

Security Analysis and Improvement of An Anonymous Attribute-Based Proxy Re-encryption

Hongjian Yin and Leyou Zhang(✉)

School of Mathematics and Statistics, Xidian University, Xi'an 710126, China
lyzhang@mail.xidian.edu.cn

Abstract. The ciphertext-policy attribute-based proxy re-encryption (CP-AB-PRE) is a flexible proxy re-encryption (PRE), which makes the encryptor control its encrypted data at a fine-grained level and update the access policy. However, most of constructions focuses only on the data security, rather than on user privacy protection. In order to protect users' attribute privacy, recently, a novel secure CP-AB-PRE named anonymous CP-AB-PRE was first proposed by Zhang et al. However, we found that their scheme fails to achieve anonymity, which means that their scheme cannot realize users' attribute privacy protection. In order to remedy this security gap, a novel anonymous CP-AB-PRE scheme is proposed, which can protect user attribute privacy by hiding the access policy. Theoretical analysis and simulation results demonstrate that our proposed scheme is secure and efficient.

Keywords: Attribute-based proxy re-encryption · Anonymity
Security · Privacy protection · Ciphertext-policy

1 Introduction

With the development of cloud computing, it has become a trend that more and more companies and individual users store their sensitive data by third parties such as Amazon, Google and Alibaba. In order to guarantee data confidentiality, these data should be encrypted before uploading. However, in many cases, it requires complex access control for protected data, that is, only can the user who satisfies some attributes get the protected data. Sahai and Waters [1] solved this issue by introducing the attribute-based encryption (ABE). Generally, there are two kinds of ABE involving ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In a CP-ABE scheme, the user secret keys are associated with a set of attributes and ciphertext is embedded with an access structure. The user will be able to decrypt the ciphertext only if the attributes associated with his secret keys satisfy the access structure of the ciphertext. In a KP-ABE scheme, users' secret keys are embedded with an access structure and ciphertext is associated with a set of attributes. Successful decryption of the ciphertext requires if

and only if the ciphertext attribute set satisfies the access structure associated with the user secret keys.

In 1998, Blaze et al. [5] proposed the first PRE scheme in public key cryptosystem. In their scheme, it allows a proxy to translate a ciphertext encrypted under Alice's public key into one that can be decrypted by Bob's secret key. In 2008, Guo et al. [9] proposed the first attribute-based proxy re-encryption (AB-PRE) scheme in the type of key policy. Subsequently, the first ciphertext policy attribute-based proxy re-encryption scheme was proposed by Liang et al. [10]. In CP-AB-PRE schemes, a proxy is specified by users in advance. The proxy can receive a proxy re-encryption key to transform a ciphertext associated with an access policy into another one with a new policy. After the first CP-AB-PRE scheme, many PRE schemes based on CP-ABE have been presented [11, 18, 19]. In these schemes, access structures are embedded in the ciphertext and whoever obtains the ciphertext can see the content of the access structure. However, in some cases, the access structure may be sensitive. For example, in military applications, the access structures may contain military secrets, such as sensitive information like organizational structure.

In order to protect users' privacy, Zhang et al. [15] proposed an anonymous CP-AB-PRE recently. In this scheme, they claimed that their scheme was the first one that made access structure hidden and access policy update simultaneously. Unfortunately, we found that their scheme cannot achieve anonymity, in other words, any malicious user can only utilize public parameters to determine whether the ciphertexts are encrypted under the given access structure or not.

In this paper, we first give the security analysis of Zhang et al.'s scheme and show that their scheme does not realize users' attribute privacy protection. Then we propose an improvement scheme to remedy their security gap. In our proposed scheme, the attribute privacy is protected by hiding the access policy. In the standard model, the proposed scheme is proved to be secure.

2 Preliminaries

2.1 Hardness Assumptions

Decisional Bilinear Diffie-Hellman (DBDH) assumption. Let $a, b, c, z \in_R \mathbb{Z}_p$, and $g \in_R \mathbb{G}$ be a generator. The DBDH assumption holds in group \mathbb{G} if no probabilistic polynomial-time (PPT) algorithm can distinguish the tuple $[g, g^a, g^b, g^c, e(g, g)^{abc}]$ from $[g, g^a, g^b, g^c, g^z]$ with non-negligible advantage.

