A Novel Proxy Re-encryption Scheme Based on Identity Property and Stateless Broadcast Encryption Under Cloud Environment

Shoulin Yin, Hang Li, and Lin Teng
(Corresponding author: Hang Li)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: lihangsoft@163.com)

(Received Mar. 30, 2018; Revised and Accepted July 12, 2018; First Online Apr. 4, 2019)

Abstract

Due to low efficiency of traditional proxy re-encryption scheme in cloud environment, we propose a novel proxy re-encryption scheme based on identity property under cloud environment in this paper. The new scheme makes full use of the advantages of identity property encryption, proxy re-encryption and stateless broadcast encryption to provide safe and reliable cloud storage. Identity property encryption utilizes the user's identity property as public key that can reduce the process of certificate validation. Proxy re-encryption can realize the fine-grain access control. In addition, stateless broadcast encryption can completely resist fully collusion resistant (i.e. Though one cancels the cooperation between users, they cannot decrypt the message). Finally, experimental results demonstrate that the new scheme not only reduces the consumption of system, but realizes the encryption efficiency and security.

Keywords: Cloud Environment; Identity Property; Proxy Re-encryption; Stateless Broadcast Encryption

1 Introduction

Cloud computing is the comprehensive development of parallel computing [8,19], distributed computing and grid computing. Cloud has attracted widespread attention and recognition as it transfers the traditional computing and storage functions into the cloud environment, which saves lots of hardware cost for users. Data stored in the cloud is out of control for the data owner. The traditional access control method cannot well guarantee the data security. Additionally, cloud service provider is unbelievably. Especially, when the cloud is attacked, the data is inevitably leaked [12].

In order to protect the user's data in the cloud, data owners need to encrypt sensitive data and store ciphertext in the cloud. Although cloud is attacked, users do not have to worry about the leakage of data with new privacy-preserving methods [2, 3, 15, 21]. But this model accordingly leads to the difficulty of data sharing between users. After receiving the ciphertext, the receiver cannot directly decrypt it. Generally, if users want to share the ciphertext, they should download ciphertext and decrypt it into plaintext. Follow send the decrypted data to other user. This process will consume amount of network resources and computational resources, also lose the advantage of cloud storage.

Blaze [1] proposed proxy re-encryption scheme that the ciphertext decrypted by sender can be directly transformed into the ciphertext decrypted by receiver. The third party can be authorized to re-encrypt the stored encrypted data. Under the cloud storage environment, proxy re-encryption can make the cloud calculate directly. By transforming the outsourcing to encrypt data, agent can transform the ciphertext without leaking encrypted data, which can save a lot of network resources, make full use of the cloud computing resources and implement security access of encrypted data [10, 11].

Completely, proxy re-encryption has been widely applied in cloud storage area and drawn wide attention by the researchers. Yin [6] put forward a new security cloud storage data encryption scheme based on identity proxy re-encryption in this article. This scheme could flexibility share data with other users security without fully trusted cloud. For the detailed structure, he used a strong unforgeable signature scheme to make the transmuted ciphertext have publicly verification combined identity-based encryption. Li [9] proposed a multi-keyword search algorithm based on polynomial function and safety inner-product method. Liu [16] proposed a density-based clustering method for K-anonymity privacy protection. And Xu [18] proposed a versatile primitive referred to as conditional identity-based broadcast PRE (CIBPRE) and formalized its semantic security, which allowed a sender to encrypt a message to multiple receivers by specifying

these receivers' identities, and the sender could delegate a re-encryption key to a proxy so that he could convert the initial ciphertext into a new one to a new set of intended receivers.

Existing schemes have realized ciphertext sharing, however, there are still some problems in terms of usability and efficiency.

- The cloud can convert the ciphertext data of data owner by using the re-encryption key generated by the data owner. If the cloud is not credible, the data will be sent to the receiver or the cloud conspires with the receiver. Then the user's privacy can be leaked, and the user will not be able to realize the fine-grained access control for the encrypted data in cloud.
- When sharing data, each receiver corresponds to a re-encryption key, the cloud also needs to generate a re-encrypted ciphertext for each user. The number of ciphertexts is proportional to receivers resulting in wasting of cloud computational and storage resources.
- In traditional public key system, it is necessary for the authentication center to bind the user and certificate, and the user needs to certificate management and certificate authentication, which causes a great deal of management consumption.

