A Secure Revocable Identity-Based Proxy Re-encryption Scheme for Cloud Storage

Wei Luo(✉) and Wenping Ma

State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China
rovid008@163.com

Abstract. Identity-based encryption algorithm is applied to cloud storage to protect data security and provide a flexible access control scheme. However, in the existing schemes, the private key generator (PKG) knows secret keys of all users, which means that the PKG can decrypt all ciphertexts. In this paper, we propose a secure identity-based proxy re-encryption scheme, in which the PKG only generates partial secret keys for users. This can ensure users' data confidentiality and privacy security. Its security is based on the decision bilinear Diffie-Hellman (DBDH) assumption in the random oracle model. Besides, our scheme can resist collusion attacks and support user revocation. In addition, we compare our scheme with other existing schemes. The result demonstrates our scheme is comparable with other schemes in computation complexity.

Keywords: Cloud storage · Data security
Identity-based encryption · Proxy re-encryption · Access control

1 Introduction

Cloud storage has been rapidly used in recent years, which makes it possible that users can access and share their data anywhere and anytime just by using mobile devices jointing the Internet. But most of cloud storage systems simply store uploaded data without encryption, which brings a danger that users' data could be leaked due to a malicious attack or operational error by the cloud service provider. It is also desirable that some encryption algorithms and access policies are employed in cloud storage systems.

There are many encryption schemes proposed based on identity-based encryption for cloud storage systems. However, in most scenarios, the private key generator (PKG) issues the full secret keys for users. In this case, the PKG can decrypt all the ciphertext. What's the worse, data leaks can result if other users collude with the PKG or the PKG is compromised by an adversary.

This work was funded by National Key R&D Program of China under grant No. 2017YFB0802400, National Natural Science Foundation of China under grant No. 61373171 and 111 Project under grant No. B08038.

X. Sun et al. (Eds.): ICCCS 2018, LNCS 11064, pp. 519–530, 2018.
https://doi.org/10.1007/978-3-030-00009-7_47

1.1 Our Contribution

To solve this problem, we propose a novel identity-based proxy re-encryption (IB-PRE) scheme by splitting the private key [1]. The main contributions of this paper are the following:

1. In our proposed IB-PRE scheme, the PKG only generates the partial secret keys for users, which can provide the confidentiality of users' data and privacy security. Besides, the PKG does not participate in the generation of re-encryption keys.
2. Authentication is provided in the processes of secret key generation and data access. It ensures that authenticated users can obtain what data they want and that data cannot be intercepted by illegal users.
3. Even if the designated decryptor colluded with the proxy server, the data owner's secret key could not be obtained.

1.2 Organization

The remainder of this paper is organized as follows: Sect. 2 introduces related works on identity-based encryption schemes. The syntax of our identity-based proxy re-encryption scheme, security model and complexity assumption are detailed in Sect. 3. Our scheme is described in detail in Sect. 4. We make a security analysis for our proposed scheme in Sect. 5. Performance analysis is discussed in Sect. 6. Section 7 concludes this paper.

2 Related Work

In 1984, Shamir first proposes identity-based encryption (IBE) in order to achieve the purpose of the simplification of key management system [2]. IBE is an efficient cryptographic system, where the public key can be any string which can uniquely represent the user identity (such as id card number, telephone number and email address, etc.). The secret key is extracted from private key generator (PKG).

In [3], Green et al. propose the concept of IBE proxy re-encryption, which allows the proxy to translate a ciphertext encrypted by the sender's identity into one computed by the recipient's identity. But the size of its re-encrypted ciphertext is so large.

In [4], Matsuo proposes a proxy re-encryption system for IBE, which allows the proxy to translate ciphertext encrypted by the sender's public key (identity) into the re-encrypted ciphertext can be decrypted by using the recipient's secret key. A little disadvantage of this scheme is that there is no authentication (secret key verification, and the requester's identity verification).

In [5], Chu et al. propose two identity-based proxy re-encryption schemes, which are both proved secure in the standard model. One is efficient in both computation and ciphertext length, and the other achieves chosen ciphertext security. The scheme also has no authentication (secret key verification, and the requester's identity verification).

