((\lvert S\rvert + \lvert J\rvert)m + k) \cdot \log p$
Scheme [34]	$(3mn + (\lvert S\rvert \cdot p + 1) \cdot n + m^2)\cdot \log p$	$k \cdot m \cdot \log p$	$(3mn + (\lvert S\rvert \cdot p + 1 + k\lvert S\rvert)\cdot n)\cdot \log p$	$(1 + 2m) \cdot k \cdot \log p$
Scheme [35]	$(3\lvert S\rvert + 3) \cdot n \cdot \log p$	$(n + \lvert S\rvert \cdot n) \cdot \log p$	$(n\lvert S\rvert + 2n + mn + m) \cdot \log p$	$(n + \lvert S\rvert \cdot n) \cdot k \cdot \log p$
Scheme [36]	$((2mn + m^2)\lvert S\rvert + 2mn + 2m) \cdot \log p$	$2(\lvert S\rvert(\lvert S\rvert - 1)m^2)\cdot \log p$	$(mn\lvert S\rvert + n + 4m^2) \cdot \log p$	$(2m + (1+m)\lvert S\rvert) \cdot \log p$
Our RL-ABE	$(mn + n * \eta + m^2 + mn\lvert S\rvert + (\lvert i\rvert + 3)n) \cdot \log p$	$(1 + n * \eta)\lvert S_i\rvert\cdot \log p$	$(m\lvert J\rvert + mn + \eta + 1) \cdot \log p$	$(n * \eta + (1+m)\lvert J\rvert)\cdot \log p$

Collusion-resistance, Security Revocation and Quantum algorithm-resistance. According to the Table 2, our RL-ABE scheme can realize all of the security goals mentioned above, while other schemes cannot. Note that "$\surd$" means to have the ability, and "$\times$" means to not.

5 Performance Analysis

5.1 Storage Cost

In this section, we compare the storage cost of the CP-ABE scheme [11], lattice-based encryption scheme [25], lattice based CP-ABE scheme [33], [34], [35], [36], and our RL-ABE scheme in Table 3. In Table 3, $|S|$ represents the number of attributes in the system, $|S_i|$ represents the number of attributes of user i, $|J|$ represents the number of attributes related to the ciphertext, $|i|$ represents the number of users in the system in the scheme, $|K|$ represents the number of distributed KGCs in the scheme and k represents the bits of plaintexts that are encrypted once in the scheme [11], [25], [33], [34].

KGC. The KGC needs to store the public keys, public parameters and master secret keys. As shown in Table 3, the storage cost of KGC in our scheme is less than that in scheme [25], [33], [34], [36].

Also, as shown in Table 3, the storage cost of KGC in our scheme is larger than that in scheme [11], [35].

User. Users need to store their secret keys. As shown in Table 3, we can know $|S_i| < |S|$, the users storage cost in our scheme is less than that in scheme [25], [33], [34], [36].

Also, as shown in Table 3, the users storage cost in our scheme is larger than that in scheme [11], [35].

Data Owner. Data owners need to store their access policies, messages and some parameters. As shown in Table 3, the data owner storage cost in our scheme is less than that in scheme [25], [33], [34], [36].

Also, as shown in Table 3, the data owner storage cost in our scheme is larger than that in scheme [11], [35].

CS. The CS needs to store the ciphertexts. As shown in Table 3, the storage cost for CS in our scheme is less than that in scheme [25], [33], [34], [35], [36].

Also, as shown in Table 3, the storage cost for CS in our scheme is larger than that in scheme [11].

5.2 Communication Cost

In this section, we compare the communication cost for our RL-ABE scheme with the scheme [11], [25], [33], [34], [35], [36] in Fig. 2. Since the communication cost of each scheme is mainly decided by the ciphertexts, we apply the length of ciphertexts to represent the communication cost for each scheme and compare them when the length of ciphertexts message is the integer multiple of 512 bits, from 512 bits to 16896 bits. Also, we set $n = 128$, $p = 257$, $m = 6n\lceil\log p\rceil$, $|S| = 100$, $|J| = 50$ and $|i| = 120$. The results are shown in the Fig. 2.

Note that, in scheme [36], the algorithm can encrypt $2m$ bits of messages at a time, and in our scheme, we can encrypt $n^*\boldsymbol{\eta}$ bits of messages at a time, the communication cost of the two schemes will not change when the length of message l does not change the range of $\lfloor\frac{l}{2m}\rfloor$ and $\lfloor\frac{l}{n\eta}\rfloor$. Therefore, the curves of the scheme [36] and our scheme contain phased fold lines.

