Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2016, Article ID 5235714, 12 pages
http://dx.doi.org/10.1155/2016/5235714

Research Article

Efficient and Adaptively Secure Attribute-Based Proxy Reencryption Scheme

Huixian Li[1] and Liaojun Pang[2]

[1]*School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China*
[2]*State Key Laboratory of Integrated Services Networks, School of Life Science and Technology, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Huixian Li; lihuixian@nwpu.edu.cn

Received 8 January 2016; Revised 31 March 2016; Accepted 26 April 2016

Academic Editor: Mauro Conti

Ciphertext-Policy Attribute-Based Proxy Reencryption (CP-ABPRE) has found many practical applications in the real world, because it extends the traditional Proxy Reencryption (PRE) and allows a semitrusted proxy to transform a ciphertext under an access policy to the one with the same plaintext under another access policy. The existing CP-ABPRE schemes were proven secure only in the selective security model, a limited model, which is an unnatural constraint on the attacker. The scheme proved in this model can only be called selectively secure one. However, from a security perspective, the adaptively secure CP-ABPRE scheme is more desirable. In this paper, an adaptively secure CP-ABPRE scheme is proposed, which is based on Waters' dual system encryption technology. The proposed scheme is constructed in composite order bilinear groups and proven secure under the complexity assumptions of the subgroup decision problem for 3 primes (3P-SDP). Analyses show that our proposal provides higher computational efficiency compared with the existing schemes.

1. Introduction

With the development of Internet and open distributed networks, the Attribute-Based Encryption (ABE) scheme [1] has drawn great attention of researchers in recent years. Unlike the Public Key Encryption mechanism, ABE scheme takes attributes as the public key and associates the ciphertext and user's secret key with attributes, so that it provides more flexible access control mechanism over encrypted data. This dramatically reduces the cost of network bandwidth and sending node's operation in fine-grained access control of data sharing. Therefore, ABE has a broad prospect in the large-scale distributed applications to support one-to-many communication mode. Traditional ABE has two variants according to the form of access policy: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) [2]. In a KP-ABE system, ciphertexts are associated with attribute sets and secret keys are associated with access policies. However, CP-ABE is complementary, and the sender could specify access control policy, so, compared with KP-ABE schemes, CP-ABE schemes are more suitable for the realistic scenes.

As the research and application of the ABE go ahead, Proxy Reencryption (PRE) [3] has been introduced into ABE schemes. Considering such a scenario, in the email forwarding, Alice is going on vacation and wishes the others like Bob could still read the message in her encrypted emails. With an Attribute-Based Proxy Reencryption (ABPRE) system, in which a proxy is allowed to transform a ciphertext under a specified access policy into the one under another access policy, she could meet her intentions without giving her secret key to either the mail server or Bob. So ABPRE schemes [4] are needed in most of practical network applications, especially Ciphertext-Policy ABPRE (CP-ABPRE) schemes [5], which have more flexible access control policy than Key-Policy ABPRE (KP-ABPRE) schemes [4]. Generally speaking, an ABPRE scheme has an authority, a sender, a user called a delegator who needs to delegate his/her decryption ability to someone else, a proxy who helps the delegator to generate a reencrypted ciphertext, and some receivers as participants. Recently, due to their widespread use in the realistic scenes, widespread attention was paid to ABPRE schemes by researchers and some excellent ABPRE schemes have been proposed [6–12].

However, most of existing ABPRE schemes [6–12] were proven secure only in the selective security model [13], in which an adversary must firstly choose an attack target before the public parameters are published. This restriction on an attacker was not natural, which causes attackers to behave differently from the way in a real environment. And most of existing schemes [11–15] demanded a number of paring operations, which indeed costs much in the communications. Therefore, motivated by these concerns, an efficient and adaptively secure CP-ABPRE scheme is proposed in our paper. Our scheme overcomes the restriction on an attacker in a selective security model and could be better applied to the open distributed networks. In the meantime, our proposal supports any monotone access formulas and costs less computational overhead compared with the existing schemes.

The rest of this paper is organized as follows. In the next section, we shall briefly review related works in the field of ABE. In Section 3, some preliminaries including complexity assumptions, access structures, and CP-ABPRE model are provided. Then, the concrete CP-ABPRE scheme is given in Section 4. In Section 5, we analyze the correctness and security of our scheme and compare our scheme with existing schemes in terms of access structure, security, and computations efficiency. Finally, the conclusion is drawn in Section 6.

2. Related Works

In 2005, Sahai and Waters [16] proposed a new type of IBE [17] called Fuzzy IBE (FIBE) which regards identities as a set of descriptive attributes. It is often regarded as the first concept of ABE [1, 18]. ABE can be categorized as either KP-ABE or CP-ABE, and the latter is more flexible and more suitable for the realistic scenes [2]. In 2007, Cheung and Newport [19] used AND gates on positive and negative to express attributes in order to achieve their CP-ABE scheme's access policy and proved the security under the DBDH assumption. And then Nishide et al. [20] designed a new CP-ABE scheme with AND gates on multivalue attributes as its access policy. To realize fine-grained access control strategy, Bethencourt et al. [21] used the Access Tree in their scheme. In order to design CP-ABE schemes with flexible strategy under the DBDH assumption, Goyal et al. [22] and Liang et al. [23] adopted Bounded Access Tree, respectively. Later, Ibraim et al. [24] used the general Access Tree to eliminate the boundary constraints in the literature [22, 23]. In 2011, Waters [25] used Linear Secret Sharing Scheme (LSSS) access structure under q-PBDHE assumption to construct a CP-ABE scheme.