In [6,9], Boldyreva et al. propose an IBE scheme with revocation mechanisms, which significantly improves key-update efficiency.

In [7], Tang et al. propose an inter-domain IBE proxy re-encryption scheme with low computation complexity. However, it is proved in [10] that the collusion attack against Tang's scheme. Then, Han et al. propose an identity-based data storage scheme supporting intra-domain and inter-domain queries, which is proved to be IND-sID-CPA secure and against the collusion attack. Also, Wang et al. propose two new identity-based proxy re-encryption schemes to prevent collusion attacks in [8], one of which is proved IND-PrID-CPA secure in the random oracle model, and the other of which achieves the IND-PrID-CCA security.

Liang et al. propose a cloud-based revocable identity-based proxy re-encryption scheme in [11]. However, Wang et al. show Liang's scheme has serious security problems and propose an improved scheme in [12], which not only achieves collusion resistance, but also takes lower decryption computation and achieves constant size re-encrypted ciphertext.

3 Background

In this section, we introduce the background of our proposed identity-based proxy re-encryption scheme.

3.1 Syntax of Our Secure Revocable IB-PRE Cloud Storage Scheme

There are four entities in our secure revocable identity-based proxy re-encryption cloud storage scheme as shown in Fig. 1: the private key generator (PKG), the proxy server (PS), the data owner (O) and the requester (R). The PKG is honest but curious, which issues secret keys for users. The proxy server stores the ciphertexts, re-encrypts the original ciphertexts and sends them to the requester who obtains access permission. The data owner encrypts data using public key (identity) and outsources them to the proxy server. The data owner authenticates the requester, generates the re-encryption keys independently and sends them to the PS. The requester obtaining the access permission can decrypt the re-encrypted ciphertexts.

Our secure revocable identity-based proxy re-encryption scheme is comprised 9 phases: Setup, KeyGen, IBEnc, Query, Permit, ReKeyGen, ReEnc, IBDec, Revoke.

Setup(k): This algorithm takes as inputs a security parameter k and outputs the public parameters *params*, the master secret key *MSK* for the *PKG*.

KeyGen(*params*, O): This algorithm takes as inputs the public parameters *params* and an identity O, and outputs a secret key SK'_O for the user with the identity O.

IBEnc(*params*, O, m): This algorithm takes as inputs the public parameters *params*, the identity O and the message m, and outputs the ciphertext CT, which is sent to the proxy server *PS*.

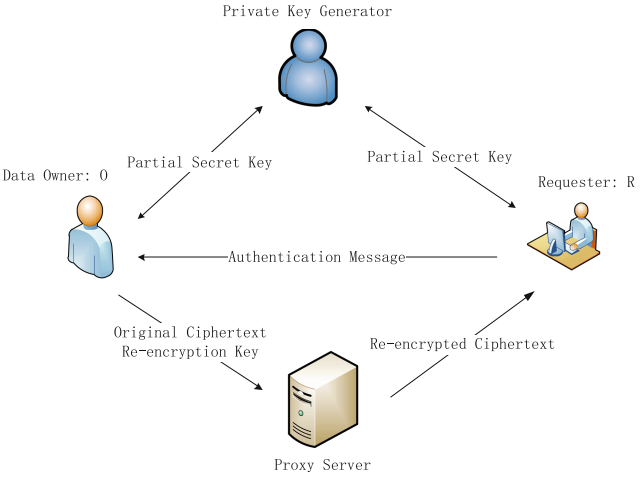

Fig. 1. System model

Query(R, SK'_R, CT): The requester R queries the data outsourced by the owner O. This algorithm takes as inputs the requester's identity R, secret key SK'_R and the ciphertext CT, and outputs an authentication information Ψ, which is sent to the proxy server PS.

Permit($params$, R, Ψ, $SK_{R,2}$): The data owner authenticates the requester by verifying the authentication information Ψ. If the requester is legal, continue to execute the next algorithm ReKeyGen(•). Otherwise, output $\perp$.

ReKeyGen(Ψ, R): This algorithm takes as inputs the authentication information Ψ and the identity R of the requester, and outputs the re-encryption key $RK_{O\to R}$, which is sent to the proxy server PS.