The Decision Linear (D-Linear) Assumption. Suppose $g \in_R \mathbb{G}$ is a generator and $a_1, a_2, a_3, a_4, z \in_R \mathbb{Z}_p$. The D-Linear assumption is said to hold in \mathbb{G} if no PPT algorithm can distinguish the tuple $[g, g^{a_1}, g^{a_2}, g^{a_1 a_3}, g^{a_2 a_4}, g^{a_3 + a_4}]$ from $[g, g^{a_1}, g^{a_2}, g^{a_1 a_3}, g^{a_2 a_4}, g^z]$ with an advantage non-negligible.

The Computational Bilinear Diffie-Hellman (CBDH) Assumption. Suppose $g \in_R \mathbb{G}$ is a generator and $a, b, c \in_R \mathbb{Z}_p$. We say that the CBDH assumption holds in \mathbb{G} if given $[g, g^a, g^b, g^c]$, no PPT algorithm can compute $e(g, g)^{abc}$ with an advantage non-negligible.

2.2 Definitions Anonymous of CP-AB-PRE Scheme

An anonymous CP-AB-PRE scheme consists of the following six algorithms:

Setup: This algorithm takes the security parameter λ as input and generates a public key PK , a master secret key MK .

KeyGen: This algorithm takes MK and a set of attributes L as input and generates a secret key SK_L associated with L .

Encrypt: This algorithm takes PK , a message \mathcal{M} , and an access policy W as input, and generates a ciphertext CT_W .

RKGen: This algorithm takes a secret key SK_L and an access policy W' as input and generates a re-encryption key $RK_{L \rightarrow W'}$.

Reencrypt: This algorithm takes a re-encryption key $RK_{L \rightarrow W'}$ and a ciphertext CT_W as input, first checks whether the attribute list in $RK_{L \rightarrow W'}$ satisfies the access policy of CT_W or not. If check passes, it generates a re-encrypted ciphertext $CT'_{W'}$; otherwise, it returns \perp .

Decrypt: This algorithm takes CT_W and SK_L associated with L as input and returns the message \mathcal{M} if the attribute list L satisfies the access policy W specified for CT_W . If $L \not\models W$, it returns \perp .

2.3 Security Model

The indistinguishability against selective ciphertext-policy and chosen-plaintext attacks (IND-sCP-CPA) model [2,3,5] and the selective master key security (sMKS) model [6] are described as follows.

IND-sCP-CPA Game

Init: \mathcal{A} submits two challenge ciphertext policies W_0^* and W_1^* to the challenger.

Setup: The challenger runs the Setup algorithm and outputs the public key PK to the adversary \mathcal{A} .

Phase 1: The adversary \mathcal{A} queries the following oracles in polynomial time:

(i) KeyGen oracle: \mathcal{A} submits an attribute list L , the challenger returns SK_L if $(L \not\models W_0^* \wedge L \not\models W_1^*)$ or $(L \models W_0^* \wedge L \models W_1^*)$. Otherwise, it outputs \perp .

(ii) RKGen oracle: The adversary \mathcal{A} submits L and W , if $(L \not\models W_0^* \wedge L \not\models W_1^*)$ or $(L \models W_0^* \wedge L \models W_1^*)$, the challenger returns \mathcal{A} the re-encryption key $RK_{L \rightarrow W}$. Otherwise, it outputs \perp .

(iii) Reencrypt oracle: \mathcal{A} submits L , W' and an anonymous ciphertext CT_W under an access policy W , if $((L \not\models W_0^* \wedge L \not\models W_1^*)$ or $(L \models W_0^* \wedge L \models W_1^*)$) and $L \models W$, the challenger gives \mathcal{A} $CT_{W'}$. Otherwise, it outputs \perp .

Challenge: Once Phase 1 is over, \mathcal{A} outputs two equal length messages \mathcal{M}_0 and \mathcal{M}_1 . It is required that $\mathcal{M}_0 = \mathcal{M}_1$ if any secret key on L satisfying $L \models W_0^* \wedge L \models W_1^*$ has been queried. The challenger randomly chooses a bit $\nu \in \{0, 1\}$, computes $CT_{W_\nu^*} = \text{Encrypt}(PK, \mathcal{M}_\nu, W_\nu^*)$ and sends $CT_{W_\nu^*}$ to \mathcal{A} , where W_ν^* is hidden.

Phase 2: It is similar to Phase 1.