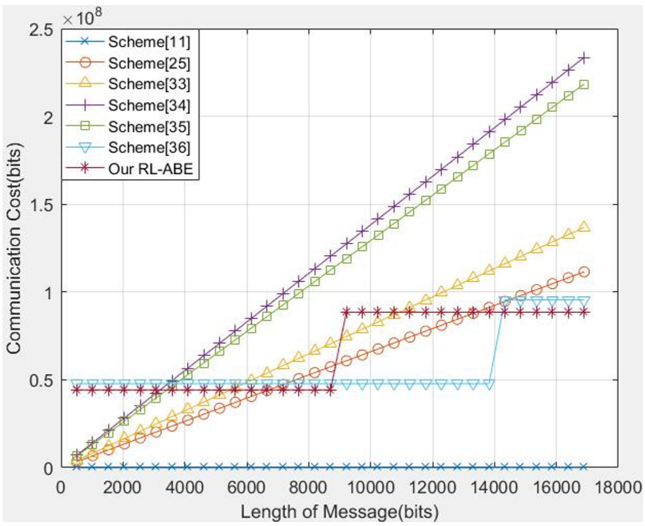

Fig. 2. The comparison of communication cost.

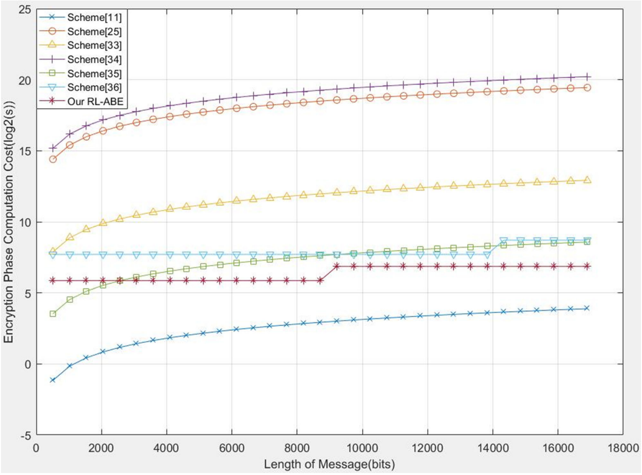

Fig. 3. Computation cost for encryption.

As shown in Fig. 2, we can see that the communication cost in our RL-ABE scheme is at the same order of magnitude with scheme [36]. The reason is that the length of ciphertexts need to be transported in our scheme is at the same order of magnitude with scheme [36].

When the length of plaintext is long enough, the communication cost of our RL-ABE scheme is less than that of scheme [11], [25], [33], [34], [35].

5.3 Computation Cost

In this section, we compare the computation cost for our RL-ABE scheme with the scheme [11], [25], [33], [34], [35], [36] in Figs. 3 and 4, respectively. Since the encryption and decryption computation cost for each scheme is related to the ciphertexts, we apply encryption and decryption time depending on the length of ciphertexts to represent the computation cost for each scheme, and compare them when the length of ciphertexts message is the integer multiple of 512 bits, from 512 bits to 16896 bits. Also, we set n=128, $p = 257$, $m = 6n[\log p]$, $|S| = 100$, $|J| = 50$, $|S_i \cap J| = 10$, $|K| = 20$ and $|i| = 120$. The results are shown in the Figs. 3 and 4, respectively.

Note that the unit of y-axis is log2(s) because the computation cost for scheme [25] and [34] at encryption phase, and the computation cost for scheme [25] and [36] at decryption phase are beyond an order of magnitude for other schemes. Also, in scheme [36], the algorithm can encrypt $2m$ bits of messages at a time, and in our scheme, we can encrypt $n^*\boldsymbol{\eta}$ bits of messages at a time. The computation cost for the two schemes will not change when the length of message l holds the range from $\lfloor \frac{l}{2m} \rfloor$ to $\lfloor \frac{l}{n\eta} \rfloor$. Therefore, the curves of the scheme [36] and our scheme contain phased fold lines.

5.3.1 Computation Cost for Encryption

As shown in Fig. 3, we can see that the computation cost for encryption in our RL-ABE scheme is less than that in scheme [25], [33], [34], [35], [36].

Also, as shown in Fig. 3, the computation cost for encryption in our RL-ABE scheme is larger than that in scheme [11].