ReEnc(CT, $RK_{O\to R}$): This algorithm takes as inputs the original ciphertext CT and the re-encryption key $RK_{O\to R}$, and outputs the re-encrypted ciphertext CT'. The proxy server PS sends the re-encrypted ciphertext CT' to the requester R.

IBDec(•): The decryptor responses as follows with respect to the following two cases:

Case 1. IBDec(CT, SK'_O): This algorithm takes as inputs the original ciphertext CT and the secret key SK'_O of the data owner O, and outputs the message m.

Case 2. IBDec(CT', SK'_R): This algorithm takes as inputs the re-encrypted ciphertext CT' and the secret key SK'_R of the requester, and outputs the message m.

Revoke(id, RL): This algorithm takes as inputs the current revocation list RL and the identity id of the user to be revoked, and outputs the updated revocation list.

The correctness of an IB-PRE scheme is defined as follows: Given $params$, and two users' identities O and R, if

– $SK'_O \longleftarrow KeyGen(params, O)$,
– $SK'_R \longleftarrow KeyGen(params, R)$,
– $RK_{O\to R} \longleftarrow ReKeyGen(\Psi, R)$,

then the following results must hold:

1. $IBDec(CT, SK'_O) = m$,
2. $IBDec(CT', SK'_R) = m$.

3.2 Security Model

In this section, we present the security model of the chosen plaintext attacks (CPA) of an IB-PRE scheme. Before defining it, we make sure the following condition to be satisfied: given a challenge ciphertext CT^* for identity O^*, the adversary can make the following queries without knowing the secret key SK'_{O^*}, the secret key SK'_R and the proxy re-encryption key $RK_{O^*\to R}$. Let O^* be the target identity with which the adversary want to be challenged to the challenger.

Game CPA

Setup. The challenger $\mathbb{C}$ runs Setup(k) to generate the public parameters *params*, the master secret key *MSK*, and sends *params* to adversary $\mathbb{A}$.

Phase 1. $\mathbb{A}$ can make the following queries:

1. Secret Key Query. $\mathbb{A}$ inputs the identity O, and $\mathbb{C}$ returns the SK'_O.
2. Proxy Re-encryption Key Query. $\mathbb{A}$ inputs the identity (O, R), and $\mathbb{C}$ returns the $RK_{O\to R}$.

Challenge. When $\mathbb{A}$ wants to end phase 1, it submits O^* and messages (m_0, m_1) of equal length. $\mathbb{C}$ flips a fair coin with $\{0, 1\}$ and obtains $\gamma \in \{0, 1\}$. It computes a challenge ciphertext CT^* for the message m_γ under the identity O^* and sends CT^* to $\mathbb{A}$.

Phase 2. $\mathbb{A}$ can adaptively make the following additional queries:

1. Secret Key Query. $\mathbb{A}$ inputs the identity O, where $O \neq O^*$, and $\mathbb{C}$ responds as in phase 1.
2. Proxy Re-encryption Key Query. $\mathbb{A}$ inputs the identity (Ψ, R), where $O \neq O^*$ and $R \neq O^*$, and $\mathbb{C}$ responds as in phase 1.

Guess. A outputs a guess γ' on γ.

Definition 1 (IND-PrID-CPA) [8]**.** In Game CPA, $\mathbb{A}$ wins the game if $\gamma' = \gamma$. An IB-PRE scheme is said to be indistinguishable against adaptively chosen an identity and chosen plaintext attacks (IND-PrID-CPA) if there is not any polynomial time algorithm with a non-negligible advantage in winning Game CPA.

3.3 Complexity Assumption

We describe the computation problems used within this work in this subsection.

Definition 2 (Bilinear Groups). Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative groups with prime order p and g be a generator of group $\mathbb{G}_1$. A bilinear map e: $\mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ is a map with between the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with the following properties:

- Bilinearity: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for $g_1, g_2 \in \mathbb{G}_1$ and two random numbers $a, b \in Z_p^*$.
- Non-degeneracy: $e(g, g) \neq 1$ where 1 is the identity element of the group $\mathbb{G}_1$.
- Computability: There is an efficient algorithm to compute $e(g_1, g_2)$ for all $g_1, g_2 \in \mathbb{G}_1$.

