

Qos Aware Secure Data Storage and Revocation Mechanism in Cloud Computing

¹, Gayathri.M, ² Amutha.A

¹, M.E. Student, Department of Computer Science and Engineering ,P.S.R Engineering college, Anna University, Chennai.

²Associate Professor, Department of Information Technology, Anna University, Chennai.

Abstract—Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

Index Terms—Cloud computing, data sharing, revocation, Identity-based encryption, ciphertext update, decryption key exposure.



1 INTRODUCTION

CLOUD computing is a paradigm that provides massive computation capacity and huge memory space at a low cost [1]. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud [2], Microsoft's Azure [3] and Amazon's S3 [4], can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society [5], [6]. However, it also suffers from several security threats, which are the primary concerns of cloud users [7].

Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data.

A natural solution to conquer the aforementioned prob-

lem is to use cryptographically enforced access control such as identity-based encryption (IBE). Furthermore, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals:

- **Data confidentiality:** Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.
- **Backward secrecy:** Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the *subsequently* shared data that are still encrypted under his/her identity.
- **Forward secrecy:** Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be *previously* accessed by him/her.

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographical tool to achieve the above security goals. We also note that there exist other security issues that are equally important for a practical system of data sharing, such as the authenticity and availability of the shared data [8], [9], [10], [11], [12]. But the research on these issues is beyond the scope of this paper.

the aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period. As indicated in Figure 1, a RIBE-based data sharing system works as follows:

- Step 1: The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the ciphertext of the shared data to the cloud server.
- Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.
- Step 3: In some cases, e.g., Alice's authorization gets expired, David can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

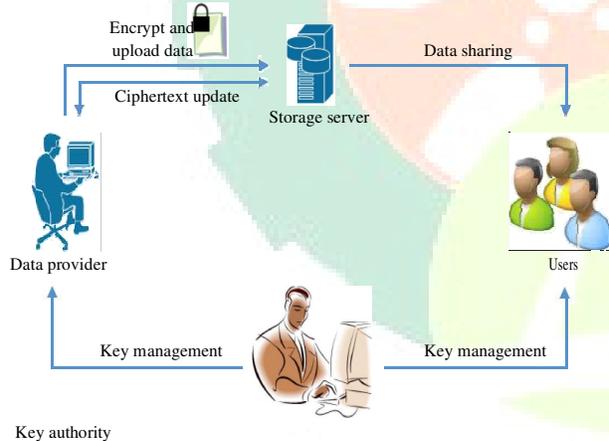


Fig. 1. A natural RIBE-based data sharing system

Obviously, such a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the ciphertext periodically by using secret key.

Another challenge comes from efficiency. To update the ciphertext of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-re-encrypt-upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage. One method to avoid this problem is to require

the cloud server to directly re-encrypt the ciphertext of the shared data. However, this may introduce ciphertext extension, namely, the size of the ciphertext of the shared data is linear in the number of times the shared data have been updated. In addition, the technique of proxy re-encryption can also be used to conquer the aforementioned problem of efficiency. Unfortunately, it also requires users to interact with the cloud server in order to update the ciphertext of the shared data.

1.2 Related work

1.2.1 Revocable identity-based encryption

The concept of identity-based encryption was introduced by Shamir [13], and conveniently instantiated by Boneh and Franklin [14]. IBE eliminates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed. In the traditional PKI setting, the problem of revocation has been well studied [15], [16], [17], [18], [19], and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE.

Boneh and Franklin [14] first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, and non-revoked users periodically received private keys for each time period from the key authority. Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar [20] introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users. However, this scheme only achieves selective security. Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud [21] proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme [22], Chen et al. [23] constructed a RIBE scheme from lattices.

Recently, Seo and Emura [24] proposed an efficient RIBE scheme resistant to a realistic threat called decryption key exposure, which means that the disclosure of decryption key for current time period has no effect on the security of decryption keys for other time periods. Inspired by the above work and [25], Liang et al. [26] introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and ciphertext update. To reduce the complexity of revocation, they utilized a broadcast encryption scheme [27] to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key. However, this kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users. Furthermore, to update the ciphertext, the key authority in their scheme needs to maintain a table for each user to

produce the re-encryption key for each time period, which significantly increases the key authority's workload.

1.2.2 Forward-secure cryptosystems

In 1997, Anderson [28] introduced the notion of forward security in the setting of signature to limit the damage of key exposure. The core idea is dividing the whole lifetime of a private key into T discrete time periods, such that the compromise of the private key for current time period cannot enable an adversary to produce valid signatures for previous time periods. Subsequently, Bellare and Miner provided formal definitions of forward-secure signature and presented practical solutions. Since then, a large number of forward-secure signature schemes [29], [30], [31], [32], [33] has been proposed.

In the context of encryption, Canetti, Halevi and Katz [34] proposed the first forward-secure public-key encryption scheme. Specifically, they firstly constructed a binary tree encryption, and then transformed it into a forward-secure encryption with provable security in the random oracle model. Based on Canetti et al.'s approach, Yao et al. [35] proposed a forward-secure hierarchical IBE by employing two hierarchical IBE schemes, and Nieto et al. [36] designed a forward-secure hierarchical predicate encryption.

Particularly, by combining Boldyreva et al.'s [20] revocation technique and the aforementioned idea of forward security¹, in CRYPTO 2012 Sahai, Seyalioglu and Waters [37] proposed a generic construction of so-called revocable-storage attribute-based encryption, which supports user revocation and ciphertext update simultaneously. In other words, their construction provides both forward and backward secrecy. What must be pointed out is that the process of ciphertext update of this construction only needs public information. However, their construction cannot be resistant to decryption key exposure, since the decryption is a matching result of private key and update key.