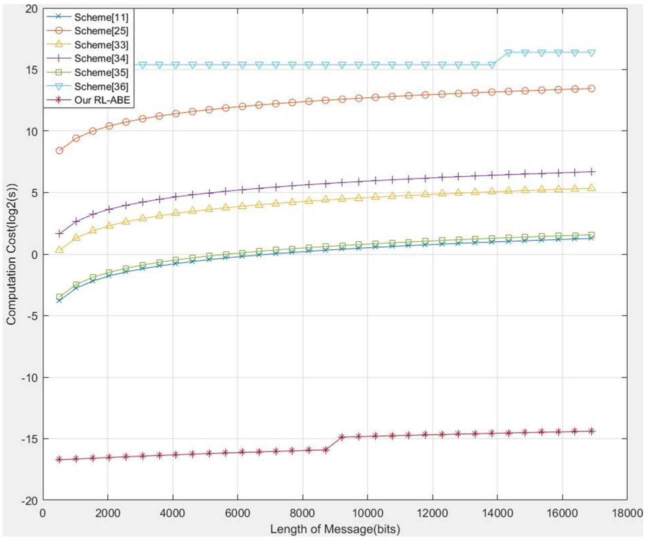

Fig. 4. Computation cost for decryption.

5.3.2 Computation Cost for Decryption

As shown in Fig. 4, we can see that the computation cost for decryption in our RL-ABE scheme is less than that in scheme [36]. The reason is that the size of secret key components related to attributes in scheme [36] is larger than that in our scheme.

As shown in Fig. 4, when the length of plaintext is long enough, the computation cost for decryption in our RL-ABE scheme is less than that in scheme [11], [25], [33], [34], [35].

6 Conclusion

In this paper, we propose a revocable lattice-based CP-ABE scheme RL-ABE, which is based on the hardness of R-LWE problem. Our RL-ABE scheme can both resist quantum algorithm attack and realize fine-grained access control over users' access right through renewing their access right with secure attribute revocation. Our scheme can be formally proved to resist quantum algorithm attack and withstand collusion attack. In addition, the performance analysis demonstrates that our scheme can ensure high efficiency.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (NO.61372103), Key Project of Chinese National Programs for Fundamental Research and Development (NO.2013CB338003), Key Lab of Information Network Security of Ministry of Public Security (C19607) and Key Laboratory of Computer Network Technology of Jiangsu Province. Rui Jiang is a co-first author.

Reference

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptogr. Techn.*, 1984, pp. 47–53.
[2] A. Sahai and B. Waters,"Fuzzy identity-based encryption," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2005, pp. 457–473.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[4] V. Goyal *et al.*, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[5] Y. Zhang, X. Chen, J. Li, H. Li, and F. Li, "Attribute-based data sharing with flexible and direct revocation in cloud computing," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 11, pp. 4028–4049, 2014.

[6] X. Liang, R. Lu, and X. Lin, "Ciphertext policy attribute based encryption with efficient revocation," in *Proc. IEEE Symp. Security Privacy*, 2010, pp. 321–334.

[7] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute based systems," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 99–112.

[8] P. K. Tysowski and M. A. Hasan, "*Hybrid attribute-based encryption and re-encryption for scalable mobile applications in clouds*," *IEEE Trans. Cloud Comput.*, vol. 1, no. 2, pp. 172–186, Jul.-Dec. 2013.

[9] J. Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 10, pp. 2271–2282, Oct. 2013.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[11] K. Yang, X. Jia, and K. Ren, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, Jul. 2014.

[12] X. F. Huang, Q. TAO, B. D. Qin, and Z. Q. Lin, "Multi-authority attribute based encryption scheme with revocation," in *Proc. IEEE 24th Int. Conf. Comput. Commun. Netw.*, 2015, pp. 1–5.

[13] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1767–1777, Jun. 2017.

[14] S. C. Chang and J. L. Wu, "A Privacy-preserving cloud-based data management system with efficient revocation scheme," in *Proc. IEEE Int. Conf. Parallel Distrib. Comput. Appl. Technol.*, 2017, pp. 1–8.

[15] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Trans. Serv. Comput.*, vol. 10, no. 5, pp. 785–796, Sep.-Oct. 2017.

[16] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

[17] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.

[18] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *Proc. 17th Annu. Int. Cryptol. Conf.*, 1997, pp. 112–131.

[19] D. Micciancio, "Improving lattice based cryptosystems using the hermite normal form," in *Proc. Int. Conf. Cryptogr. Lattices*, 2001, pp. 126–145.