Guess: \mathcal{A} outputs a bit $\nu' \in \{0, 1\}$ as a guess of ν and it wins the aforementioned game if $\nu' = \nu$.

In the above game, we define the advantage of \mathcal{A} as $Adv_0^{\mathcal{A}} = |Pr[\nu' = \nu] - 1/2|$. In this model, it is required in the challenge phase that $\mathcal{M}_0 = \mathcal{M}_1$ if the adversary obtains a secret key SK_L matching both W_0^* and W_1^* . Otherwise, the adversary can directly decrypt the challenge ciphertext to get the bit value ν . Hence, it easily follows that the security models of anonymous CP-AB-PRE would make no sense without such a restriction.

sMKS Game

Init: \mathcal{A} submits an attribute list L^* to the challenger.

Setup: The same as that of IND-sCP-CPA game.

Queries: \mathcal{A} queries the following oracles in polynomial time:

- (i) KeyGen oracle: \mathcal{A} submits an attribute list L , if $L \neq L^*$, SK_L is returned by the challenger to \mathcal{A} . Otherwise, it outputs \perp .
- (ii) RKGen oracle: \mathcal{A} submits L and W , the challenger generates a proxy re-encryption key $RK_{L \rightarrow W}$ for \mathcal{A} .
- (iii) Reencrypt oracle: \mathcal{A} submits L , W' , and CT_W under an access policy W , the challenger returns CT'_W as a re-encryption ciphertext to \mathcal{A} . Note that, the access policy W is not revealed in CT'_W to achieve anonymity.

Output: \mathcal{A} outputs an attribute secret key SK_{L^*} , and it succeeds if SK_{L^*} is valid for L^* .

In this game, the advantage of \mathcal{A} is defined $Adv_1^{\mathcal{A}} = Pr[\mathcal{A} \text{ succeeds}]$.

Definition 1. *An anonymous CP-AB-PRE scheme is selective master key security if no probabilistic polynomial time adversary \mathcal{A} has a non-negligible advantage in winning the master key security game.*

3 Security Analysis of Zhang et al.'s Scheme

In this section, we will show that Zhang et al.'s scheme has the weakness of anonymity, in other words, it cannot realize ciphertext policy hidden. In the following, we explain why the above scheme is not anonymous.

Some parts of ciphertexts and public keys g , $T_{i,t}$, $C_{i,t,\Delta}$ and C'_0 is a Decision DiffieHellman (DDH) tuple, from which the attribute information $T_{i,t}$ can be revealed. More precisely, for an attribute $T_{i,t}$, an attacker can run the DDH test $e(\prod_{i \in W} C_{i,t,\Delta}, g) \stackrel{?}{=} e(\prod_{i \in W'} T_{i,t}, C'_0)$ because g and $T_{i,t}$ are public keys, then the attacker can determine whether W' is used in ciphertext or not, that is, for attribute $T_{i,t}$ or not. In conclusion, the DDH test attack work successfully due to $C_{i,t,\Delta}$ and C'_0 which are used in matching phase only.

4 An Improved Scheme and Proof of Security

4.1 An Improved Scheme

From the security analysis, we can know that, the main issue is in original match-then-re-encrypt technique. To fill this security gap, we propose a novel

match-then-re-encrypt technique replace the one used in Zhang et al.'s scheme. From this simple modification, our scheme achieves anonymity without losing any feature of anonymous CP-AB-PRE. The following is our construction.

Setup (1^λ). Attribute authority chooses $g_2, g_3 \in_R \mathbb{G}$ and $y \in_R \mathbb{Z}_p$. For each attribute w_i with $1 \leq i \leq n$, it chooses $a_{i,t}, b_{i,t}, \tau_{i,t} \in_R \mathbb{Z}_p$ and computes $T_{i,t} = g^{\tau_{i,t}}$, $g_1 = g^y$, $Y = e(g_1, g_2)$, $A_{i,t} = T_{i,t}^{a_{i,t}}$, $B_{i,t} = T_{i,t}^{b_{i,t}}$, where $1 \leq i \leq n, 1 \leq t \leq n_i$. Then it chooses $w \in_R \mathbb{G}$, $\alpha, t_0, t_1, t_2, t_3 \in_R \mathbb{Z}_p$, and $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in_R \mathbb{Z}_p$ and computes $v = g^{t_1}$, $u = g^{t_2}$, $V = g^{t_3}$, $w = g^{t_0}$, $g_0 = v^\alpha$, $g_{0i} = g^{\beta_i}$, $g_{1i} = g^{\alpha_i}$, $A = e(g_0, g_2)$. The system public key $PK = \langle g, g_0, g_1, g_2, g_3, Y, A, u, v, V, w, \{g_{0i}, g_{1i}, \{T_{i,t}, A_{i,t}, B_{i,t}\}_{1 \leq t \leq n_i}\}_{1 \leq i \leq n} \rangle$ and master key $MK = \langle g_2^y, y, \{\alpha_i, \beta_i, \{a_{i,t}, b_{i,t}, \tau_{i,t}\}_{1 \leq t \leq n_i}\}_{1 \leq i \leq n} \rangle$.