Aiming at the above problems, combining with the characteristics of stateless broadcast encryption and identity-based proxy re-encryption, this paper proposes a novel proxy re-encryption scheme based on identity property under cloud environment to achieve efficient and convenient ciphertext storage and sharing. The remainder of this paper is organized as follows. Section 2 presents the Bilinear map and identify-based broadcast encryption scheme. In Section 3, new scheme in this paper is described. Security proof and performance analysis are given in Section 4. Section 5 finally concludes the paper.

2 Preliminaries

2.1 Bilinear Map

Theorem 1. Bilinear map. *When the mapping function $e : G_1 \times G_2 \to G_T$ satisfies the following conditions, it can be called bilinear map [22, 23].*

- G_1 and G_T are two $q-order$ groups, where q is a prime;
- For all $a, b \in Z_q^*$, it generates apparatus g of G_1, which meets $e(g^a, g^b) = e(g, g)^{ab}$;
- Non-degeneracy, that is, if g is a member of G_1, then $e(g, g)$ is a member of G_T;
- e is computable. For all $p, q \in G_1$, $e(p, q)$ can be calculated by an effective algorithm.

2.2 Identify-based Stateless Broadcast Encryption Scheme-ISBBE

Identity-based stateless broadcast encryption scheme [5, 13, 14] consists of four algorithms: $Setup_{ISBBE}(\lambda, N)$, $Extract_{ISBBE}(MK_{IBBE}, ID)$, $Enc_{ISBBE}(PK_{ISBBE}, S, m)$, and $Dec_{ISBBE}(PK_{ISBBE}, ID, SK_{ISBBE}^{ID}, C, S)$. The positive integer is the maximum number of N receivers in the encryption process. ISBBE algorithm is described as follows:

1) $Setup_{IBBE}(\lambda, N)$. Input security parameter λ and N to construct bilinear map $e : G \times G \to G_T$,where G and G_T are two $q-order$ elliptic curve groups, q is a prime, $|q| = \lambda$. w and v are two different parameters. Randomly select two generators $(g, h) \in G^2$ and $\gamma \in Z_p^*$, choose a hash function $H : 0, 1^* \to Z_p^*$ mapping 0/1 string to Z_p^*. Finally, output the main public parameter PK_{IBBE} and the master secret parameter MK_{IBBE}, where: $PK_{IBBE} = (p, G, G_T, e, w, v, h, h^{\gamma}, \cdots, h^{\gamma^N}, H)$ and $MK_{IBBE} = (g, \gamma)$.

2) $Extract_{IBBE}(MK_{IBBE}, ID)$. Input the main secret parameter and the user's identity ID. After calculation, it generates the private key corresponding to his/her identity SK_{IBBE}^{ID}. $SK_{IBBE}^{ID} = \frac{1}{g\gamma + H(ID)}$.

3) $Enc_{ISBBE}(PK_{ISBBE}, S, m)$. Input main public parameter, a user set S and all plaintexts m, but the number of users in set S is less than N. Randomly select $k \in Z_p^*$, output ciphertext C, where: $C = (c_1, c_2, c_3)$, $c_1 = w^{-k}$, $c_2 = h^{k \cdot \Pi_{ID_i \in S}(\gamma + H(ID_i))}$ and $c_3 = v^k \cdot m$.

4) $Dec_{ISBBE}(PK_{ISBBE}, ID, SK_{ISBBE}^{ID}, C, S)$. Input the main public parameter, a user identity and his/her private key, a ciphertext and a set of users. Execute decryption operation for the ciphertext:

$$CK = (e(c_1, h^{\Delta_\gamma(ID,S)) \cdot e(SK_{ISBBE}^{ID}, c_2)})^{\frac{i}{\Pi_{ID_i \cap ID_i \neq ID} H(ID_i)}},$$

$$\Delta_\gamma(ID, S) = \frac{1}{\gamma}(\Pi_{ID_i \in S \cap ID_i \neq ID}(\gamma + H(ID_i)) - \gamma (\Pi_{ID_i \in S \cap ID_i \neq ID} H(ID_i))).$$

Finally, the plaintext m is calculated as, $m = \frac{c_3}{v^k}$.

3 Novel Proxy Re-encryption Scheme Based on Identity Property-PIRIP

Our new scheme-PIRIP comprises seven algorithms: $Setup_{PIRIP}$, $Etract_{PIRIP}$, Enc_{PIRIP}, $RKExtract_{PIRIP}$, $ReEnc_{PIRIP}$, $Dec1_{PIRIP}$, $Dec2_{PIRIP}$.