1.3 Our contributions

In this paper, we introduce a notion called revocable-storage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfills the three security goals. More precisely, the following achievements are captured in this paper:

- We provide formal definitions for RS-IBE and its corresponding security model;
- We present a concrete construction of RS-IBE. The proposed scheme² can provide confidentiality and backward/forward² secrecy simultaneously;
- We prove the security of the proposed scheme in the standard model, under the decisional ℓ -Bilinear Diffie-Hellman Exponent (ℓ -BDHE) assumption. In addition, the proposed scheme can withstand de-cryption key exposure;
- The proposed scheme is efficient in the following ways:

1. They utilized the idea to provide the forward secrecy of ciphertext, rather than secret key as in the original case.

2. As in [37], our scheme achieves forward security under the assumption that the encrypted data is stored in the cloud and users do not store the encrypted/decrypted data locally.

- The procedure of ciphertext update only need-*s public information*. Note that no previous identity-based encryption schemes in the literature can provide this feature;
- The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by $O(\log(T)^2)$, where T is the total number of time periods.

Outline. The remainder of this paper is structured as follows: In **section 2**, we introduce the preliminaries involved in our construction. Then we present the definitions of RS-IBE in **section 3**, and provide the concrete construction in **section 4**, followed with the corresponding security analysis, performance discussions, and the implementation results of the scheme. Finally, we conclude in **section 5**.

2 PRELIMINARIES

In this section, we first briefly present the basic concepts on bilinear pairing and decisional ℓ -BDHE assumption. Then, an algorithm used to perform efficient revocation is introduced.

2.1 Bilinear pairing and complexity assumption

Definition 1 (Bilinear pairing). Let G_1 and G_2 be two cyclic groups with prime order q , and g be a generator of G_1 . A bilinear pairing is a map $e: G_1 \times G_1 \rightarrow G_2$ with the following properties:

- *Bilinearity:* $e(u^a, h^b) = e(u, h)^{ab}$ for all $u, h \in G_1$, $a, b \in \mathbb{Z}_q^*$.
- *Non-degeneracy:* $e(g, g) \neq 1$.
- *Computability:* There exists an efficient algorithm to compute $e(u, h)$ for any $u, h \in G_1$.

Definition 2 (Decisional ℓ -BDHE Assumption). The decisional ℓ -BDHE problem is formalized as follows. Choose a group G_1 with prime order p according to the security parameter λ .

Select a generator g of G_1 and $a, s \leftarrow \mathbb{Z}_p$, and let $f_i = g^{a^i}$. Provide the vector $\mathbf{f} = (g, g^s, f_1, \dots, f_\ell, f_{\ell+2}, \dots, f_{2\ell})$ and an element $D \in G_2$ to a probabilistic polynomial-time (PPT) algorithm \mathbf{C} , it outputs 0 to indicate that $D = e(g^s, g^{a^{\ell+1}})$, and outputs 1 to indicate that D is a random element from G_2 .

The advantage of \mathbf{C} solving the decisional ℓ -BDHE problem in G_1 is defined as follows:

$$\text{Adv}_{\mathbf{C}}^{\text{decisional } \ell\text{-BDHE}}(\lambda) = \Pr_{\mathbf{C}}(\mathbf{C}(\mathbf{f}, D = e(g^s, g^{a^{\ell+1}})) = 0)$$

We say that the decisional ℓ -BDHE assumption holds in G_1 provided that no PPT algorithm can solve the decisional ℓ -BDHE problem with a non-negligible advantage.

2.2 KUNodes algorithm

Our RS-IBE scheme uses the same binary tree structure introduced by Boldyreva, Goyal and Kumar [20] to achieve efficient revocation. To describe the revocation mechanism, we first present several notations. Denote by ϵ the root node of the binary tree \mathbf{BT} , and $\text{Path}(\eta)$ the set of nodes on the path from ϵ to the leaf node η (including ϵ and η). For a non-leaf node θ , we let θ_l and θ_r stand for its left and right

child, respectively. Given a time period t and revocations list RL , which is comprised of the tuples (η_j, t_j) indicating that the node η_j was revoked at time period t_j , the algorithm $KUNodes(BT, RL, t)$ outputs the smallest subset Y of nodes of BT such that Y contains an ancestor for each node that is not revoked before the time period t .

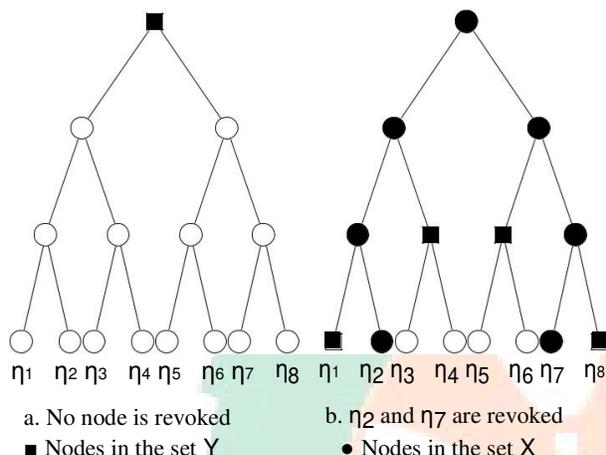


Fig. 2. An instance of the algorithm $KUNodes$

Informally, to identify the set Y , the algorithm first marks all the ancestors of revoked nodes as revoked, then outputs all the non-revoked children of revoked nodes. As an example, we present two instances of the algorithm $KUNodes$ in Figure 2. The formal description is given below.

Algorithm 1 $KUNodes(BT, RL, t)$

```

1:  $X, Y \leftarrow \emptyset$ 
2: for all  $(\eta_j, t_j) \in RL$  do
3:   if  $t_j \leq t$  then
4:     Add Path( $\eta_j$ ) to X
5:   end if
6: end for
7: for all  $\theta \in X$  do
8:   if  $\theta_l \notin X$  then
9:     Add  $\theta_l$  to Y
10:  end if
11:  if  $\theta_r \notin X$  then
12:    Add  $\theta_r$  to Y
13:  end if
14: end for
15: if  $Y = \emptyset$  then
16:   Add the root node  $\epsilon$  to Y
17: end if
18: return Y

```

3 DEFINITION AND SECURITY MODEL OF RS-IBE

In this section, we first provide the formal definition of RS-IBE, and then give the corresponding security model.