We say (p, $\mathbb{G}_1$, $\mathbb{G}_2$, e, g) a bilinear groups.

Definition 3 (Decision Bilinear Diffie-Hellman (DBDH) Assumption) [9]**.** Given a bilinear groups $(p, \mathbb{G}_1, \mathbb{G}_2, e, g)$, define two distributions $D_0 = (A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^{abc})$ and $D_1 = (A, B, C, Z) = (g^a, g^b, g^c, e(g, g)^z)$, where $a, b, c, z \in Z_p^*$. The DBDH problem in the bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, e, g)$ is to decide a bit γ from given D_γ, where $\gamma \in 0, 1$. The advantage of adversary $\mathbb{A}$ in soving the DBDH problem in the bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, e, g)$ is defined by

$$Adv_{\mathbb{A}}^{DBDH} = \big|Pr[\mathbb{A}(D_0) \longrightarrow 1] - Pr[\mathbb{A}(D_1) \longrightarrow 1]\big|.$$

4 Our Construction

In this section, we propose a secure revocable identity-based proxy re-encryption scheme, in which the PKG does not generate the full secret keys for users.

Based on the IB-PRE scheme [10], we propose a secure IB-PRE scheme with low computation complexity. The description of our secure IB-PRE scheme is as follows.

- Setup(k): The PKG takes a security parameter k as input, and returns a bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, e)$ with prime order p, where e: $\mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$. And choose cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{G}_1$. Let g, θ be the generators of $\mathbb{G}_1$. Then, the PKG sets $g_1 = g^\alpha$, $g_2 = g^\beta$, $\zeta = \theta^\alpha$, $\alpha, \beta \in Z_p^*$, and initializes a user list $UL = \Phi$ and a revocation list $RL = \Phi$. Finally, the PKG publishes the system parameters $params = (p, \mathbb{G}_1, \mathbb{G}_2, e, g, g_1, g_2, \theta, H)$ and keeps the master secret key $MSK = (\alpha, \beta, \zeta)$ secret.
- KeyGen($params$, O): The PKG takes the public parameters $params$ and an identity O as inputs, and outputs a partial secret key SK_O for the user with the identity O. The PKG randomly chooses $l_O \in Z_p^*$, and computes

$$SK_{O,1} = \theta^\alpha (H(O \oplus g_2))^{l_O},\ SK_{O,2} = g^{l_O}.$$

The partial secret key for the user O is $SK_O = (SK_{O,1}, SK_{O,2})$. The PKG sends $\{SK_O, l_O\}$ to the user O through a secure channel such as email. The user O can verify the partial secret key by

$$e(SK_{O,1}, g) \stackrel{?}{=} e(g_1, \theta) \cdot e(H(O \oplus g_2), SK_{O,2})$$

The user O chooses $q \in Z_p^*$ and computes the secret key $SK'_O = (SK'_{O,1}, SK'_{O,2})$.

$$SK'_{O,1} = \theta^{\alpha}(H(O \oplus g_2 \oplus q)^{l_O},\ SK'_{O,2} = SK_{O,2}.$$

- IBEnc(*params*, O, m): The data owner O takes the public parameters *params*, his/her identity O and the message m as inputs, and outputs the ciphertext CT, which is sent to the proxy server PS. The data owner O chooses $\varphi \in Z_p^*$ and computes the original ciphertext $CT = (C_1, C_2, C_3)$.

$$C_1 = m \cdot e(g, g_1)^{\varphi},\ C_2 = g^{\varphi},\ C_3 = (H(O \oplus g_2 \oplus q))^{\varphi}.$$