[20] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 40th Annu. ACM Symp. Theory Comput.*, 2008, pp. 197–206.

[21] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annu. ACM Symp. Theory Comput.*, 2005, pp. 84–93.

[22] S. Ling, D. H. Phan, and D. Stehlé, "Hardness of k-LWE and applications in traitor tracing," *Algorithmica*, vol. 156, no. 1, pp. 1–35, 2014.

[23] F. Wang, X. Wang, C. Wang, "Lattice-based dynamical and anonymous broadcast encryption scheme," in *Proc. IEEE Int. Conf. P2P Parallel Grid Cloud Internet Comput.*, 2016, pp. 853–858.

[24] S. Ling *et al.*, "Hardness of k-LWE and applications in traitor tracing," *Algorithmica*, 156, no. 1, PP. 1–35, 2014.

[25] K. S. Kim and I. R. Jeong, "Collusion-resistant unidirectional proxy re-encryption scheme from lattices," *J. Commun. Netw.*, vol. 18, no. 1, pp. 1–7, 2016.

[26] D. Stehle, R. Steinfeld, K. Tanaka, and K. Xagawa, "Efficient public key encryption based on ideal lattices," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*, 2009, vol. 5912, pp. 617–635.

[27] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2010, pp. 1–23.

[28] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," in *Proc. Int. Conf. Topics Cryptol.: Ct-Rsa*, 2011, pp. 319–339.

[29] A. Georgescu, "Anonymous lattice-based broadcast encryption," in *Proc. Inf. Commun. Technol. EurAsia Conf.*, 2013, pp. 353–362.

[30] T. Pöppelmann and T. Güneysu, "Towards practical lattice-based public-key encryption on reconfigurable hardware," in *Proc. Int. Conf. Sel. Areas Cryptography*, 2013, pp. 68–85.

[31] T. Wang *et al.*, "Efficient chosen-ciphertext secure encryption from R-LWE," in *Proc. Int. Conf. Wireless Personal Commun.*, 2017, pp. 1–16.

[32] J. Buchmann *et al.*, "High-performance and lightweight lattice-based public-key encryption," in *Proc. 2nd ACM Int. Workshop IoT Privacy Trust Security*, 2016, pp. 2–9.

[33] J. Zhang and Z. Zhang, "A ciphertext policy attribute-based encryption scheme without pairings," in *Proc. Int. Conf. Inf. Security*, 2011, vol. 7537, pp. 324–340.

[34] Y. Wang, "Lattice ciphertext policy attribute-based encryption in the standard model," *Int. J. Netw. Security*, vol. 16, no. 6, pp. 444–451, 2014.

[35] S. F. Tan and A. Samsudin, "Lattice ciphertext-policy attribute-based encryption from ring-LWE," in *Proc. IEEE Int. Symp. Technol. Manage. Emerg. Technol.*, 2015, pp. 258–262.

[36] J. Zhao and H. Gao, "LSSS Matrix-Based Attribute-Based Encryption on Lattices," in *Proc. IEEE Int. Conf. Comput. Intell. Security*, 2018, pp. 253–257.

[37] X. Liu *et al.*, "Threshold attribute-based encryption with attribute hierarchy for lattices in the standard model," *IET Inf. Security*, vol. 8, no. 4, pp. 217–223, 2014.

[38] Li Juyan, C. Ma, and K. Zhang, "A novel lattice-based CP-ABPRE scheme for cloud sharing," *Symmetry*, vol. 11, no. 1262, pp. 32–46, 2019.

Siyu Zhao is currently working toward the graduate degree with the School of Information Science and Engineering, Southeast University, Nanjing, China. His research interests include data access control, data sharing protocol, and data integrity verification in cloud environments.

Rui Jiang received the PhD degree from Shanghai Jiaotong University, Shanghai, China, in 2005. He is currently an associate professor with Southeast University, China. His current research interests include secure analysis and design of communication protocols, secure cloud computing and big data, secure network and systems communications, mobile voice end-to-end secure communications, and applied cryptography.

Bharat Bhargava (Fellow, IEEE) is currently a professor of computer science with Purdue University. He is conducting research in security and privacy issues in distributed systems and sensor networks. This involves identity management, secure routing and dealing with malicious hosts, adaptability to attacks, and experimental studies. His recent work involves attack graphs for collaborative attacks. He has won five best paper awards in addition to the technical achievement award and golden core award from IEEE.