3.1 Syntax of RS-IBE

Definition 3 (Revocable-Storage Identity-Based Encryption). A revocable-storage identity-based encryption scheme with

message space M , identity space I and total number of time periods T is comprised of the following seven polynomial time algorithms:

- **Setup** $(1^\lambda, T, N)$: The setup algorithm takes as input the security parameter λ , the time bound T and the maximum number of system users N , and it outputs the public parameter PP and the master secret key $M SK$, associated with the initial revocation list $RL = \emptyset$ and state st .
- **PKGen** $(PP, M SK, ID)$: The private key generation algorithm takes as input $PP, M SK$ and an identity $ID \in I$, and it generates a private key SK_{ID} for ID and an updated state st .
- **KeyUpdate** $(PP, M SK, RL, t, st)$: The key update algorithm takes as input $PP, M SK$, the current revocation list RL , the key update time $t \leq T$ and the state st , it outputs the key update KU_t .
- **DKGen** (PP, SK_{ID}, KU_t) : The decryption key generation algorithm takes as input PP, SK_{ID} and KU_t , and it generates a decryption key $DK_{ID,t}$ for ID with time period t or a symbol \perp to illustrate that ID has been previously revoked.
- **Encrypt** (PP, ID, t, M) : The encryption algorithm takes as input PP , an identity ID , a time period $t \leq T$, and a message $M \in M$ to be encrypted, and outputs a ciphertext $CT_{ID,t}$.
- **CTUpdate** $(PP, CT_{ID,t}, t)$: The ciphertext update algorithm takes as input $PP, CT_{ID,t}$ and a new time period $t \geq t$, and it outputs an updated ciphertext $CT_{ID,t}$.
- **Decrypt** $(PP, CT_{ID,t}, DK_{ID,t})$: The decryption algorithm takes as input $PP, CT_{ID,t}, DK_{ID,t}$, and it recovers the encrypted message M or a distinguished symbol \perp indicating that $CT_{ID,t}$ is an invalid ciphertext.
- **Revoke** (PP, ID, RL, t, st) : The revocation algorithm takes as input PP , an identity $ID \in I$ to be revoked, the current revocation list RL , a state st and revocation time period $t \leq T$, and it updates RL to a new one.

Definition 4 (Correctness of RS-IBE). We say that a RS-IBE scheme is correct provided that, for any $(PP, M SK, RL, st) \leftarrow Setup(1^\lambda, T, N)$, $ID \in I$, $t \leq T$, $M \in M$, all possible states st and a revocation lists RL , if ID is not revoked at time period t , then for $(SK_{ID}, sk) \leftarrow PKGen(PP, M SK, ID)$, $KU_t \leftarrow KeyUpdate(PP, M SK, RL, t, sk)$, $DK_{ID,t} \leftarrow DKGen(PP, SK_{ID}, KU_t)$, and $CT_{ID,t} \leftarrow Encrypt(PP, ID, t, M)$, it is required that:

- If $t \geq t$, then $Decrypt(PP, CT_{ID,t}, DK_{ID,t}) = M$. Otherwise, $Decrypt(PP, CT_{ID,t}, DK_{ID,t}) = \perp$ with all but negligible probability.
- For $t \geq t$, it holds that $CTUpdate(PP, CT_{ID,t}, t) \equiv Encrypt(PP, ID, t, M)$ holds.

Here, \equiv indicates equality in statistical distribution.

3.2 Security model

Definition 5 (IND-RID-CPA). A RS-IBE scheme is IND-RID-CPA secure provided that for any PPT adversary A , it has negligible advantage in the following security game between a challenger C and the adversary A :

- Setup. C performs $Setup(1^\lambda, T, N) \rightarrow (PP, M SK)$ and sends PP to A ;

- Phase 1. **A** makes the following queries in an adaptive way:
 - a. $\mathbf{O}_{SK}(ID)$: **C** performs $\mathbf{PKGen}(P, P, M, SK, ID) \rightarrow (SK_{ID}, st)$ and returns SK_{ID} to **A**;
 - b. $\mathbf{O}_{KU}(t)$: **C** runs $\mathbf{KeyUpdate}(P, P, M, SK, RL, t, st) \rightarrow KU_t$ and returns KU_t ;
 - c. $\mathbf{O}_{DK}(ID, t)$: **C** runs $\mathbf{PKGen}(P, P, M, SK, ID) \rightarrow (SK_{ID}, st)$ and $\mathbf{DKGen}(P, P, SK_{ID}, KU_t) \rightarrow DK_{ID,t}$, then forwards $DK_{ID,t}$ to **A**;
 - d. $\mathbf{O}_{RV}(ID, t)$: **C** updates the current revocation list RL by running $\mathbf{Revoke}(P, P, ID, RL, t, st) \rightarrow RL$ and returns the updated RL to **A**;
- Challenge. **A** signals the query is over and sends $(M_0, M_1, ID^*, t^*, st)$ to **C** subject to the restriction that $M_0, M_1 \in \mathbf{M}$ and $|M_0| = |M_1|$. Then, **C** chooses a random bit $\beta \leftarrow \{0, 1\}$ and returns the challenged ciphertext $CT_{ID^*,t^*} \leftarrow \mathbf{Encrypt}(P, P, ID^*, t^*, M_\beta)$ to **A**;
- Phase 2. **A** begins another query phase as phase 1;
- Guess. **A** outputs a bit β as a guess of β ;

The restrictions explicitly made on **A**'s queries in the game are as follows:

- 1) $\mathbf{O}_{KU}(t)$ and $\mathbf{O}_{RV}(ID, t)$ can only be queried in a sequential order in time. That is, the time t should be greater than or equal to the time of all previous queries;
- 2) $\mathbf{O}_{RV}(ID, t)$ cannot be queried if $\mathbf{O}_{KU}(t)$ was queried;
- 3) If $\mathbf{O}_{SK}(ID^*)$ was queried then $\mathbf{O}_{RV}(ID^*, t)$ must be queried, where $t \leq t^*$;
- 4) $\mathbf{O}_{DK}(ID, t)$ cannot be queried before $\mathbf{O}_{KU}(t)$ was queried;
- 5) $\mathbf{O}_{DK}(ID^*, t^*)$ cannot be queried.