However, unfortunately, the security of those CP-ABE schemes that we mentioned above was proven in a weaker security model, called the selective-policy security model which derived from the selective-ID security model for constructing an IBE scheme without the random oracle model [26]. In the selective security model, the adversary must firstly declare which policy he wishes to be challenged on before the public parameters are published. This restriction on the attacker is not natural, which causes attacker to behave differently from the real environment [13]. Considering the restrictions of the selective security model, researchers expected that the ABE scheme should be designed and proven secure under the adaptive security model. So, in order to overcome the drawbacks of the selectively secure ABE schemes, Lewko et al. [13] proposed an adaptively (or fully) secure ABE scheme by using the dual system encryption technique [27] which is a common method for proving an adaptively secure scheme in IBE or ABE. Later, Lewko and Waters [28] provided a new methodology which can transform the selectively secure schemes to adaptively secure ones and presented a CP-ABE scheme that is proven fully secure. In 2014, Garg et al. [29] constructed the first fully secure ABE scheme that can handle access control policies expressible as polynomial-size circuits. Afterwards, some excellent adaptively secure ABE schemes were proposed [3, 30, 31].

Recently, in the field of cryptography, the concept of PRE has been proposed to make data sharing more efficient. Introduced by Mambo and Okamoto [32] and first defined by Blaze et al. [33], PRE can support the delegation of decryption rights, which is never considered in extending the traditional Public Key Encryption (PKE). In PRE, a semitrusted proxy is enabled to transform a ciphertext encrypted under one's public key into a new ciphertext intended for others with the plaintext unchanged. The decryption proxy, however, can learn nothing about the secret key or the plaintext. Due to these characteristics, PRE has many practical applications. For example, Xu et al. [34] built an encrypted cloud email system with PRE, which allows a user to send an encrypted email to multiple receivers, store his encrypted emails in an email server, and review his history. In addition, it can also be used in secure distributed files systems, cloud storage, on-line Electronic Medical Record (EMR), and so on [4, 5, 35–39].

To date, PRE has been extended to adapt different cryptographic systems. The ABPRE is one of the extensions in which a user is able to empower designated users to decrypt reencrypted ciphertext by deploying attributes. In 2008, Guo et al. [40] proposed the first ABPRE scheme and it is also the first KP-ABPRE scheme. In 2009, Liang et al. [6] proposed the first CP-ABPRE scheme, in which the proxy is enabled to transform a given ciphertext under a specified access policy into the one under another access policy. But, unfortunately, only AND gates on positive and negative attributes are supported by their access policy. In 2010, Luo et al. [7] proposed a new CP-ABPRE scheme which supports AND gates on multivalue and negative attributes. Compared with [6], it has a new property named reencryption control which means that the user can decide which ciphertext can be reencrypted later during the encryption process. Later, Seo and Kim [8] presented another CP-ABPRE scheme which only needs a constant number of bilinear pairing operations. So the computation cost and ciphertext length are reduced significantly compared to previous schemes [7, 27]. In 2013, Li [9] presented a new CP-ABPRE scheme in which the ciphertext policy is matrix access policy based on LSSS matrix access structure. In 2014, Chung et al. [10] analyzed these CP-ABPRE schemes [6–8, 33] and made comparisons of them by some criteria. The aforementioned CP-ABPRE schemes, however, are only CPA-secure. To tackle this

problem, Liang et al. [11], for the first time, proposed a new single-hop unidirectional CP-ABPRE scheme supporting any monotonic access formulas. Despite being constructed in the random oracle model, it is proved to be CCA-secure. In 2015, Kawai [12] proposed a flexible CP-ABPRE scheme in which the reencryption key generation can be outsourced in Attribute-Based Encryption and proved their scheme is secure in the selective security model.

All these CP-ABPRE schemes mentioned above, unfortunately, were only proven to be selectively secure [13], which is just discussed above. A CP-ABPRE system with selective security, which limits an adversary to choose an attack target before playing a security game, might not scale well in practice as well. This is because a realistic adversary is able to adaptively choose his attack target when attacking a cryptosystem. Therefore, an adaptively secure CP-ABPRE scheme is extremely desirable in most practical network applications. In 2014, Liang et al. [14], for the first time, formalized the notion of adaptive security for CP-ABPRE systems and proposed a new CP-ABPRE scheme, which is proven adaptively secure in the standard model, but their scheme demands a number of paring operations that imply huge computational overheads. In 2015, Backes et al. [15] presented an Inner-Product Proxy Reencryption scheme. Although their scheme can easily be converted into an Attribute-Based Proxy Reencryption scheme, the ciphertext is only associated with AND gates access structure, which does not conform to the flexible access policy. Motivated by these concerns, in this paper, we propose an efficient and adaptively secure CP-ABPRE scheme which supports any monotone access formulas.