1) Initialization. KGC (key generation center) executes the initialization algorithm $Setup_{PIRIP}$ and the key generation algorithm $Extract_{PIRIP}$. The private key is generated according to the user's identity ID. Additionally, the whole system is initialized.

2) Initializing ciphertext uploading and encrypting. The ciphertext receiver set is denoted as S_1. It performs the initializing encryption algorithm Enc_{PIRIP}, encrypts the plaintext and generates ciphertext which can be decrypted by receiver. The initialized ciphertext is sent to the cloud, which can be stored in stateless broadcast.

3) Initializing ciphertext downloading and decrypting. When a receiver in S_1 is online, the initialized ciphertext can be downloaded from the cloud. Then it executes initial ciphertext decryption algorithm $Dec1_{PIRIP}$ and gets the plaintext.

4) Ciphertext sharing. If one of the receivers in S_1 wants to share this data with other users that are not in S_1 (new receivers set is denoted as S_2), he can execute the encryption key generation algorithm $RKExtract_{PIRIP}$, generate a re-encryption key and send it to the cloud. Cloud executes proxy re-encryption algorithm $ReEnc_{PIRIP}$, makes re-encryption calculation for the initialized ciphertext to generate re-encryption ciphertext. Re-encryption ciphertext can no longer execute re-encryption calculation, that is, no re-encryption forwarding.

5) Re-encrypted ciphertext downloading and decrypting. When one of the receivers in S_2 is online, he can download encrypted ciphertext from the cloud and execute the encrypted ciphertext decryption algorithm $Dec2_{PIRIP}$ to decrypt it.

3.1 New Scheme Implement

1) Initializing algorithm $Setup_{PIRIP}(\lambda, N)$.

   - Input the security parameter $\lambda \in Z_p^*$ and $N \in Z_p^*$, where N is the receiver's upper limit value in a single encryption.
   - Construct bilinear map $e : G \times G \to G_\gamma$, where G and G_γ are two $q-order$ elliptic curves, q is a prime and $|q| = \lambda$.
   - Randomly select four generators $(g, h, u, t) \in G^4$, $\gamma \in Z_p^*$, and two hash functions $H_1 : 0, 1^* \to Z_p^*$, $H_2 : G_\gamma \to G$. H_1 maps any length 0/1 to Z_p^*, H_2 is used to map the elements in G_T to G.
   - Output the main public parameter PK_{PIRIP} (as the parameter required for encryption, sending it to all users) and the master secret parameter MK_{PIRIP} (reserved by KGC and generating private key for the user). $PK_{PIRIP} = (p, G, G_T, e, w, v, h, h', \cdots, h^{\gamma^N}, u, u^\gamma, \cdots, u^{\gamma^N}, t, t^\gamma, \cdots, t^{\gamma^N}, H_1, H_2)$, $MK_{PIRIP} = (g, \gamma)$. Where $w = g^\gamma$, $v = e(g, h)$.

2) Key generation algorithm $Extract_{PIRIP}(MK_{PIRIP}, ID)$.

   Input parameter MK_{PIRIP} and the user's identity ID, output the private key SK_{PIRIP}^{ID} corresponding to the user identity. $SK_{PIRIP}^{ID} = \frac{1}{g^{\gamma+H_1(ID)}}$.

3) Initialize encryption algorithm Enc_{PIRIP} (PK_{PIRIP}, S, m, a).

   Input parameter PK_{PIRIP}, plaintext m, user set S and set access condition $a \in Z_p^*$, where S is less than N. Then randomly select $k \in Z_p^*$, output initial ciphertext C. $C = (c_1, c_2, c_3, c_4)$, $c_1 = w^{-k}$, $c_2 = h^{k \cdot \Pi_{ID_{i \in S}}(\gamma + H_1(ID_i))}$, $c_3 = v^k \times m$ and $c_4 = (u \cdot t^\alpha)^{k \cdot \Pi_{ID_{i \in S}}(\frac{\gamma + H_1(ID_i)}{H_1(ID_i)})}$.

4) Generate re-encrypt key: $RKExtract_{PIRIP}(PK_{PIRIP}, ID, SK_{PIRIP}^{ID}, S', \alpha)$.