- Query(R, SK'_R, CT): The requester R queries the data outsourced by the owner O. The requester R takes the identity R, secret key SK'_R and the ciphertext CT as inputs, and outputs an authentication information Ψ, which is sent to the data owner O. The requester R computes $F = g_2^l$ and $Q = F \cdot SK'_{R,1}$, and sends an authentication information $\Psi = \{H(R \oplus g_2 \oplus q'), R, C_2, Q, F\}$ to the data owner O.
- Permit(*params*, R, Ψ, $SK_{R,2}$): The data owner authenticates the requester by verifying the authentication information Ψ. If the requester is legal, continue to execute the next algorithm (ReKeyGen($\bullet$)). Otherwise, output $\perp$. First, the data owner O queries the PKG on the partial secret key $SK_{R,2}$ of the requester R. The PKG search the identity of the requester in the revocation list RL. If the requester is a revoked user, the PKG responds the data owner $\perp$. Otherwise, respond with $SK_{R,2}$ of the requester. Receiving $SK_{R,2}$, the data owner O checks

$$e(Q, g) \stackrel{?}{=} e(g_1, g) \cdot e(H(R \oplus g_2 \oplus q'), SK_{R,2}) \cdot e(F, g)$$

- ReKeyGen(Ψ, R): The data owner takes the authentication information Ψ and the identity R of the requester as inputs, and outputs the re-encryption key $RK_{O \to R}$, which is sent to the proxy server PS. The data owner O computes the re-encryption key as

$$RK_{O \to R} = \left(\frac{H(R \oplus g_2 \oplus q')}{H(O \oplus g_2 \oplus q)}\right)^{\varphi}.$$

- ReEnc(CT, $RK_{O \to R}$): The proxy server takes the original ciphertext CT and the re-encryption key $RK_{O \to R}$ as inputs, and outputs the re-encrypted ciphertext CT' which is sent to the requester R. The proxy server PS computes the re-encrypted ciphertext as

$$C'_1 = C_1,\ C'_2 = C_2,\ C'_3 = RK_{O \to R} \cdot C_3.$$

  The proxy server PS sends the re-encrypted ciphertext $CT' = (C'_1, C'_2, C'_3)$ to the requester R.
- IBDec($\bullet$): The decryptor responses as follows with respect to the following two cases:

- Case 1. IBDec(CT, SK'_O): The data owner O takes the original ciphertext CT and his/her secret key SK'_O as inputs, and outputs the message m. The data owner O decrypts the original ciphertext as $m = C_1 \cdot \frac{e(SK'_{O,2}, C_3)}{e(SK'_{O,1}, C_2)}$.
- Case 2. IBDec(CT', SK'_R): The requester R takes the re-encrypted ciphertext CT' and his/her secret key SK'_R as inputs, and outputs the message m. The requester R decrypts the re-encrypted ciphertext as $m = C'_1 \cdot \frac{e(SK'_{R,2}, C'_3)}{e(SK'_{R,1}, C'_2)}$.

– Revoke(id, RL): The PKG updates the revocation list by $RL \leftarrow RL \bigcup \{id\}$, where id is the identity of the user to be revoked, and returns the updated revocation list.

Theorem 1 (Correction of Our Proposed IB-PRE Scheme). The proposed IB-PRE scheme is correct.

Proof. The correctness can be checked by the following equations.

– Correctness for case 1.

$$\begin{aligned} & C_1 \cdot \frac{e(SK'_{O,2}, C_3)}{e(SK'_{O,1}, C_2)} \\ &= m \cdot e(g, g_1)^{\varphi} \cdot \frac{e(g^{l_O}, (H(O \oplus g_2 \oplus q))^{\varphi})}{e(g_1(H(O \oplus g_2 \oplus q)^{l_O}, g^{\varphi})} \\ &= m \cdot e(g^{\varphi}, g_1) \cdot \frac{e(g^{\varphi}, (H(O \oplus g_2 \oplus q))^{l_O})}{e(g_1(H(O \oplus g_2 \oplus q)^{l_O}, g^{\varphi})} \\ &= m \cdot \frac{e(g^{\varphi}, g_1(H(O \oplus g_2 \oplus q))^{l_O})}{e(g_1(H(O \oplus g_2 \oplus q)^{l_O}, g^{\varphi})} \\ &= m \end{aligned} \tag{1}$$

– Correctness for case 2.