Our contributions can be briefly outlined as follows. (1) A new scheme is proposed and it overcomes the restriction on the attacker in a selective security model in the existing schemes [6–9, 11] and is proved to be adaptively secure. (2) Our proposal supports any monotone access formulas including what the AND gate access structure supports. (3) Our scheme costs less computational overhead compared with the corresponding scheme [14]. (4) We try to construct our scheme in composite order groups and use three assumptions to prove its security.

3. Preliminaries

3.1. Composite Order Bilinear Groups. Composite order bilinear groups were introduced by Boneh et al. [41]. First, let G and G_T be a cyclic additive group and a multiplication cyclic group of order N, where $N = p_1p_2p_3$ and p_1, p_2, and p_3 are three distinct prime numbers. Let $e : G \times G \to G_T$ be a bilinear map.

Then, let G_{p_1}, G_{p_2}, and G_{p_3} denote the subgroups of order p_1, p_2, and p_3 in group G, respectively. Because G is a cyclic group, it is easy to conclude that if h and l are group elements chosen from different subgroups, then $e(h, l) = 1$. This is called the orthogonality property in composite order bilinear groups.

3.2. Complexity Assumptions. We now present three assumptions of the subgroup decision problem for 3 primes (3P-SDP) [13]. First, we let G and G_T be two cyclic groups of order N, where $N = p_1p_2p_3$ and p_1, p_2, and p_3 are three distinct primes. And we let G_{p_1}, G_{p_2}, and G_{p_3} denote the subgroups of order p_1, p_2, and p_3 in G, respectively. Let $e : G \times G \to G_T$ be a bilinear map.

Assumption 1. We randomly choose element g as the generator of G_{p_1} and element X_3 as the generator of G_{p_3}. Given $D = (N, G, G_T, e, g, X_3)$, $T_1 \in G_{p_1p_2}$ and $T_2 \in G_{p_1}$. Let λ be the security parameter and the advantage of a polynomial time algorithm A in breaking Assumption 1 is defined as

$$\mathrm{Adv}_A^1(\lambda) = \left|\Pr\left[A\left(D, T_1\right) = 1\right] - \Pr\left[A\left(D, T_2\right) = 1\right]\right|. \quad (1)$$

Definition 2. Assumption 1 holds if there is no polynomial time algorithm A which has a nonnegligible advantage $\mathrm{Adv}_A^1(\lambda)$.

Assumption 3. We randomly choose elements $g, X_1 \in G_{p_1}$, $X_2, Y_2 \in G_{p_2}$, and $X_3, Y_3 \in G_{p_3}$. Given $D = (N, G, G_T, e, g, X_1X_2, X_3, Y_2Y_3)$ and $T_1 \in G$, $T_2 \in G_{p_1p_3}$. Let λ be the security parameter and the advantage of a polynomial time algorithm A in breaking Assumption 3 is defined as

$$\mathrm{Adv}_A^2(\lambda) = \left|\Pr\left[A\left(D, T_1\right) = 1\right] - \Pr\left[A\left(D, T_2\right) = 1\right]\right|. \quad (2)$$

Definition 4. Assumption 3 holds if there is no polynomial time algorithm A which has a nonnegligible advantage $\mathrm{Adv}_A^2(\lambda)$.

Assumption 5. We randomly choose elements $\alpha, s \in Z_N$, $g \in G_{p_1}$, $X_2, Y_2, Z_2 \in G_{p_2}$, and $X_3 \in G_{p_3}$. Given $D = (N, G, G_T, e, g, g^{\alpha}X_2, X_3, g^sY_2, Z_3)$ and $T_1 = e(g, g)^{\alpha s}$, $T_2 \in G_T$. Let λ be the security parameter and the advantage of a polynomial time algorithm A in breaking Assumption 5 is defined as

$$\mathrm{Adv}_A^3(\lambda) = \left|\Pr\left[A\left(D, T_1\right) = 1\right] - \Pr\left[A\left(D, T_2\right) = 1\right]\right|. \quad (3)$$

Definition 6. Assumption 5 holds if there is no polynomial time algorithm A which has a nonnegligible advantage $\mathrm{Adv}_A^3(\lambda)$.

3.3. Access Structures. In this paper, the role of the participants is taken by the attributes. As shown in [42], any monotone access structure can be represented by a Linear Secret Sharing Scheme.