   Input parameter PK_{PIRIP}, user identity ID and the private key SK_{PIRIP}^{ID}, required transforming user set S' and access condition $\alpha \in Z_p^*$. Randomly select $(k', s) \in Z_p^{*2}$, output the encryption key $d_{ID \to S'|\alpha}$. $d_{ID \to S'|\alpha} = (d_1, d_2, d_3, d_4)$, $d_1 = w^{-k'}$, $d_2 = h^{k' \cdot \Pi_{ID_{i \in S'}}(\gamma + H_1(ID_i))}$, $d_3 = H_2(v^{k'}) \cdot h^s$ and $d_4 = SK_{ID}(u \cdot t^\alpha)^{\frac{S}{H_1(ID)}}$.

5) Proxy re-encryption algorithm: $ReEnc(PK_{PIRIP}, d_{ID \to S'|\alpha}, C, S)$.

   Input parameter PK_{PIRIP}, re-encryption key $d_{ID \to S'|\alpha} = (d_1, d_2, d_3, d_4)$, initial ciphertext $C = (c_1, c_2, c_3, c_4)$ and a set of user identity S. Output re-encryption ciphertext C'. $C' = (c_1', c_2', c_3', c_4', c_5')$. Where $c_1' = d_1$, $c_2' = d_2$, $c_3' = d_3$ and $c_4' = d_4$. $c_5' = c_3 \cdot (e(c_1, h^{(\Delta\gamma)^{ID,S}}) \cdot e(d_4, c_2))^{\frac{-1}{\Pi_{ID_{i \in S \cap ID_i \neq ID}} H_1(ID_i)}}$. $\Delta\gamma(ID, S) = \frac{1}{\gamma}(\Pi_{ID_{i \in S \cap ID_i \neq ID}}(\gamma + H_1(ID_i)) - \Pi_{ID_{i \in S \cap ID_i \neq ID}} H_1(ID_i))$.

6) Initialize ciphertext decryption algorithm: $Decl_{PIRIP}(PK_{PIRIP}, ID, SK_{PIRIP}^{ID}, C, S)$.

   Input parameter PK_{PIRIP}, user identity ID and the private key SK_{PIRIP}^{ID}, initial ciphertext $C = (c_1, c_2, c_3, c_4)$ and a set of user identity S. Execute decryption calculation, output plaintext.

$$K = (e(c_1, h^{\Delta_\gamma}(ID, S)) \cdot e(SK_{PIRIP}^{ID}, c_2))^{\frac{1}{\Pi_{ID_{i \in S \cap ID_i \neq ID}} H_1(ID_i)}}$$

   Plaintext m is calculated as.

$$m = \frac{c_3}{K}.$$

7) Re-encryption ciphertext decryption algorithm: $Dec2_{PIRIP}(PK_{PIRIP}, ID', SK_{PIRIP}^{ID'}, C', S')$.

Input parameter PK_{PIRIP}, the user identity ID' and his/her private key $SK_{PIRIP}^{ID'}$, an initialized ciphertext $C' = (c'_1, c'_2, c'_3, c'_4, c'_5)$ and a set of user identity S' to execute decryption calculation.

$$K = (e(c'_1, h^{\Delta_\gamma}(ID', S')) \cdot e(SK_{PIRIP}^{ID'}, c'_2))^{\frac{1}{\Pi_{ID_i \in S \cap ID_i \neq ID'} H_1(ID_i)}}.$$

$$\Delta_\gamma(ID', S') = \frac{1}{\gamma}(\Pi_{ID_i \in S' \cap ID_i \neq ID'}(\gamma + H_1(ID_i)) - \Pi_{ID_i \in S' \cap ID_i \neq ID'} H_1(ID_i)).$$

$$K' = \frac{c'_3}{H_2(K)}.$$

So we can get plaintext,

$$m = c'_5 \cdot e(K', c'_4).$$

3.2 Security of New Scheme and Proof

3.2.1 Consistency of New Scheme

Theorem 2. *For any initial ciphertext generated by the correct steps: $C \leftarrow Enc_{PIRRP}(PK_{PIRRP}, S, m, \alpha)$, any private key generated by the correct steps: $SK_{PIRRP}^{ID} \leftarrow Extract_{PIRRP}(MK_{PIRRP}, ID)$, if $ID \in S$, then execute $Dec1_{PIRRP}(PK_{PIRRP}, ID, SK_{PIRRP}^{ID}, C, S)$ algorithm to calculate the plaintext m.*

Proof. When $ID \in S$,

$$(e(c_1, h^{\Delta_\gamma(ID,S)}) \cdot e(SK_{PIRRP}^{ID}, c_2))^{\frac{1}{\Pi_{ID_i \in S \cap ID_i \neq ID} H_1(ID_i)}} = v^k$$

$$m = \frac{c_3}{v^k}.$$

Therefore, when $ID \in S$, $Dec1_{PIRRP}(PK_{PIRRP}, ID, SK_{PIRRP}^{ID}, C, S) = m$. □

Namely, the correctly generated initial ciphertext can be decrypted by the selected receiver to obtain the original plaintext.