$$\begin{aligned} & C'_1 \cdot \frac{e(SK'_{R,2}, C'_3)}{e(SK'_{R,1}, C'_2)} \\ &= C_1 \cdot \frac{e(SK'_{R,2}, RK_{O \to R} \cdot C_3)}{e(SK'_{R,1}, C_2)} \\ &= m \cdot e(g, g_1)^{\varphi} \cdot \frac{e(g^{l_R}, (\frac{H(R \oplus g_2 \oplus q')}{H(O \oplus g_2 \oplus q)})^{\varphi} \cdot (H(O \oplus g_2 \oplus q))^{\varphi})}{e(g_1(H(R \oplus g_2 \oplus q')^{l_R}, g^{\varphi})} \\ &= m \cdot e(g, g_1)^{\varphi} \cdot \frac{e(g^{l_R}, (H(R \oplus g_2 \oplus q'))^{\varphi})}{e(g_1(H(R \oplus g_2 \oplus q')^{l_R}, g^{\varphi})} \\ &= m \cdot e(g^{\varphi}, g_1) \cdot \frac{e(g^{\varphi}, (H(R \oplus g_2 \oplus q'))^{l_R})}{e(g_1(H(R \oplus g_2 \oplus q')^{l_R}, g^{\varphi})} \\ &= m \cdot \frac{e(g^{\varphi}, g_1(H(R \oplus g_2 \oplus q'))^{l_R})}{e(g_1(H(R \oplus g_2 \oplus q')^{l_R}, g^{\varphi})} \\ &= m \end{aligned} \tag{2}$$

5 Security Analysis

Theorem 2 (IND-PrID-CPA of Our Proposed IB-PRE Scheme) [8]. Our proposed IB-PRE scheme is IND-PrID-CPA secure under the DBDH assumption in the random oracle model. That is to say, if there is an adversary that can break the IND-PrID-CPA security of our proposed IB-PRE scheme with the non-negligible advantage ε within time t, then we can construct an algorithm that can solve the DBDH problem in $\mathbb{G}_2$ with the non-negligible advantage ε' within time t', such that

$$\varepsilon' \geq \frac{\varepsilon}{e \cdot (q_s + 2q_r)} \quad and \quad t' = t + \phi(t),$$

where e is the base of natural logarithm, $\phi(t)$ denotes the time required to answer all queries, q_s and q_r are the numbers of secret key queries and proxy re-encryption key queries, respectively.

Proof. The idea of proof is similar to the proof procedure in [8]. Due to space limitations, we omit the complete proof of security here.

Theorem 3. Our scheme can resist the collusion attack.

Proof. Since the secure random number involved in the generation of the re-encryption key in our scheme, the data owner's secret key can not be calculated even if the designated decryptor can compromise the proxy server to obtain the re-encryption key.

6 Performance Analysis

In this section, we compare our scheme with other existing schemes. First, we make a comparison based on the security and features of all schemes as shown in Table 1. The security of all schemes is based on the Decision Bilinear Diffie-Hellman (DBDH) assumption. [7,11] are IND-CPA secure and others are IND-sID-CPA or IND-PrID-CPA secure. [7] suffers from a collusion attack, which is demonstrated in [10]. [10] and our scheme support the secret key verification and the identity verification of the requester. [8] only supports the secret key verification. Besides, [11,12] and our scheme support the user revocation.

Then, we compare our scheme with other scheme in term of efficiency. Here, we suppose that the prime number p of all schemes is same. This suggests the order of all the bilinear groups is equal. $|\mathbb{G}|/|\mathbb{G}_i|$ denotes one element in the group $\mathbb{G}/\mathbb{G}_i$ and $|p|$ denotes the length of the binary representation. From Table 2, we see that our scheme is the least in communication cost, and [7] is comparable with other schemes. [11,12] have greater communication cost, where $|Path(\eta)|$ denotes the number of nodes in the path $Path(\eta)$ and l denotes the times of re-encryption. Table 3 shows the comparison of computation complexity. We assume that all operations are dyadic operation. T_E denotes one exponentiation and $\tau_P/\tau_{\hat{P}}$ denotes one pairing operation. Obviously, our scheme has the advantages compared with other schemes. [11,12] also have greater computation complexity.