KeyGen (PK, MK, L). After receiving an attribute $A^* = [A_1^*, A_2^*, \dots, A_n^*]$, where $A_i^* \in \{0, 1\}$ with $i \in [1, n]$, the attribute authority computes $h_i = (h_{i-1})^{\alpha_i^* \beta_i^{1-A_i^*}}$, $d_\Delta = g_3^{\hat{d}}$, $d_0 = g_2^s h_n^\gamma$, $d_1 = v^\gamma$, $d_2 = w^\gamma$, $d_3 = u^{\gamma t_1}$ and $d_4 = V^{\gamma t_1}$ where $\gamma \in_R \mathbb{Z}_p$, $h_0 = g$. Then it picks random elements $\{r_i, \lambda_i \in_R \mathbb{Z}_p\}_{1 \leq i \leq n}$, sets $r = \sum_{i=1}^n r_i$. For $1 \leq i \leq n$, it computes $[D_0, D_{i,0}, D_{i,1}, D_{i,2}] = [g_2^{y-r}, g_2^{r_i} B_{i,k_i}^{\lambda_i \alpha_i, k_i}, g^{\lambda_i \alpha_i, k_i}, g^{\lambda_i \beta_i, k_i}]$. Then, $SK_L = \langle d_\Delta, d_0, d_1, d_2, d_3, d_4, D_0, \{D_{i,0}, D_{i,1}, D_{i,2}\}_{1 \leq i \leq n} \rangle$.

Encrypt (PK, M, W). To encrypt $M \in \mathbb{G}_T$ under an access policy $W = [W_1, W_2, \dots, W_n]$, data owner chooses $s, s', s_{1i}, s_{2i} \in_R \mathbb{Z}_p$, $s_1 = \sum_{i=1}^n s_{1i}$, $s_2 = \sum_{i=1}^n s_{2i}$ and computes $\tilde{C} = MY^s$, $C_0 = g^s$, $C_{RE} = g_3^s$, $C'_i = h_n^{s_{1i}} u^{s_{2i}}$, $C'_0 = A_1^s$, $C'_1 = w^{s_1} V^{s_2}$, $C'_2 = g^{s_2}$, $C'_3 = v^{s_1}$. And data owner computes $[C_{i,t,1}, C_{i,t,2}] = [B_{i,t}^{s-s'}, A_{i,t}^{s'}]$, if $v_{i,t} \in W_i$. Otherwise, $[C_{i,t,\Delta}, C_{i,t,1}, C_{i,t,2}]$ are random elements in \mathbb{G} . Then the ciphertext of M with respect W is $CT_W = \langle C_0, C_{RE}, \tilde{C}, C'_0, C'_1, C'_2, C'_3, \{\{C_{i,t,1}, C_{i,t,2}\}_{1 \leq t \leq n_i}, C'_i\}_{1 \leq i \leq n} \rangle$.

RKGen (SK_L, W'). This algorithm takes SK_L and W' as input. Then it chooses $d \in_R \mathbb{Z}_p$ and computes g^d , $\hat{d}_\Delta = d_\Delta g_3^d$, $\hat{d}_0 = d_0$, $\hat{d}_1 = d_1$, $\hat{d}_2 = d_2$, $\hat{d}_3 = d_3 d_\Delta$, $\hat{d}_4 = d_4 g_3^d$, $\hat{D}_0 = D_0$, $\hat{D}_{i,0} = D_{i,0} g_3^d$, $\hat{D}_{i,1} = D_{i,1}$, $\hat{D}_{i,2} = D_{i,2}$, $\mathbb{C} = \text{Encrypt}(PK, E(g^d), W')$. Then, the proxy re-encryption key corresponding W' is $RK_{L \rightarrow W'} = \langle \hat{D}_\Delta, \{\hat{D}_{i'}\}_{i'=1,2,3,4}, \{\hat{D}_0, \hat{D}_{i,0}, \hat{D}_{i,1}, \hat{D}_{i,2}\}_{1 \leq i \leq n}, \mathbb{C} \rangle$.