Theorem 3. *For any encrypted ciphertext: $C' = ReEnc_{PIRRP}(PK_{PIRRP}, d_{ID \to S'|\alpha}, C, S)$ and any private key generated by the correct steps $SK_{PIRRP}^{ID'} \leftarrow Extract_{PIRRP}(MK_{PIRRP}, ID')$, where $d_{ID \to S'|\alpha'} \leftarrow RKExtract_{PIRRP}(PK_{PIRRP}, ID, SK_{PIRRP}^{ID}, S', \alpha')$, $C \leftarrow Enc_{PIRRP}(PK_{PIRRP}, S, m, \alpha)$ and $SK_{PIRRP}^{ID} \leftarrow Extract_{PIRRP}(MK_{PIRRP}, ID)$ are correctly implemented, if $ID \in S$, $\alpha = \alpha'$ conditions are satisfied at the same time, then performing $Dec2_{PIRRP}(PK_{PIRRP}, ID', SK_{PIRRP}^{ID'}, C', S')$, m can be calculated.*

Theorem 2 presents that any properly generated encryption ciphertext can be accurately decrypted by the specified receiver. For this theorem, it is necessary to define what exactly generated ciphertext is, and who can decrypt the encrypted ciphertext. Any re-encryption ciphertext must satisfy the following conditions:

1) The generator of re-encryption key is the correct receiver of the initial ciphertext.

2) The initial ciphertext condition is same as that of re-encryption key. The receiver that correctly decrypting re-encryption ciphertext can be specified when the encryption key is generated.

3.2.2 Security of New Scheme

PIRIP scheme is with IND-sID-CPA security. If the polynomial time attacker does not know the initial ciphertext and the receiver's secret key of the re-encrypted ciphertext, it can not distinguish which one of the two plaintext is encrypted. In this case, an initial ciphertext and its re-encrypted ciphertext will not disclose any information of the plaintext without the corresponding private key.

Definition 1. *Determine the bilinear Diffie-Hellman problem.*

Group (G_1, G_2) can support the calculation of bilinear mapping $e : G_1 \times G_2 \to G_T$, g is a random generator of G_1. DBDH problem is a $(BGen(1^k)q, G_1, G_T, g, e)$ problem. For each input tuple $(g, g^a, g^b, g^c, T) \in G_1 \times G_T$ to determine a set of values $(a, b, c \in RandZ_q^*)$, T is equal to $e(g, g)^{abc}$ in group G_T.

Let K be a sufficiently large security parameter, and for a polynomial algorithm A in (G_1, G_T) group satisfying the following condition:

$$|pr[a, b, c \leftarrow Z_q^*; 1 \leftarrow A(g, g^a, g^b, g^c, e(g, g)^{abc}] - pr[a, b, c \leftarrow Z_q^*; T \leftarrow G_T; 1 \leftarrow A(g, g^a, g^b, g^c, T)]| \leq v(k).$$

Where $v(\cdot)$ is a minimum value that satisfies $v(k) < \frac{1}{p(k)}$ in all functions $p(\cdot)$.

Definition 2. *IND-sID-CPA attacking game: The IND-sID-CPA security of new scheme defines an attack game between a polynomial time attacker and a challenger. Attack game consists of several stages, attacker selects a user set S^* and a condition α^* as attack object and submit in the initial stage. In the setup stage, the challenger sets up a PIRIP scheme. In the challenge stage, the attacker randomly chooses two challenge plaintexts, one plaintext, S^* and condition α^* as encryption to generate initial ciphertext of PIRIP. Then it asks the attacker which encrypted ciphertext producing initial ciphertext. Before and after the challenge stage, the attacker may query ID's private key and re-encryption key, but does not include the private key of the initial ciphertext decrypted directly. If the attacker has no any advantage to make correct choice, it can be said that the new scheme is with IND-sID-CPA security.*

Theorem 4. *If DBDH problem is correct, new scheme is with IND-sID-CPA security under the random oracle model.*

Proof.