Definition 7 (Linear Secret Sharing Schemes (LSSS)). Let Π denote a secret sharing scheme over a participant collection P. One says that Π is called linear over Z_p if

(1) the shares distributed for each participant can form a vector over Z_p;

(2) for Π there always exists a share-generating matrix M, which has l rows and n columns. Now, function ρ is defined and used to each party. That is, the party labeling row i can be denoted as $\rho(i)$ for $i = 1, 2, \ldots, l$. The column vector $\vec{v} = (s, y_2, y_3, \ldots, y_n)$ is randomly chosen in Z_p^n. Then, $\overrightarrow{M_i} \cdot \overrightarrow{v}$ is the share belonging to party $\rho(i)$. We use LSSS matrix (M, ρ) to represent an access policy in this paper.

The linear reconstruction property can be defined as follows. Suppose that Π is an LSSS for access structure A. Let $S \in A$ denote the authorized set and define $I \subseteq \{1, 2, \ldots, l\}$ as $I = \{i \mid \rho(i) \in S\}$. Then, there exist $\{w_i \in Z_p\}_{i \in I}$ such that if $\{\lambda_i\}$ are valid shares of any secret s, we have $\sum_{i \in I} w_i \lambda_i = s$ [41]. But it does not hold for unauthorized sets. In our scheme, we will employ LSSS matrices over Z_N, where N is the product of 3 different prime numbers.

3.4. CP-ABPRE

3.4.1. Algorithm Model. Generally speaking, a CP-ABPRE scheme is composed of 6 fundamental algorithms and it has an authority, a sender, a user that we call a delegator who needs to delegate his/her decryption ability to someone else, a proxy who helps the delegator to generate a reencrypted ciphertext, and some receivers as participants. The 6 algorithms are shown as follows.

$Setup(1^\lambda, U) \rightarrow (MSK, PK)$. It is performed by an authority to establish a new CP-ABPRE system. With the security parameter λ and attributes U as input, it generates the public key (PK) and the master secret key (MSK).

$KeyGen(PK, MSK, S) \rightarrow SK_S$. With PK, MSK, and a set of attributes S that describe the key as input, this algorithm is executed by the authority for the purpose of generating a secret key SK_S.

$Enc(PK, W = (M, \rho), m) \rightarrow CT_W$. Performed by a sender, with PK, a message m, and an access policy $W = (M, \rho)$ as input, the algorithm generates a ciphertext CT_W of m such that only a user whose attributes meet the access policy W can decrypt it.

$ReKeyGen(PK, SK_S, W' = (M', \rho')) \rightarrow RK_{S \rightarrow W'}$. This algorithm is performed by the delegator. With PK, SK_S, and an access policy $W' = (M', \rho')$ as input, it generates a reencryption key $\mathrm{RK}_{S \rightarrow W'}$ for the proxy.

$ReEnc(PK, RK_{S \rightarrow W'}, CT_W) \rightarrow CT_{W'}$. It is performed by the proxy, with PK, $\mathrm{RK}_{S \rightarrow W'}$, and CT_W as input. Firstly, the proxy checks whether the attribute in $\mathrm{RK}_{S \rightarrow W'}$ meets the access policy of CT_W. If yes, it outputs a reencrypted ciphertext $\mathrm{CT}_{W'}$ and otherwise $\perp$.

$Dec(PK, CT_W, SK_S) \rightarrow m$. With PK, an original ciphertext CT_W, and a secret key SK_S as input, it returns the plaintext message m if S satisfies the access policy W specified for CT_W, and otherwise $\perp$.

$Dec_R(PK, CT_{W'}, SK_{S'}) \rightarrow m$. This algorithm returns the plaintext message m if S' meets the access policy W' specified for $\mathrm{CT}_{W'}$, and otherwise $\perp$.

3.4.2. Security Model. The adaptive security definition for a CP-ABPRE scheme is described by a security game between a challenger B and an adversary A, which is shown as follows.

Setup. B runs the *Setup* algorithm to create a new system and then sends A the public key PK.

Phase 1. A makes the following queries.

(i) Secret Key Extract Queries. B runs the *KeyGen* algorithm after A submitting sets of attribute $S_1, S_2, \ldots, S_{q_1}$ and returns secret keys SK_S to A.

(ii) Reencryption Key Extract Queries. A submits sets of attribute $S_1, S_2, \ldots, S_{q_1}$ and an access structure $W' = (M', \rho')$. Then, B runs the *ReKeyGen* algorithm and gives the reencryption key $\mathrm{RK}_{S \rightarrow W'}$ to A.

Challenge. A chooses two messages M_0 and M_1 with equal length and an access structure W^*, which cannot be met by any of the queried attribute sets $\{S_1, S_2, \ldots, S_{q_1}\}$. B randomly flips coin $\theta \in \{0, 1\}$ and encrypts M_θ under W^* to generate CT^*, which is then sent to A.

Phase 2. Phase 1 is repeated. Note that there is a restriction that no sets of attributes $\{S_{q_1+1}, S_{q_1+2}, \ldots, S_q\}$ can satisfy the access structure corresponding to B.

Guess. A outputs a guess result θ' for θ.

In the above game, the advantage of A is defined as $\mathrm{Adv}_A = |\Pr[\theta' = \theta] - 1/2|$. And the above security model can be easily extended to simulate a game between a CCA adversary and a challenger by permitting Reencryption and Decryption queries during Phases 1 and 2.