Reencrypt ($RK_{L \rightarrow W'}, CT_W$). Upon receiving $RK_{L \rightarrow W'}$ for W' , and CT_W under W , proxy server does the following without knowing W :

Matching Phase: The proxy server computes $C'_\Delta = e(C'_2, \hat{d}_\Delta)$ and checks whether $L \models W$ in terms of the following Equation (1). Specifically, $L \models W$ if and only if Equation (1) holds

$$C'_0 C'_\Delta = \frac{e(\hat{d}_0, C'_3) e(\hat{d}_3 \hat{d}_4, C'_2) e(\hat{d}_2, C'_3)}{e(C'_1, \hat{d}_1) e(\prod_{i=1}^n C'_i, \hat{d}_1)}, \quad (1)$$

where suppose the indexes satisfy $L_i = v_{i, k_i}$. It returns \perp if $L \not\models W$. Otherwise, it initiates the Re-encryption Phase.

Re-encryption Phase: The proxy server computes

$$E_i = \frac{e(C_0, \hat{D}_{i,0})}{e(C_{i,t,1}, \hat{D}_{i,1}) e(C_{i,t,2}, \hat{D}_{i,2})} = e(g, g_2)^{sr_i} e(g, g_3)^{sd}. \quad (2)$$

Subsequently, it computes $\tilde{C} = e(C_0, D'_0) \prod_{i=1}^n E_i = e(g, g_2)^{ys} e(g, g_3)^{nsd}$, and outputs a proxy re-encryption ciphertext $CT_{W'} = \langle \tilde{C}, C_{RE}, \tilde{C}, \mathbb{C} \rangle$. It follows from the subsequent Decrypt algorithm that the decryptor of re-encryption ciphertext only needs g^d to decrypt the proxy re-encryption ciphertext. Thus, we can obtain a two-time proxy re-encryption ciphertext $CT_{W''} = \langle \tilde{C}, C_{RE}, \tilde{C}, \mathbb{C}' \rangle$, where \mathbb{C}' is generated based on the algorithm Reencrypt with the ciphertext \mathbb{C} and another proxy re-encryption key $RK_{L' \rightarrow W''}$ as inputs. Specifically, $\mathbb{C}' = \text{Reencrypt}(PK, RK_{L' \rightarrow W''}, \mathbb{C})$. Similarly, the multiple time proxy re-encryption ciphertexts can be generated.

Decrypt (CT_W, SK_L). The ciphertext CT_W is tested and decrypted by a user with secret key SK_L as follows:

1. If CT_W is an original ciphertext, the user does the following:

Matching Phase: The user checks whether $L \models W$ in terms of the following Eq. (3). Suppose the indexes satisfy $L_i = v_{i,k_i}$, $L \models W$ if and only if Eq. (3) holds

$$C'_0 = \frac{e(d_0, C'_3)e(d_3d_4, C'_2)e(d_2, C'_3)}{e(C'_1, d_1)e(\prod_{i=1}^n C'_i, d_1)}. \quad (3)$$

If $L \not\models W$, it returns \perp . Otherwise, it initiates the Decryption Phase.

Decryption Phase: Suppose $L_i = v_{i,k_i}$, the user computes

$$\mathcal{M} = \frac{\tilde{C} \prod_{i=1}^n e(C_{i,k_i,1}, D_{i,k_i,1})e(C_{i,k_i,2}, D_{i,k_i,2})}{e(C_0, D_0) \prod_{i=1}^n e(C_0, D_{i,0})} \quad (4)$$

2. Else if CT_W is a one-time proxy re-encryption ciphertext consists of $\langle \tilde{C}, C_{RE}, \tilde{C}, \mathbb{C} \rangle$, the user does the following:

Matching Phase: The user checks whether $L \models W$ in accordance with \mathbb{C} by using the method in Eq. (3). If $L \not\models W$, the algorithm returns \perp . Otherwise, it initiates the Decryption Phase.