1) Initialize stage. The attacker A selects a set of users as challenge identity set S^*, where $|S^*| \leq N$. Meanwhile, it chooses a challenge condition α^*. Then S^* and α^* will be sent to the attacker B, the attacker B will sent S^* and α^* to challenger C.

2) Setup phase. Challenger C runs $Setup_{PIRIP}(\lambda, N)$ function to generate the main public parameter PK_{PIRIP} (Equation (1)) and the main secret parameter MK_{PIRIP} (Equation (2)) based on identity stateless broadcast encryption scheme for the attacker. The hash function H is a random oracle in security proof, it cannot be sent. Challenger C sends PK_{PIRIP} to attacker B, and provides hash function query $Q^H_{PIRIP}(ID)$ for attacker B. Challenger C provides a table L_{H_1} consisting of attributes (i.e. identity, hash value) to record the query identity and results.

   Attacker B randomly selects two numbers $(x, y) \in Z_p^{*2}$, generates the primary public parameter PK_{PIRIP} (Equation (11)) for the new scheme. H_1 and H_2 are considered as random oracles in the proving process, so they are not sent. Attacker B sends the simplified main public parameter to the attacker A. Attacker B provides attacker A with $Q^{H_1}_{IBBE}(ID)$ and $Q^{H_2}_{PIRIP}(Y)$ $(Y \in G_T)$ two queries to simulate the H_1 and H_2 random prediction queries. The attacker B also provides a table consisting of attributes (group element, hash value) to record the identity of L_{H_2} query and its results.

3) First query stage. Attacker B makes hash query $Q^{H_1}_{IBBE}(ID)$ and private key query $Q^{SK}_{IBBE}(ID)$ for challenger C. Attacker A makes hash query $Q^{H_1}_{IBBE}(ID)$, $Q^{H_2}_{IBBE}(ID)$, private key query $Q^{SK}_{PIRIP}(ID)$ and re-encryption key query $Q^{RK}_{PIRIP}(ID, S', \alpha)$ for attacker B.

4) Challenge stage. Attacker A determines the first query finish and sends two challenge plaintexts (m_0, m_1) to attacker B. Attacker B directly sends the challenge plaintexts (m_0, m_1) to challenger C. C executes $Enc_{IBBE}(PK_{IBBE}, S^*, m_b)$ to generate one challenge ciphertext C^*_{IBBE} (where b is a random number in [0,1]), and sends the ciphertext to attacker B. According to the structure of the ciphertext C^*_{IBBE}, we get $C^*_{IBBE} = (c_1, c_2, c_3)$. Return setup stage, attacker B randomly selects two numbers (x, y), and sets $u = h^y$, $t = h^y$. Attacker B expands C^*_{IBBE} as the available initial ciphertext $C^*_{IBBE} = (C^*_{IBBE}, c_4)$ by calculating $c_4 = (c_2^x, c_2^{y \cdot \alpha})^{\Pi_{ID_i \in S}(\frac{1}{Q^H_{PIRIP}(ID_i)})}$.

   Since $Q^H_{IBBE}(ID) = Q^H_{PIRIP}(ID)$ and

$$\begin{aligned} c_4 &= (c_2^x, c_2^{y \cdot \alpha})^{\Pi_{ID_i \in S}(\frac{1}{Q^H_{PIRIP}(ID_i)})} \\ &= (u \cdot t^{\alpha})^{k \cdot \Pi_{ID_i \in S} \frac{\gamma + Q^H_{PIRIP}(ID_i)}{Q^H_{PIRIP}(ID_i)}}. \end{aligned}$$

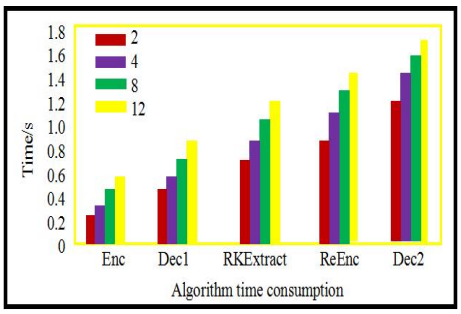

Figure 1: Time consumption of main algorithms

   C^*_{PIRIP} is an available ciphertext challenge ciphertext in the new scheme.

5) Second query stage. This stage is same as to first query stage.