The adversary **A**'s advantage in the above game is defined as

$$\text{Adv}_{\text{RS-IBE,A}}^{\text{IND-CPA}}(\lambda, T, N) = \Pr \beta = \beta - \frac{1}{2}$$

Remark 1. In the security game above, we do not provide a query oracle for the ciphertext update algorithm $\mathbf{CTUpdate}$ since the adversary can run it to a ciphertext just by using the public parameter P, P .

4 RS-IBE RESISTANT TO DECRYPTION KEY EXPOSURE

In this section, we first present a concrete construction of RS-IBE resistant to decryption key exposure, and then discuss its security and performance.

4.1 Construction

Our construction involves two binary trees \mathbf{BT} and \mathbf{T} to manage identity and time period, respectively. More precisely, for identity revocation, we follow Boldyreva et al.'s [20] strategy. That is, given an identity ID , we randomly store it in a leaf node η of \mathbf{BT} , and generate the corresponding secret key $SK_{ID} = \{(\theta, SK_{ID,\theta})\}_{\theta \in \text{Path}(\eta)}$ as in previous RIBE schemes [20], [24]. If the user ID is not revoked at time period t , there exists a node $\theta \in \text{Path}(\eta) \cap \mathbf{KUNodes}(\mathbf{BT}, RL, t)$. Consequently, given the update key $KU_t = \{(\theta, KU_{t,\theta})\}_{\theta \in \mathbf{KUNodes}(\mathbf{BT}, RL, t)}$, the user ID can obtain the decryption key for time period t by re-randomizing and combining $(\theta, SK_{ID,\theta})$ and $(\theta, KU_{t,\theta})$.

However, for a user that is revoked at time period t , there is no such node. As a result, the user cannot decrypt the ciphertext that is produced under its identity after the time period t (including t).

Let $T = 2^t$ be the total number of system time periods.

For each $1 \leq i \leq T$, the time period $t_i \in \{0, 1\}^t$ is associated with the i -th leaf node v_{t_i} of \mathbf{T} . Here, we arrange all leaf nodes of \mathbf{T} in numerical order from left to right. Given a node v of \mathbf{T} , let $b_v \in \{0, 1\}^t$ be the binary sequence corresponding to the path from the root node of \mathbf{T} to v , where 0 and 1 indicate that the path passes through the left and right child of the parent node, respectively. Conversely, given a string $b \in \{0, 1\}^t$, let v_b be the node that has a path b from the root node to it. Furthermore, denote by $b_v[j]$ and $t_i[j]$ the j -th bit of b_v and t_i respectively, and $|b_v|$ the length of b_v .

In addition, for each leaf node v_t of the binary \mathbf{T} , we define the following set: $\mathbf{T}_t = \{v | \text{Parent}(v) \in \text{Path}(v_t), v \in \text{Path}(v_t)\} \cup \{v_t\}$, where $\text{Parent}(v)$ denotes by the parent node of v . As presented in [34], such a set features the following property:

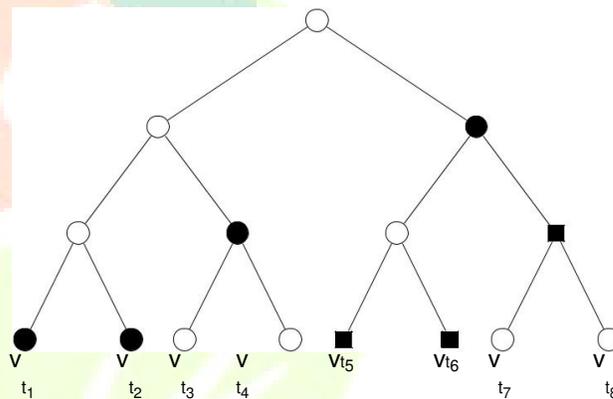


Fig. 3. An example of \mathbf{T} with depth 3

Property 1. Given two time periods t and t' such that $t < t'$, for each node $v \in \mathbf{T}_t$, there exists a node $v' \in \mathbf{T}_{t'}$ such that $b_{v'}$ is a prefix of b_v . In other words, there exists a string $b \in \{0, 1\}^t$ such that $b_v = b_v || b$, where $l = |b_v| - |b|$.

As presented subsequently, the above property enables us to update the ciphertext from time periods t to t' . For explanatory purpose, we give a binary tree with depth 3, which means that the total number of time period is 8. As shown in Figure 3, the leftmost and rightmost leaf nodes v_{t_1} and v_{t_8} correspond to the strings 0^3 and 1^3 respectively. The sets $\mathbf{T}_{t_1} = \{v_1, v_0_1, v_{t_2}, v_{t_1}\}$ and $\mathbf{T}_{t_5} = \{v_{t_1}, v_{t_6}, v_{t_5}\}$.

We present the concrete construction below.