Decryption Phase: The user does

- Performs a decryption of the original ciphertext \mathbb{C} of $E(g^d)$ using the secret key SK_L and decodes it to g^d .
 - Computes $\frac{\tilde{C}e(C_{RE}, g^d)^n}{\tilde{C}} = \mathcal{M}$.
3. Else, if $CT_W = \langle \tilde{C}, C_{RE}, \tilde{C}, \mathbb{C}' \rangle$ is an $N + 1$ time proxy re-encryption ciphertext, where \mathbb{C}' is an N time proxy re-encryption ciphertext of $E(g^d)$, then the user does the following:
 - Performs a decryption of the N time proxy re-encryption ciphertext \mathbb{C}' . If the algorithm does not return \perp , the user recovers $E(g^d)$, decodes it to g^d and proceeds.
 - Computes $\frac{\tilde{C}e(C_{RE}, g^d)^n}{\tilde{C}} = \mathcal{M}$.

4.2 Proof of Security

Theorem 1. *The anonymous CP-AB-PRE scheme is secure in the IND-sCP-CPA model, under the DBDH assumption and the D-Linear assumption.*

Theorem 2. *The anonymous CP-AB-PRE scheme is sMKS secure Under the CBDH assumption.*

The Theorems 1 and 2 can be proved secure according to [15]. Due to space limitations, detailed proofs will be given in the full version.

5 Performance Analysis

In this section, we compare our work with previous work with regard to security and efficiency. For convenience, $|PK|$, $|SK|$, $|OCT|$ and $|CT|$ denote the size of the public key, the secret key, the original ciphertext and the re-encryption ciphertext. $|G|$ and $|G_T|$ denote the bit-length of the elements in \mathbb{G} and \mathbb{G}_T . Let n be the number of all attributes in the system, N express the total number of possible values of all attributes. m is the number of attribute held by user and k denotes the total number of attributes required by the ciphertext (Tables 1 and 2).

Table 1. Security comparison among different AB-PRE schemes

| Scheme | Access structure | Anonymity | Security | Hardness |
|--------|------------------|-----------|-----------|----------------------|
| [14] | LSSS | No | Adaptive | DBDH, SUF.Sig* |
| [15] | AND | No | Selective | DBDH, D-Linear, CBDH |
| [19] | LSSS | No | Adaptive | q -parallel BDHE |
| Ours | AND | Yes | Selective | DBDH, D-Linear, CBDH |

*Strong unforgeability of one-time signature.

Table 2. Communication cost comparison among different AB-PRE schemes

| Scheme | $ PK $ | $ SK $ | $ OCT $ | $ RCT $ |
|--------|---------------------------|---------------|------------------------|-----------------------|
| [15] | $(3N + 4) G + G_T $ | $(4m + 4) G $ | $(3k + 3) G + 2 G_T $ | $ G + 3 G_T $ |
| [19] | $(n + 6) G + G_T $ | $(m + 3) G $ | $(2k + 5) G + G_T $ | $(2k + 5) G + G_T $ |
| Ours | $(3N + n + 9) G + G_T $ | $(3m + 7) G $ | $(3k + 5) G + 2 G_T $ | $ G + 3 G_T $ |

Our proposed construction is efficient in the size of the re-encryption ciphertext. Although, other schemes are little more efficient in the size of the public key, the secret key and the original ciphertext, these schemes cannot achieve user privacy protection. In order to simulate, we use the pairing-based cryptography library. The simulation experiment is done on a Windows machine with 2.67 GHz Intel(R) Core(TM) 2 Quad CPU and 4 GB ROM. The Fig. 1 shows that the re-encryption cost of our scheme is better than other schemes. In addition, our Key-Gen cost and Encryption cost is good. However, in order to achieve anonymity, it costs more time to decrypt the original ciphertext.