6) Attacker A gives a guess result $b' \in 0, 1$. Attacker B sends b' to challenger C. If $b' = b$, it implies that A wins this game. The advantage is:

$$Adv^{IND-sID-CPA}_{PIRIP,A} = |Pr[b' = b] - \frac{1}{2}|.$$

   Attacker B successfully and efficiently simulates attacking IND-sID-CPA game. Completely, if attacker A successfully breaks through the IND-sID-CPA security of new scheme, thereby, attacker B also can successfully break through the IND-sID-CPA security based on identity stateless broadcast encryption scheme. Therefore, new scheme has the IND-sID-CPA security under random oracle model.

□

4 Experiments and Analysis

In this section, we make experiments to verify the effectiveness of our new scheme with experiment environment Windows8, 4GB memory, CPU3.3GHx and MATLAB R2014b. Bilinear map parameters: Elliptic curve group $y^2 = x^3 + Ax^2 + Bx$, where $A = B = 1$; polynomial $t^m + t^a + t^b + t^c + 1$, where $a = 356$, $b = 302$, $c = 288$; base field 2^m, $m = 378$; group *order* number $q = 2^m + 2^{\frac{m+1}{2}} + 1$.

Figure1 shows that the ratio between running time and time consumption of main algorithms. We test the running time of main algorithms with access points number 2, 4, 8, 12. The results imply that there is no relation between time consumption and node numbers. Though, access points number increases twice as previous time, time consumption only increases a little.

Our new scheme realizes the fine-grained access control. Table 1 shows performance comparisons between our proposed scheme (abbreviated in PRIRP) and the literatures of BDSBE [17], AMBE [20], PTR-ABE [7], CP-ABBE [4] in cloud environment.

Table 1: Function comparison

Scheme	IBE	SBE	FGAC
BDSBE	√	×	×
AMBE	√	√	×
PTR-ABE	×	√	×
CP-ABBE	×	√	√
PRIRP	√	√	√

IBE: identity-based encryption
SBE: Stateless broadcast encryption
FGAC: fine-grained access control.

Table 2: Enc_{PRE} function complexity comparison

Scheme	B	M	MI
BDSBE	$1+S$	$7+S$	$1+S$
AMBE	$2S+3$	$3S+2$	S
PTR-ABE	$2+S$	$2S+1$	$S+1$
CP-ABBE	$S+3$	$3+2S$	$1+2S$
PRIRP	0	$S+1$	1

Tables 2, 3, 4, 5 are the complexity comparisons of Enc_{PRE} function, $Dec1_{PRE}$ function, $RKExtract_{PRE}$ function and $Dec2_{PRE}$ function. The results present that our scheme costs less time consumption and function complexity. B: Bilinear map; M: Modular Exponentiation; MI: modular inversion calculation.

5 Conclusion

Currently, re-proxy encryption is a hot issue in the security cloud storage area. This paper fully combines the advantages of identity-based encryption, re-proxy encryption and stateless broadcast encryption to propose a novel broadcast and identity-based re-proxy encryption scheme. This new scheme makes up the weakness of traditional re-proxy encryption, which not only realizes the fine-grained access control, but the sender can generate re-proxy encryption key with a set unit to solve the efficiency of the multi-user request initial ciphertext and achieve the cloud security storage and the ciphertext sharing. The experimental results show that there is no positive correlation between the time overhead of system main function and the number of access points, new scheme can ensure the system efficiency with mass user access.

Table 3: $Dec1_{PRE}$ function complexity comparison

Scheme	B	M	MI
BDSBE	$1+2S$	$6+S$	$1+3S$
AMBE	$S+4$	$2S+1$	$2S$
PTR-ABE	$2-S$	$2S+1$	$S+1$
CP-ABBE	$S+4$	$2+S$	$2+2S$
PRIRP	2	$S-1$	2

Table 4: $RKExtract_{PRE}$ function complexity comparison

Scheme	B	M	MI
BDSBE	$2+S$	$6+2S$	$1+S$
AMBE	$2S+1$	$2S+7$	$6-2S$
PTR-ABE	$2+2S$	$3S+3$	$3S-1$
CP-ABBE	$4S+2$	$2+5S$	$5+S$
PRIRP	0	$S+5$	1

Table 5: $Dec2_{PRE}$ function complexity comparison

Scheme	B	M	MI
BDSBE	$4+3S$	$5+3S$	$2+S$
AMBE	$3S+2$	$3S+7$	$5+2S$
PTR-ABE	$3+2S$	$2S+4$	$2S+1$
CP-ABBE	$5S+3$	$3+2S$	$4+2S$
PRIRP	2	$S+1$	1

References

[1] M. Blaze, G. Bleumer, M. Strauss, "Divertible protocols and atomic proxy cryptography," in *International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg*, pp. 127-144, 1998.