• **Setup**($1^\lambda, T, N$): Given a security parameter λ , the total number of time periods $T = 2^t$, the maximum number of users N , this algorithm performs as follows:

- 1) Choose bilinear groups (G_1, G_2) with prime order $p > 2^\lambda$ and the corresponding bilinear map $e : G_1 \times G_1 \rightarrow G_2$.
- 2) Select group elements $g, g_2 \xleftarrow{R} G_1$ and an integer $\alpha \xleftarrow{R} \mathbb{Z}_p^*$, and set $g_1 = g^\alpha$. Furthermore, pick two random vectors $\mathbf{u} = (u_0, u_1, \dots, u_n) \in G_1^{n+1}$ and $\mathbf{h} = (h_0, h_1, \dots, h_t) \in G_1^{t+1}$, and for each $ID \in I = \{0, 1\}^n$

and $t \in \{0, 1\}^{\ell}$, define the following two functions³:

$$F_u(ID) = \prod_{i=1}^n u_i^{ID[i]}, \quad F_h(t) = \prod_{j=1}^{\ell} h_j^{t[j]}$$

Here, $ID[i]$ is the i th bit of ID .

- Let the master secret key be $M SK = g_2^{\alpha}$, and initialize the state st with a binary tree BT of depth $\log(N)$ and the revocation list $RL = \emptyset$.
- Publish the public parameter as

$$P P = \{G_1, G_2, e, g, g_1, g_2, u, h\}.$$

• **PKGen**($P P, M SK, ID$): For an identity $ID \in I$, this algorithm generates its secret key according to the following way:

- Randomly choose and assign a leaf node η of BT to ID .
- For each node $\theta \in \text{Path}(\eta)$,
 - Recall $g_{\theta,0}$ from BT if it has been defined previously⁴. Otherwise, pick $g_{\theta,0} \leftarrow G_1$, and store the pair $(g_{\theta,0}, g_{\theta,1} = g_2^{r_{\theta,0}})$ in the node θ .
 - Choose $r_{\theta,0} \leftarrow Z_p$, and compute:

$$SK_{ID,\theta} = (SK_{\theta,0}, SK_{\theta,1}) = (g_{\theta,0}^{\alpha} F_u(ID)^{r_{\theta,0}}, g_2^{r_{\theta,0}}).$$

- Update the state as $st = BT$, and then return the secret key

$$SK_{ID} = \{(\theta, SK_{ID,\theta})\}_{\theta \in \text{Path}(\eta)}$$

• **KeyUpdate**($P P, M SK, RL, t, sk$): For each node $\theta \in \text{KUNodes}(BT, RL, t)$, do the following.

- Extract the pre-defined value $g_{\theta,1}$ from BT .
- Choose $r_{\theta,1} \leftarrow Z_p$ and set

$$KU_{t,\theta} = (KU_{\theta,0}, KU_{\theta,1}) = (g_{\theta,1}^{\alpha} \cdot F_h(t)^{r_{\theta,1}}, g_2^{r_{\theta,1}}).$$

- Return

$$KU_t = \{(\theta, KU_{t,\theta})\}_{\theta \in \text{KUNodes}(BT, RL, t)}$$

• **DKGen**($P P, SK_{ID}, KU_t$): If ID was revoked during time period t , return \perp . Otherwise, there exists some node $\theta \in \text{Path}(\eta) \cap \text{KUNodes}(BT, RL, t)$. For this node θ , parse $SK_{ID,\theta} = (SK_{\theta,0}, SK_{\theta,1})$ and $KU_{t,\theta} = (KU_{\theta,0}, KU_{\theta,1})$.

Then, choose $r_0, r_1 \leftarrow Z_p$, compute and return

$$DK_{ID,t} = (DK_{t,1}, DK_{t,2}, DK_{t,3}) \\ = (SK_{\theta,0} \cdot KU_{\theta,0} \cdot F_u(ID)^{r_0} \cdot F_h(t)^{r_1}, SK_{\theta,1} \cdot g_2^{r_0}, KU_{\theta,1} \cdot g_2^{r_1}).$$

• **Encrypt**($P P, ID, t, M$): To encrypt $M \in G_2$ with ID

at time period t , choose $s_t \leftarrow Z_p^*$, select $s_v \leftarrow Z_p^*$ for each node $v \in T_t$. Particularly, let $s_{v_t} = s_t$. Then, set the ciphertext as $CT_{ID,t} = (ID, t, C_0, C_1, C_2, \{C_v\}_{v \in T_t})$, where

$$C_0 = M \cdot e(g_1, g_2)^{s_t}, \quad C_1 = g^{-s_t}, \quad C_2 = F_u(ID)^{s_t},$$

$$C_v = (C_{v,0}, C_{v,|b_v|+1}, C_{v,|b_v|+2}, \dots, C_{v,\ell}) \\ = \prod_{j=1}^{\ell} h_j^{b_v[j] \cdot s_v} \cdot u_j^{s_v}.$$

- We naturally require that $n \leq \log(N)$

4. As indicated in [20], a pseudo-random function can be used to re-compute $g_{\theta,0}$ when necessary instead of having to store it in the node θ

• **CTUpdate**($P P, CT_{ID,t}, t'$): Parse the ciphertext as $CT_{ID,t} = (ID, t, C_0, C_1, C_2, \{C_v\}_{v \in T_t})$, where $C_v = (C_{v,0}, C_{v,|b_v|+1}, C_{v,|b_v|+2}, \dots, C_{v,\ell})$. To update the ciphertext from time period t to $t' \geq t$, do the following:

- For each node $v \in T_t$, find a node $v' \in T_{t'}$ such that $b_{v'}$ is a prefix of b_v .
- Choose $s_{v'} \leftarrow Z_p^*$, select $s_v \leftarrow Z_p^*$ for each node $v \in T_t$. Particularly, let $s_{v_t} = s_t$.
- Compute

$$C'_0 = C_0 \cdot e(g_1, g_2)^{s_{v_t}}, \quad C'_1 = C_1 \cdot q^{-s_{v_t}},$$

$$C'_2 = C_2 \cdot F_u(ID)^{s_{v_t}},$$

$$C'_{v'} = (C_{v',0}, C_{v',|b_{v'}|+1}, C_{v',|b_{v'}|+2}, \dots, C_{v',\ell})$$

$$= C_{v,0} \cdot \prod_{j=|b_v|+1}^{\ell} h_j^{b_v[j] \cdot s_{v'}} \cdot u_j^{s_{v'}}.$$

- Return $CT_{ID,t'} = (ID, t', C'_0, C'_1, C'_2, \{C'_{v'}\}_{v' \in T_{t'}})$.