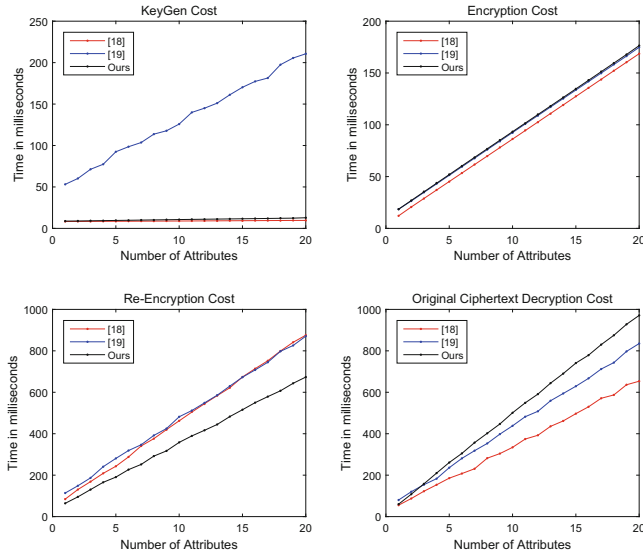


Fig. 1. Computational costs comparison among different CP-AB-PRE schemes

6 Conclusions

In this paper, we give the security analysis of Zhang et al.'s scheme and show why their scheme does not realize users' attribute privacy protection. In order to remedy this security gap, a novel scheme is proposed based on the match-then-re-encrypt and match-then-re-decrypt technique. In our scheme, the attribute privacy is protected in access policy. And it is efficient in re-encryption ciphertext size. From the analysis of safety and efficiency, the improved scheme achieves anonymity without losing any feature of Zhang et al.'s scheme.

References

1. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
2. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334 (2007)
3. Goyal, V., Pandey, O., Sahai, A., et al.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security, pp. 89–98 (2006)
4. Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535–554. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-70936-7_29
5. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144. Springer, Heidelberg (1998). <https://doi.org/10.1007/BFb0054122>

6. Ateniese, G., Fu, K., Green, M., et al.: Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.* **9**(1), 1–30 (2006)
7. Canetti, R., Hohenberger, S.: Chosen-ciphertext secure proxy re-encryption. In: *ACM Conference on Computer and Communications Security*, pp. 185–194 (2007)
8. 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
9. Guo, S., Zeng, Y., Wei, J., et al.: Attribute-based re-encryption scheme in the standard model. *Wuhan Univ. J. Nat. Sci.* **13**(5), 621–625 (2008)
10. Liang, X., Cao, Z., Lin, H., et al.: Attribute based proxy re-encryption with delegating capabilities. In: *International Symposium on Information, Computer, and Communications Security*, pp. 276–286 (2009)
11. Luo, S., Hu, J., Chen, Z.: Ciphertext policy attribute-based proxy re-encryption. In: Soriano, M., Qing, S., López, J. (eds.) *ICICS 2010*. LNCS, vol. 6476, pp. 401–415. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17650-0_28
12. Liu, Q., Wang, G., Wu, J.: Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. *Inf. Sci.* **258**(3), 355–370 (2014)
13. Zhang, L., Wu, Q., Mu, Y., et al.: Privacy-preserving and secure sharing of PHR in the cloud. *J. Med. Syst.* **40**(12), 1–13 (2016)
14. Kawai, Y., Takashima, K.: Fully-anonymous functional proxy-re-encryption. *IACR Cryptology EPrint Archive 2013*, p. 318 (2013)
15. Zhang, Y., Li, J., Chen, X., et al.: Anonymous attribute-based proxy re-encryption for access control in cloud computing. *Secur. Commun. Netw.* **9**(14), 2397–2411 (2016)
16. Shao, J.: Anonymous ID-based proxy re-encryption. In: Susilo, W., Mu, Y., Seberry, J. (eds.) *ACISP 2012*. LNCS, vol. 7372, pp. 364–375. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31448-3_27
17. Abdalla, M., Catalano, D., Fiore, D.: Verifiable random functions from identity-based key encapsulation. In: Joux, A. (ed.) *EUROCRYPT 2009*. LNCS, vol. 5479, pp. 554–571. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01001-9_32
18. Liang, K., Fang, L., Susilo, W., et al.: A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. In: *International Conference on Intelligent Networking and Collaborative Systems*, pp. 552–559 (2013)
19. Liang, K., Man, H.A., Liu, J.K., et al.: A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. *Future Gener. Comput. Syst.* **52**(C), 95–108 (2015)
20. Zhang, Y., Chen, X., Li, J., et al.: Anonymous attribute-based encryption supporting efficient decryption test. In: *ACM SIGSAC Symposium on Information, Computer and Communications Security*, pp. 511–516 (2013)