Definition 8. A Ciphertext-Policy Attribute-Based Proxy Reencryption scheme is adaptively secure (or fully secure) if the advantage of any polynomial time adversary is negligible in above game.

3.4.3. Master Secret Security. Master secret security is an important property for unidirectional PRE defined by Ateniese et al. [43]. Roughly speaking, even if the dishonest proxy colludes with the receiver who can decrypt the reencrypted ciphertext, it is still impossible for them to get any information on delegator's secret key and the plaintext [44].

Definition 9. The master secret security of a CP-ABPRE scheme can be defined based on the following master secret security game.

Setup. The challenger B runs the *Setup* algorithm to create a new system and then sends the adversary A the public key (PK).

Queries. A makes the following queries.

(i) Extract(S). B runs the *KeyGen* algorithm after A submitting attribute sets S and returns secret keys SK_S to A.

(ii) RKExtract(S, W'). A submits attribute sets S and an access structure $W' = (M', \rho')$ to B. Then, B runs the *ReKeyGen* algorithm and returns the reencryption key $\mathrm{RK}_{S \rightarrow W'}$ to A.

Output. A outputs the secret key SK_{S^*} corresponding to the attribute sets S^*.

In the above game, the advantage of A is defined as $\mathrm{Adv}_A = \Pr[A \text{ succeeds}]$. A CP-ABPRE scheme meets master secret security if there is no polynomial time adversary A who has a nonnegligible advantage in winning the above game.

Lemma 10. *For a CP-ABPRE scheme, the plaintext security implies the master secret security. That is to say, for a CP-ABPRE scheme, if there is an adversary A who can break its master secret security defined above, then there also exists an adversary A' who can break this CP-ABPRE scheme.*

In Section 5, we will prove that there is no polynomial time adversary who can break the CP-ABPRE scheme with a nonnegligible advantage. So Lemma 10 is obvious.

4. The Proposed CP-ABPRE Scheme

In this section, we shall introduce our adaptively secure CP-ABPRE scheme. Before this, in order to facilitate understanding, notations used throughout the paper are summarized in Notations.

Our adaptively secure CP-ABPRE scheme is constructed in composite order linear groups of order $N = p_1p_2p_3$ (p_1, p_2, and p_3 are 3 different prime numbers) with LSSS access structure. Let G_{p_i} denote the subgroup of order p_i in G where $i \in \{1, 2, 3\}$. The subgroup G_{p_2} is only used in security proof. Our scheme is shown as follows.

(1) Setup$(1^\lambda, U)$. Taking as input the security parameter λ and system attribute set U, the trusted authority chooses random elements $\eta, a \in Z_N$, a generator $g \in G_{p_1}$, an element $g_0 \in G_{p_1}$, and a generator $X_3 \in G_{p_3}$. And then it computes $g_1 = e(g, g)^\eta$ and $g_2 = g^a$. For each attribute $x \in U$, it also chooses a random element $h_x \in Z_N$ and computes $H_x = g^{h_x}$. The public key is denoted as

$$\mathrm{PK} = \left(N, g_0, g_1, g_2, H_x, \ \forall x \in U\right). \tag{4}$$

The trusted authority sets the master secret key as $\mathrm{MSK} = (\eta, X_3)$.

(2) KeyGen(PK, MSK, S). Taking the public key (PK), the master secret key (MSK), and the user attribute set S as input, this algorithm first chooses a random value $t \in Z_N$ and another three random elements $R_0, R_0', R_x \in G_{p_3}$. Then, it computes the secret key as

$$\begin{aligned}&\mathrm{SK}\\ &= \left(S, K = g^\eta g^{at} R_0, L = g^t R_0', K_x = H_x^t R_x, \ \forall x \in S\right).\end{aligned} \tag{5}$$

(3) Enc(PK, W, m). This algorithm takes as input the public key (PK), an access policy $W = (M, \rho)$, and a message m, where M is an $l \times n$ matrix and the function ρ associates rows of M to attributes. This algorithm randomly chooses a column vector $\vec{v} = (s, y_2, y_3, \ldots, y_n) \in Z_N^n$. These values will be used to share the encryption exponent s. For $i = 1, 2, \ldots, l$, it computes $\lambda_i = \vec{M}_i \cdot \vec{v}$, where $\vec{M}_i$ denotes the ith row of M. Then, the algorithm chooses random numbers $r_1, r_2, \ldots, r_l \in Z_N$.