• **Decrypt**($P P, CT_{ID,t}, DK_{ID,t}$): If $t < t'$ return \perp . Otherwise, update the ciphertext $CT_{ID,t}$ to get $CT_{ID,t'}$, and parse $CT_{ID,t'} = (ID, t', C'_0, C'_1, C'_2, \{C'_{v'}\}_{v' \in T_{t'}})$ and $DK_{ID,t'} = (DK_{t',1}, DK_{t',2}, DK_{t',3})$. Then, return

$$M = C'_0 \cdot e(C'_1, DK_{t',1}) \cdot e(C'_2, DK_{t',2}) \cdot e(C'_{v_t}, DK_{t',3}).$$

• **Revoke**($P P, ID, RL, t, st$): To revoke ID at time period t , update the revocation list by $RL \leftarrow RL \cup \{(ID, t)\}$ and return the updated RL .

CORRECTNESS. We verify the correctness of our scheme as follows: Firstly, given a node $\theta \in \text{KUNodes}(BT, RL, t) \cap \text{Path}(\eta)$, we have that

$$DK_{t,\theta} = (SK_{\theta,0} \cdot KU_{\theta,0} \cdot F_u(ID)^{r_0} \cdot F_h(t)^{r_1}, SK_{\theta,1} \cdot g_2^{r_0}, KU_{\theta,1} \cdot g_2^{r_1}) \\ = (g_2^{\alpha} F_u(ID)^{r_{\theta,0} + r_0} F_h(t)^{r_{\theta,1} + r_1}, g_2^{r_{\theta,0} + r_0}, g_2^{r_{\theta,1} + r_1}).$$

Then, for a ciphertext $CT_{ID,t} = (ID, t, C_0, C_1, C_2,$

$$\{C_v\}_{v \in T_t}), \text{ we note that } C_{v_t,0} = F_h(t)^{s_t}. \text{ Thus, it holds that} \\ C_0 \cdot e(C_1, DK_{t,1}) \cdot e(C_2, DK_{t,2}) \cdot e(C_{v_t,0}, DK_{t,3}) \\ = M \cdot e(g_1, g_2)^{s_t} \cdot e(g^{-s_t}, g_2^{\alpha} \cdot F_u(ID)^{r_{\theta,0} + r_0} \cdot F_h(t)^{r_{\theta,1} + r_1}) \\ \cdot e(F_u(ID)^{s_t}, g_2^{r_{\theta,0} + r_0}) \cdot e(F_h(t)^{s_t}, g_2^{r_{\theta,1} + r_1}) \\ = M \cdot e(g_1, g_2)^{s_t} \cdot e(g^{-s_t}, g_2^{\alpha}) \\ = M.$$

Furthermore, note that the algorithm **CTUpdate** chooses fresh random exponents $\{s_v\}_{v \in T_{t'}}$ to update the original ciphertext $CT_{ID,t}$. Thus, $CT_{ID,t'}$ is not only a valid cipher-text under time period t' , but also is statistically indistinguishable from the output of **Encrypt**($P P, ID, t', M$).

4.2 Security analysis

Theorem 1. If there exists a PPT adversary \mathbf{A} breaking the IND-RID-CPA security of the proposed RS-IBE scheme, then there exists an algorithm \mathbf{C} solving the decisional ℓ -BDHE problem such that

$$\text{Adv}_{\mathbf{C}}^{\ell\text{-BDHE}}(\lambda) \geq \frac{1}{32Tq^2(n+1)} \cdot \text{Adv}_{\text{RS-IBE,A}}^{\text{IND-RID-CPA}}(\lambda)$$

TABLE 1
Comparisons of communication and storage cost with previous works

Schemes	Private key size	Update key size	Ciphertext size
Libert and Vergnaud [22]	$O(\log N) \tau_{G_1}$	$O(r \log N/r) \tau_{G_1}$	$O(1) \tau_{G_1} + O(1) \tau_{G_2}$
Seo and Emura [24]	$O(\log N) \tau_{G_1}$	$O(r \log N/r) \tau_{G_1}$	$O(1) \tau_{G_1} + O(1) \tau_{G_2}$
Liang et al. [26]	$O(1) \tau_{G_1}$	$O(1) \tau_{G_1}$	$O(1) \tau_{G_1} + O(1) \tau_{G_2}$
Our scheme	$O(\log N) \tau_{G_1}$	$O(r \log N/r) \tau_{G_1}^{\dagger}$	$O(\log(T)) \tau_{G_1} + O(1) \tau_{G_2}$

* τ_{G_1} and τ_{G_2} are the sizes of group elements in G_1 and G_2 , respectively. N is the maximum number of system users. r is the number of revoked users. T is the total number of time periods.

\dagger In fact, it is $O(r \log(N/r))$ when $1 \leq r \leq N/2$, and $O(N-r)$ when $N/2 < r \leq N$.

TABLE 2
Comparisons of time complexity with previous works

Schemes	Encryption	Decryption	CTUpdate
Libert and Vergnaud [22]	$O(1)e + O(1)p$	$O(1)p$	0
Seo and Emura [24]	$O(1)e + O(1)p$	$O(1)p$	0
Liang et al. [26]	$O(1)e + O(1)p$	$O(1)p$	$O(N)e + O(1)p$
Our scheme	$O(\log T)e + O(1)p$	$O(1)p$	$O(\log(T))e + O(1)p$

* p and e indicate the cost of performing a bilinear pairing and exponentiation.