[2] F. Deng, Y. Zhu, "Novel one-round certificateless group authenticated key agreement protocol (In Chinese)" *Computer Engineering & Applications*, vol. 53, no. 5, pp. 111-115, 2017.

[3] S. H. Islam, A. Singh, "Provably secure one-round certificateless authenticated group key agreement protocol for secure communications," *Wireless Personal Communications*, vol. 85, no. 3, pp. 879-898, 2015,

[4] S. Jin, Y. HU, "Full secure attribute-based broadcast encryption achieved through selective techniques," *DEStech Transactions on Environment, Energy and Earth Science*, 2016. (`file:///C:/Users/user/Downloads/4528-5543-1-SM.pdf`)

[5] J. Kim, W. Susilo, H. A. Man, J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 3, pp. 679-693, 2015.

[6] C. H. Lan, H. F. Li, S. L. Yin, L. Teng, "A new security cloud storage data encryption scheme based on identity proxy Re-encryption," *International Journal of Network Security*, vol. 19, no. 5, pp. 804-810, 2017.

[7] M. S. Lee, J. Lee, J. D. Hong, "An efficient public trace and revoke scheme using augmented broadcast encryption scheme," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 26, no. 1, pp. 17-30, 2016.

[8] Y. Li, W. Dai, Z. Ming, M. Qiu, "Privacy protection for preventing data over-collection in smart city," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1339-1350, 2016.

[9] H. Y. Li, H. F. Li, K. B. Wei, S. L. Yin, C. Zhao, "A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 2, pp. 413-422, Mar. 2017.

[10] K. Liang, L. Fang, D. S. Wong, W. Susilo, "A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds," *Concurrency & Computation Practice & Experience*, vol. 27, no. 8, pp. 2004-2027, 2015.

[11] K. Liang, H. A. Man, J. K. Liu, W. Susilo, "A DFA-based functional proxy Re-encryption scheme for secure public cloud data sharing," *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 10, pp. 1667-1680, 2014.

[12] J. Liu, S. L. Yin, H. Li, L. Teng, "A density-based clustering method for K-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[13] W. Liu, J. Liu, Q. Wu, B. Qin, Y. Li, "Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption," *International Journal of Information Security*, vol. 15, no. 1, pp. 35-50, 2016.

[14] A. Souyah, K. M. Faraoun, "Fast and efficient randomized encryption scheme for digital images based on quadtree decomposition and reversible memory cellular automata," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 715-732, 2016.

[15] L. Teng, H. Li, J. Liu, S. L. Yin, "A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.

[16] L. Teng, H. Li, "A high-efficiency discrete logarithm-based multi-proxy blind signature scheme," *International Journal of Network Security*, vol. 20, no. 6, pp.1200-1205, 2017.

[17] S. Wang, W. Yang, Y. Lin, "Balanced double subset difference broadcast encryption scheme," *Security & Communication Networks*, vol. 8, no. 8, pp. 1447-1460, 2015.

[18] P. Xu, T. Jiao, Q. Wu, W. Wang, H. Jin, "Conditional identity-based broadcast proxy Re-encryption and its application to cloud email," *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66-79, 2016.

[19] S. L. Yin, J. Liu, "A K-means approach for map-reduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov., 2016.

[20] J. Zhang, J. Mao, "Anonymous multi-receiver broadcast encryption scheme with strong security," *International Journal of Embedded Systems*, vol. 9, no. 2, pp. 177-187, 2017.

[21] Q. Zhang, L. T. Yang, X. G. Liu, Z. K. Chen, P. Li, "A tucker deep computation model for mobile multimedia feature learning," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 13, no. 3, pp. 1-39:18, 2017.

[22] H. Zhu, "A provable privacy-protection system for multi-server environment," *Nonlinear Dynamics*, vol. 82, no. 1, pp. 835-849, 2015.

[23] H. Zhu, X. Hao, "A provable authenticated key agreement protocol with privacy protection using smart card based on chaotic maps," *Nonlinear Dynamics*, vol. 81, no. 2, pp. 1-11, 2015.

Shoulin Yin received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016 and 2013 respectively. Now, he is a doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, Filter Algorithm, image processing and Data Mining. Email:352720214@qq.com.

Hang Li obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hang Li is a full professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Li had published more than 30 international journal and international conference papers on the above research fields. Email:910675024@qq.com.