The ciphertext is generated as

$$\begin{aligned}\mathrm{CT} = \Big(&C = me(g, g)^{\eta s}, C' = g^s, C'' = g_0^s, C_i\\ &= g^{a\vec{M}_i \cdot \vec{v}} H_{\rho(i)}^{-r_i}, D_i = g^{r_i}, \ \forall i \in \{1, 2, \ldots, l\}\Big).\end{aligned} \tag{6}$$

(4) ReKeyGen(PK, SK, W'). To generate a reencryption key for another access policy $W' = (M', \rho')$, this algorithm takes as input the public key PK, the secret key $\mathrm{SK} = (S, K, L, K_x, \ \forall x \in S)$, and another access policy $W' = (M', \rho')$. It needs to choose a random element $\beta \in Z_N$ and computes $\widehat{C} = Enc(\mathrm{PK}, W', g^\beta)$. Then the reencryption key is set to

$$\mathrm{RK} = \left(S, rk_1 = Kg_0^\beta, rk_2 = L, K_x' = K_x, \widehat{C}, \ \forall x \in S\right). \tag{7}$$

(5) ReEnc(PK, RK, CT). This algorithm takes as input the public key (PK), a reencryption key (RK), and a ciphertext $\mathrm{CT} = (C, C', C'', C_i, D_i, \ \forall i)$. It first checks whether the attribute set in RK meets the access policy of CT. It computes

$$C_t = \frac{e\left(C', rk_1\right)}{\prod_{i \in I}\left(e\left(C_i, rk_2\right) e\left(D_i, K'_{\rho(i)}\right)\right)^{w_i}} \tag{8}$$

and outputs a reencrypted ciphertext $\mathrm{CT}' = (C, C', \widehat{C}, C_t)$ if yes and outputs $\perp$ otherwise.

(6) Dec(PK, CT, SK). The original ciphertext decryption algorithm takes the public key (PK), an original ciphertext (CT) for access policy W, and a secret key (SK) for an attribute set S as input. Assume that S meets W and $I \subset \{1, 2, \ldots, l\}$ is defined as $I = \{i \mid \rho(i) \in S\}$. Then, let $\{w_i \in Z_N\}_{i \in I}$ be a set of constants such that if $\{\lambda_i\}$ are valid shares of any secret s according to M, then, $\sum_{i \in I} w_i \lambda_i = s$ holds.

The message m can be recovered as

$$\begin{aligned}m &= \frac{C\prod_{i \in I}\left(e\left(C_i, L\right) e\left(D_i, K_{\rho(i)}\right)\right)^{w_i}}{e\left(C', K\right)}\\ &= \frac{C}{e\left(\prod_{i \in I} C_i^{-w_i}, L\right) e\left(C', K\prod_{i \in I} K_{\rho(i)}^{-w_i}\right)}.\end{aligned} \tag{9}$$

(7) Dec$_R(PK, CT', SK')$. The reencrypted ciphertext decryption algorithm takes the public key (PK), a reencrypted ciphertext CT' for access policy W', and a secret key SK' for an attribute set S' as input. If S' satisfies W', this algorithm computes as follows:

(7.1) Decrypt g^β from $\widehat{C}$ by the *Dec* algorithm.

(7.2) Then compute the message m by $m = Ce(C'', g^\beta)/C_t$.

5. Analyses and Proof

5.1. Correctness Analyses. The correctness of the scheme is based on the bilinear character of pairing $e : G \times G \to G_T$. First, we show the correctness of the original ciphertext decryption as follows:

$$m = \frac{C\prod_{i\in I}\left(e\left(C_i, L\right)e\left(D_i, K_{\rho(i)}\right)\right)^{w_i}}{e\left(C', K\right)}$$

$$= \frac{me\left(g,g\right)^{\eta s}\prod_{i\in I}\left(e\left(g^{a\vec{M}_i\cdot\vec{v}}H_{\rho(i)}^{-r_i}, g^t R_0'\right)e\left(g^{r_i}, H_{\rho(i)}^t R_{\rho(i)}\right)\right)^{w_i}}{e\left(g^s, g^\eta g^{at}\right)}$$

$$= \frac{me\left(g,g\right)^{\eta s}e\left(g,g\right)^{at\sum_{i\in I}(\vec{M}_i\cdot\vec{v})w_i}}{e\left(g,g\right)^{\eta s}e\left(g,g\right)^{sat}} = m. \tag{10}$$

Then, the correctness of the decryption algorithm for the reencrypted ciphertext is shown as follows:

$$m = \frac{Ce\left(C'', g^\beta\right)}{C_t} = \frac{Ce\left(C'', g^\beta\right)\prod_{i\in I}\left(e\left(C_i, rk_2\right)e\left(D_i, K'_{\rho(i)}\right)\right)^{w_i}}{e\left(C', rk_1\right)}$$

$$= \frac{me\left(g,g\right)^{\eta s}e\left(g_0^s, g^\beta\right)\prod_{i\in I}\left(e\left(g^{a(\vec{M}_i\cdot\vec{v})}H_{\rho(i)}^{-r_i}, g^t R_0'\right)e\left(g^{r_i}, H_{\rho(i)}^t R_{\rho(i)}\right)\right)^{w_i}}{e\left(g^s, g^\eta g^{at} g_0^\beta R_0\right)} \tag{11}$$

$$= \frac{me\left(g,g\right)^{s\eta}e\left(g_0^s, g^\beta\right)e\left(g,g\right)^{at\sum_{i\in I}(\vec{M}_i\cdot\vec{v})w_i}}{e\left(g,g\right)^{s\eta}e\left(g,g_0\right)^{s\beta}e\left(g,g\right)^{sat}} = m.$$

Both the original ciphertext decryption and the reencrypted ciphertext decryption processes in Section 4 are correct because the message m can be recovered correctly. Hence, our CP-ABPRE scheme is also correct.