TABLE 3
Comparisons of security and functionality with previous works

Schemes	Model	Assumption	PKU	PCU	CA	DKE	FS	BS
Libert and Vergnaud [22]	Adaptive	DBDH	✓	✗	✓	✗	✓	✗
Seo and Emura [24]	Adaptive	DBDH	✓	✗	✓	✓	✓	✗
Liang et al. [26]	Adaptive	DBDH	✗	✗	✗	✓	✓	✓
Our scheme	Adaptive	ℓ -dBDE	✓	✓	✓	✓	✓	✓

* Adaptive means an adaptive-secure model. DBDH is Decisional Bilinear Diffie-Hellman assumption, and ℓ -dBDE is decisional ℓ -Bilinear Diffie-Hellman Exponent assumption. CA is collusion attack. DKE is decryption key exposure. FS and BS indicate forward and backward secrecy, respectively.

Therefore, it holds that

$$\Pr[E] \geq \min_{E_1, E_2, E_3} \Pr[E_1 \wedge (E_{2,1} \wedge E_{2,2} \wedge E_{2,3})]$$

$$\geq \frac{1}{32Tq^2(n+1)}$$

Now, recall that under the condition that C does not abort, if $D = e(g^s, g^{ae+1})$ then C perfectly simulates the experiment, and thus

$$\Pr[C(f, D = e(g^s, g^{ae+1})) = 0] = \text{Adv}_{\text{RS-IBE}, A_2}^{\text{IND-RID-CPA}}(\lambda, T, N) + \Pr[E]$$

However, if D is a random element from G_2 then encrypted message M_g^* is perfectly hidden from the A 's view, and thus

$$\Pr[C(f, D \leftarrow G_2) = 0] = \frac{1}{2} \cdot \Pr[E]$$

By combining the above equalities, we get that

$$\text{Adv}_{\text{IND-RID-CPA}}^{\text{IND-RID-CPA}}(\lambda) = \Pr[C(f, D = e(g^s, g^{ae+1})) = 0] \geq \frac{1}{32Tq^2(n+1)} \cdot \text{Adv}_{\text{RS-IBE}, A}^{\text{IND-RID-CPA}}(\lambda, T, N)$$

This completes the proof. \square

4.3 Performance discussions

In this section, we discuss the performance of the proposed RS-IBE scheme by comparing it with previous works in terms of communication and storage cost, time complexity and functionalities, which are summarized in Table 1, Table 2 and Table 3.

From Table 1 we can see that the sizes of private key and update key in schemes [22], [24] and our scheme are all upper bounded by $O(r \log N/r)$, since these schemes all utilize binary data structure to achieve revocation. On the other hand, Liang et al.'s [26] scheme involves a broadcast encryption scheme to distribute update key such that their scheme has constant sizes of private key and update key. Furthermore, by delegating the generation of re-encryption key to the key authority, the ciphertext size of their scheme also achieves constant. However, to this end, the key authority has to maintain a data table for each user to store the user's secret key for all time periods, which brings $O(T) \tau_{G_1}$

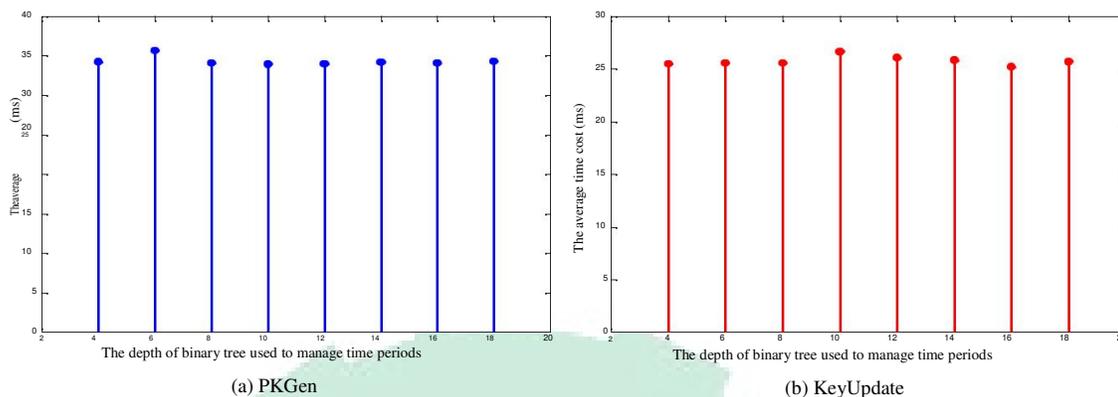


Fig. 5. The time costs of the algorithms **PKGen** and **KeyUpdate**.

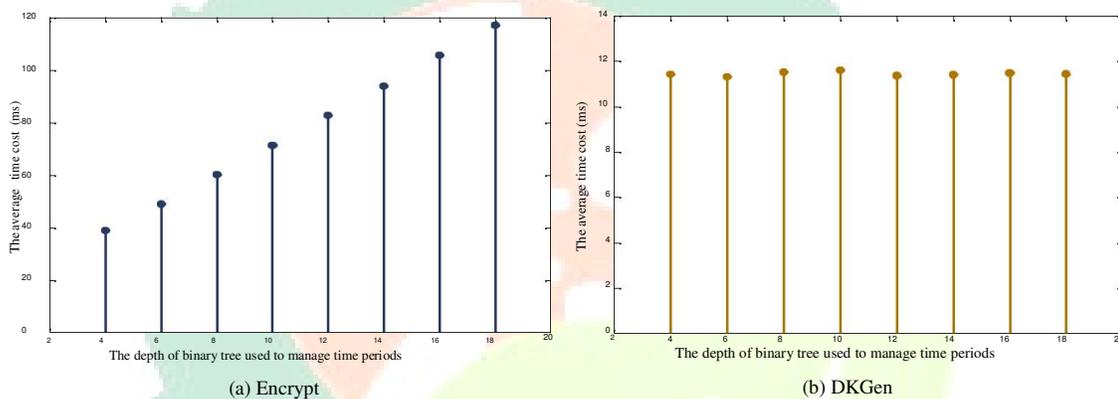


Fig. 6. The time costs of the algorithms **Encrypt** and **DKGen**.