Table 1. Security and features comparison of our scheme with other schemes

Schemes	Complexity assumption	Security	Authentication	User revocation
[4]	DBDH	IND-sID-CPA	No	No
[7]	DBDH	IND-CPA	No	No
[8]	DBDH	IND-PrID-CPA	Yes	No
[10]	DBDH	IND-sID-CPA	Yes	No
[11]	DBDH	IND-CPA	No	Yes
[12]	DBDH	IND-ID-CPA	No	Yes
Our scheme	DBDH	IND-PrID-CPA	Yes	Yes

Table 2. Communication cost comparison of our scheme with other schemes

Schemes	Secret key	Original ciphertext	Re-encryption key	Re-encrypted ciphertext
[4]	$2\|\mathbb{G}\|$	$2\|\mathbb{G}\| + \|\mathbb{G}_1\|$	$\|p\| + \|\mathbb{G}\|$	$2\|\mathbb{G}\| + \|\mathbb{G}_1\|$
[7]	$\|\mathbb{G}\|$	$\|\mathbb{G}\| + \|\mathbb{G}_1\|$	$2\|\mathbb{G}\| + \|\mathbb{G}_1\|$	$2\|\mathbb{G}\| + 3\|\mathbb{G}_1\|$
[8]	$2\|\mathbb{G}_1\|$	$3\|\mathbb{G}_1\| + \|\mathbb{G}_2\|$	$2\|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\| + \|\mathbb{G}_2\|$
[10]	$3\|\mathbb{G}\|$	$2\|\mathbb{G}\| + \|\mathbb{G}_\tau\|$	$3\|\mathbb{G}\| + \|\mathbb{G}_\tau\|$	$5\|\mathbb{G}\| + \|\mathbb{G}_\tau\|$
[11]	$2\|\mathbb{G}\|$	$3\|\mathbb{G}\| + \|\mathbb{G}_T\|$	$9\|\mathbb{G}\| + 2\|\mathbb{G}_T\|$	$(l+3)\|\mathbb{G}\| + (2l+1)\|\mathbb{G}_T\|$
[12]	$2\|Path(\eta)\|\|\mathbb{G}\|$	$3\|\mathbb{G}\| + \|\mathbb{G}_T\|$	0	$6\|\mathbb{G}\| + \|\mathbb{G}_T\|$
Our scheme	$2\|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\| + \|\mathbb{G}_2\|$	$\|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\| + \|\mathbb{G}_2\|$

Table 3. Computation complexity comparison of our scheme with other schemes

Schemes	Encryption	Re-encryption key generation	Re-encryption	Decryption	Re-decryption
[4]	$4T_E + \tau_{\hat{P}}$	T_E	$T_E + \tau_{\hat{P}}$	$2\tau_{\hat{P}}$	$2\tau_{\hat{P}}$
[7]	$2T_E + \tau_{\hat{P}}$	$2T_E + \tau_{\hat{P}}$	$2T_E + 2\tau_{\hat{P}}$	$\tau_{\hat{P}}$	$4\tau_{\hat{P}}$
[8]	$4T_E + \tau_{\hat{P}}$	$3T_E$	$2\tau_{\hat{P}}$	$2\tau_{\hat{P}}$	$2\tau_{\hat{P}}$
[10]	$4T_E + \tau_P$	$6T_E + \tau_P$	0	$2\tau_P$	$2T_E + 2\tau_P$
[11]	$6T_E + \tau_P$	$12T_E + \tau_P$	$2l\tau_P$	$3\tau_P$	$2T_E + 4\tau_P / 2lT_E + (l+3)\tau_P$
[12]	$4T_E + \tau_P$	0	$4T_E + \tau_P$	$3\tau_P$	$6\tau_P$
Our scheme	$3T_E + \tau_P$	T_E	0	$2\tau_P$	$2\tau_P$

In addition, we conducted experiments on our scheme using Pairing Based Cryptography (PBC) library [13]. Here, we use the Microsoft Visual C++ conversion pbc-0.4.7-vc. All algorithms were coded using C programming language and conducted on a system with Intel(R) Core(TM) i5-3470 CPU at 3.20 GHz and 3.20 GHz and 4.00 GB RAM in Windows 7. Type A pairings are used in the simulation, which are constructed on the curve $y^2 = x^3 + x$ over the field F_q for some prime $q = 3 \mod 4$. This pairing is symmetric, where the order of groups is 160 bits, the base field size is 512 bits and the embedding degree is 2.