5.2. Security Proof. Dual system encryption [27] is considered as a common and powerful tool to transform a selectively secure scheme into an adaptively secure one [13, 45, 46]. In a dual system encryption scheme, both keys and ciphertexts have two forms: normal and semifunctional [13]. A normal key can be used to decrypt normal or semifunctional ciphertexts, while a semifunctional key can only be used to decrypt normal ciphertexts. Notably, the semifunctional keys and ciphertexts are only used in security proof. To prove the security of our CP-ABPRE scheme, we firstly define the semifunctional keys and ciphertexts as follows.

Let g_2 be a generator of G_{p_2}.

Semifunctional Ciphertexts. We firstly use the *Enc* algorithm to generate normal ciphertext and choose element $c \in Z_N$ randomly. Then, we choose random values $z_x \in Z_N$ for each attribute, random values $\gamma_i \in Z_N$ for the ith row of matrix M, and a random column vector $\vec{u} \in Z_N^n$. The semifunction ciphertext is set as

$$C' = g^s g_2^c,$$

$$C_i = g^{a\vec{M}_i\cdot\vec{v}}H_{\rho(i)}^{-r_i}g_2^{\vec{M}_i\cdot\vec{u}+\gamma_i z_{\rho(i)}},$$

$$D_i = g^{r_i}g_2^{-\gamma_i} \tag{12}$$

$$\forall i \in \{1, 2, \ldots, l\}.$$

Semifunctional Key. We use *KeyGen* algorithm to generate normal secret key. And then we choose random exponents $b, d \in Z_N$ to set the semifunctional key as follows.

A semifunctional key of type 1 is

$$K = g^\eta g^{at} R_0 g_2^d,$$

$$L = g^t R_0' g_2^d, \tag{13}$$

$$K_x = H_x^t R_x g_2^{bz_x} \quad \forall x \in S.$$

A semifunctional key of type 2 (in type 1 $b = 0$) is

$$K = g^\eta g^{at} R_0 g_2^d,$$

$$L = g^t R_0', \tag{14}$$

$$K_x = H_x^t R_x \quad \forall x \in S.$$

We should note that there will be an extra factor $e(g_2, g_2)^{cd-\sum_{i\in I} b\vec{M}_i\cdot\vec{u}w_i} = e(g_2, g_2)^{cd-bu_1}$ ($u_1 = (1, 0, 0, \ldots, 0)\cdot\vec{u}$) when a semifunctional key is used to decrypt a semifunctional ciphertext. But when the formula $cd = bu_1$ holds, the semifunctional key of type 1 called a nominally semifunctional key can decrypt the semifunctional ciphertext successfully.

Our proof of security relies on Assumptions 1, 3, and 5 defined in Section 3. The security proof is obtained via a hybrid argument over a sequence of games defined bellow. Let Q be the maximum number of key queries that the adversary makes, and a series of games are defined as follows,

$Game_{real}$. It denotes the real CP-ABPRE security game defined in Section 3, with normal keys and ciphertexts.

$Game_0$. It is similar to the above real game except that the challenge ciphertext is transformed into semifunctional one.

$Game_{k,1}$. In the game, the challenge ciphertext is semifunctional, the first $k-1$ queried keys are semifunctional ones of type 2, the kth key is semifunctional one of type 1, and the rest of the keys are normal ones.

$Game_{k,2}$. The challenge ciphertext is semifunctional, the first k queried keys are semifunctional ones of type 2, and the remaining keys are normal ones.

$Game_{Final}$. All keys are semifunctional ones of type 2 and the challenge ciphertext is semifunctional encryption of a random message which is independent of the two messages provided by the adversary. So the advantage of the adversary in this game is negligible.

In the latter part of this section, we will prove that the above games are indistinguishable under the composite assumption.

Lemma 11. *Assume that there is a polynomial time adversary A such that $Game_{real}Adv_A - Game_0Adv_A = \varepsilon$. Then, we can construct another polynomial time algorithm B that can break Assumption 1 with a nonnegligible advantage ε.*

Proof. We establish a polynomial time algorithm B which receives $\{g, X_3, T\}$ to simulate either $\text{Game}_{\text{real}}$ or Game_0 with A based on setting whether $T \in G_{p_1p_2}$ or $T \in G_{p_1}$.

Setup. B chooses random exponents $a, \eta, h_x \in Z_N$ $(\forall x)$, sends the public key $\text{PK} = (N, g, g_0, e(g,g)^\eta, g^a, H_x = g^{h_x}\ \forall x)$ to the adversary A, and at the same time securely keeps the master secret key $\text{MSK} = (\eta, X_3)$.

Phase 1. B responds to whatever A's key requests by using the *KeyGen* algorithm to make normal keys, since it has the MSK.