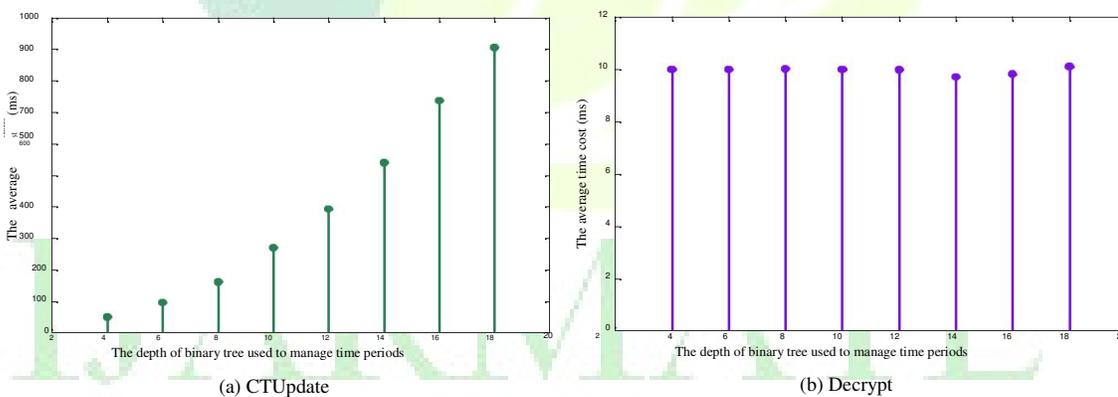


Fig. 7. The time costs of the algorithms **CTUpdate** and **Decrypt**.

storage cost for the key authority. Conversely, the ciphertext size of our scheme is just linear in $\log(T)^2$. In addition, we note that in all listed schemes, the private key generator needs to periodically produce an update key, it must be online if each time period is rather short, e.g., an hour. However, from the perspective of practical applications, the frequency of updating users' decryption keys should not be too small. A time period like a week, half a month or a month is more desirable. As a consequence, the private key generator just needs to produce an update key for the next

period when the current time period is over. Thus the PKG does not need to be always online. Another limitation of these listed schemes is that the generated ciphertext has the size linear with the number of receivers. To overcome this issue, a natural manner is to construct a similar scheme in the setting of broadcast encryption.

On the aspect of time complexity, as illustrated in Table 2, the enumerated schemes all have constant time of

- [13] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptography*. Springer, 1985, pp. 47–53.
- [14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586– 615, 2003.
- [15] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.
- [16] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in *Advances in Cryptology–CRYPTO 1998*. Springer, 1998, pp. 137–152.
- [17] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology– CRYPTO 2001*. Springer, 2001, pp. 41–62.
- [18] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology–EUROCRYPT 2003*. Springer, 2003, pp. 272–293.
- [19] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in *Financial Cryptography and Data Security*. Springer, 2007, pp. 247–259.
- [20] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 417–426.
- [21] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity-based encryption," in *Topics in Cryptology–CT-RSA 2009*. Springer, 2009, pp. 1–15.
- [22] —, "Towards black-box accountable authority ibe with short ciphertexts and private keys," in *Public Key Cryptography–PKC 2009*. Springer, 2009, pp. 235–255.
- [23] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in *Information Security and Privacy*. Springer, 2012, pp. 390–403.
- [24] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in *Public-Key Cryptography–PKC 2013*. Springer, 2013, pp. 216–234.
- [25] —, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in *Topics in Cryptology– CT-RSA 2013*. Springer, 2013, pp. 343–358.
- [26] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Computer Security-ESORICS 2014*. Springer, 2014, pp. 257–272.
- [27] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts," *International journal of information security*, vol. 12, no. 4, pp. 251–265, 2013.
- [28] R. Anderson, "Two remarks on public-key cryptology (invited lecture)," 1997.
- [29] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in *Advances in Cryptology–CRYPTO 1999*. Springer, 1999, pp. 431–448.
- [30] M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," in *Advances in Cryptology–ASIACRYPT 2000*. Springer, 2000, pp. 116–129.
- [31] A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in *Security in communication Networks*. Springer, 2003, pp. 241–256.
- [32] X. Boyen, H. Shacham, E. Shen, and B. Waters, "Forward-secure signatures with untrusted update," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 191–200.
- [33] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forward-secure identity-based signature: security notions and construction," *Information Sciences*, vol. 181, no. 3, pp. 648–660, 2011.
- [34] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Advances in Cryptology–Eurocrypt 2003*. Springer, 2003, pp. 255–271.
- [35] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, "Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption," in *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, 2004, pp. 354–363.
- [36] J. M. G. Nieto, M. Manulis, and D. Sun, "Forward-secure hierarchical predicate encryption," in *Pairing-Based Cryptography–Pairing 2012*. Springer, 2013, pp. 83–101.
- [37] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Advances in Cryptology–CRYPTO 2012*. Springer, 2012, pp. 199–217.
- [38] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology–EUROCRYPT 2005*. Springer, 2005, pp. 114–127.
- [39] B. Lynn. (2014) Pbc library: The pairing-based cryptography library. [Online]. Available: <http://crypto.stanford.edu/pbc/>