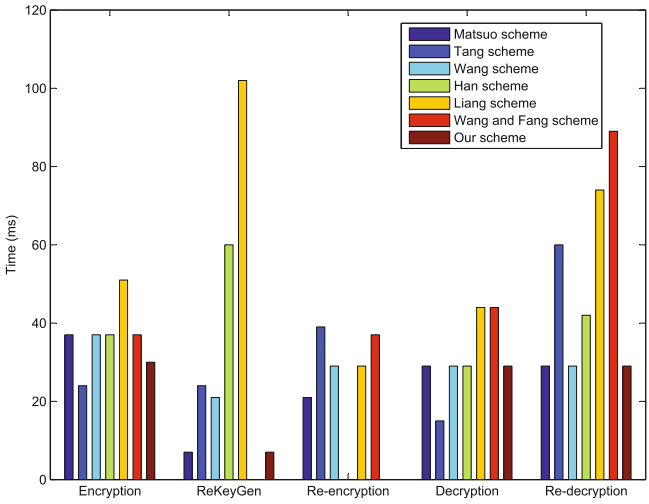

Fig. 2. Simulation results

The simulation results are shown in Fig. 2. We observe that our scheme has a significant advantage in ReKegGen, Re-encryption and Re-decryption. Although [7] has less runtime in Encryption and Decryption, it takes more time in Re-encryption and Re-decryption.

7 Conclusion

In this paper, we propose a secure revocable identity-based proxy re-encryption scheme for cloud storage, in which the PKG does not generate full secret keys for users. Therefore, the PKG can not decrypt the ciphertext without knowing the secret keys of users. Besides, the generation of re-encryption keys does not involve the participation of the PKG. Our proposed scheme is provably secure under the standard assumption (DBDH) in the random oracle model. In addition, our scheme is comparable with other schemes in computation complexity.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40061-5_29
2. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
3. Green, M., Ateniese, G.: Identity-based proxy re-encryption. In: Katz, J., Yung, M. (eds.) ACNS 2007. LNCS, vol. 4521, pp. 288–306. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72738-5_19
4. Matsuo, T.: Proxy re-encryption systems for identity-based encryption. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 247–267. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73489-5_13
5. Chu, C.-K., Tzeng, W.-G.: Identity-based proxy re-encryption without random oracles. In: Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.) ISC 2007. LNCS, vol. 4779, pp. 189–202. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-75496-1_13
6. Boldyreva, A., Goyal, V., Kumar, V.: Identity-based encryption with efficient revocation. In: Proceedings of the 15th ACM Conference on Computer and Communications Security, pp. 417–426. ACM, New York (2008)
7. Tang, Q., Hartel, P., Jonker, W.: Inter-domain identity-based proxy re-encryption. In: Yung, M., Liu, P., Lin, D. (eds.) Inscrypt 2008. LNCS, vol. 5487, pp. 332–347. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01440-6_26
8. Wang, L., Wang, L., Mambo, M., Okamoto, E.: New identity-based proxy re-encryption schemes to prevent collusion attacks. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing 2010. LNCS, vol. 6487, pp. 327–346. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17455-1_21
9. Seo, J.H., Emura, K.: Revocable identity-based encryption revisited: security model and construction. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 216–234. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36362-7_14
10. Han, J., Susilo, W., Mu, Y.: Identity-based data storage in cloud computing. Future Gener. Comput. Syst. **29**, 673–681 (2013)
11. Liang, K., Liu, J.K., Wong, D.S., Susilo, W.: An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing. In: Kutyłowski, M., Vaidya, J. (eds.) ESORICS 2014. LNCS, vol. 8712, pp. 257–272. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11203-9_15
12. Wang, C., Fang, J., Li, Y.: An improved cloud-based revocable identity-based proxy re-encryption scheme. In: Niu, W., Li, G., Liu, J., Tan, J., Guo, L., Han, Z., Batten, L. (eds.) ATIS 2015. CCIS, vol. 557, pp. 14–26. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48683-2_2
13. Lynn, B.: PBC library. http://crypto.stanford.edu/pbc