Challenge. A provides two messages M_0 and M_1 with equal length and a challenge access matrix $W^* = (M^*, \rho)$ to B. For each row i of matrix M^*, B first chooses random values $v_2', v_3', \ldots, v_n' \in Z_N$ and a random element $r_i' \in Z_N$ to build the column vector $\overrightarrow{v}' = (1, v_2', v_3', \ldots, v_n')$. Then, B chooses a random message M_θ from M_0 and M_1 and computes the challenge ciphertext C^* as

$$\begin{aligned} C &= M_\theta e(g,g)^{s\eta} = M_\theta e(g,T)^\eta, \\ C' &= T \\ C_i &= T^{a\overrightarrow{M}_i^* \cdot \overrightarrow{v}'} T^{-r_i' h_{\rho(i)}}, \\ D_i &= T^{r_i'}, \end{aligned} \tag{15}$$

where $\theta \in \{0,1\}$ is the random coin.

Phase 2. Repeat Phase 1.

Guess. A outputs its guess result θ' of θ.

If $T \in G_{p_1}$, let $T = g^s$. This is a normal ciphertext with $\overrightarrow{v} = s\overrightarrow{v}'$ and $r_i = r_i's$. B has simulated $\text{Game}_{\text{real}}$ for A. If $T \in G_{p_1p_2}$, let $T = g^s g_2^c$. This is a semifunctional ciphertext with $u = cav'$, $\gamma_i = -cr_i'$, and $z_{\rho(i)} = h_{\rho(i)}$. By the Chinese Remainder Theorem (CRT), the values of $a, v_2', v_3', \ldots, v_n', r_i', h_{\rho(i)}$ modulo p_2 are uncorrelated to their values modulo p_1. B has simulated Game_0 for A.

Hence, if A can distinguish $\text{Game}_{\text{real}}$ and Game_0 with a nonnegligible advantage ε, B can distinguish element on G_{p_1} and $G_{p_1p_2}$ with a nonnegligible advantage ε. □

Lemma 12. *Assume that there is a polynomial time adversary A such that $Game_{k-1,2}Adv_A - Game_{k,1}Adv_A = \varepsilon$. Then, another polynomial time algorithm B, which can break Assumption 3 with a nonnegligible advantage ε, can be constructed.*

Proof. B receives $\{g, X_1X_2, X_3, Y_2Y_3, T\}$ to simulate either $\text{Game}_{k-1,2}$ or $\text{Game}_{k,1}$ with A based on setting whether $T \in G$ or $T \in G_{p_1p_3}$.

Setup. B chooses random exponents $a, \eta, h_x \in Z_N$ $(\forall x \in U)$ to generate the public key $\text{PK} = (N, g, g_0, e(g,g)^\eta, g^a, H_x = g^{h_x}\ \forall x)$ and sends it to A. At the same time, B should securely keep the master secret key $\text{MSK} = (\eta, X_3)$.

Phase 1. This phase can be divided into three parts.

(1) To form the first $k-1$ semifunctional keys of type 2, B responds to each A's key query by randomly choosing elements $t \in Z_N$ and $R_0', R_x \in G_{p_3}$ and sets

$$\begin{aligned} K &= g^\eta g^{at} (Y_2Y_3)^t, \\ L &= g^t R_0', \\ K_x &= H_x^t R_x \quad \forall x \in S. \end{aligned} \tag{16}$$

(2) To generate the normal keys of queries greater than k, B needs to run the *KeyGen* algorithm since it has the master secret key (MSK).

(3) To answer the kth query, set g^t equal to the G_{p_1} part of T. Then, B randomly chooses elements $R_0, R_0', R_x \in G_{p_3}$ and computes

$$\begin{aligned} K &= g^\eta T^a R_0, \\ L &= T R_0', \\ K_x &= T^{h_x} R_x \quad \forall x \in S. \end{aligned} \tag{17}$$

If $T \in G_{p_1p_3}$, the above key is a normal one. And if $T \in G$, it is a semifunctional one of type 1. In this case, there exists $z_x = h_x$. If we let factor g_2^b denote the G_{p_2} part of T, there is $d \equiv ba \bmod p_2$. Note that $z_x \bmod p_2$ is uncorrelated to h_x modulo p_1, let $g_2^b a$ be equal to the G_{p_2} part of K, let g_2^b be equal to the G_{p_2} part of L, and let $g_2^{bz_x}$ be equal to the G_{p_2} part of K_x.

Challenge. A provides two messages M_0 and M_1 with equal length and a challenge access matrix (M^*, ρ) for B. B sets $g^s = X_1$ and $g_2^b = X_2$. Then, B chooses random values $u_2, u_3, \ldots, u_n \in Z_N$ to define the vector $\vec{u}' = (a, u_2, u_3, \ldots, u_n)$ and randomly chooses exponent $r_i' \in Z_N$. B chooses a random message M_θ from M_0 and M_1 and computes the challenge ciphertext C^* as

$$\begin{aligned} C &= M_\theta e\left(g, X_1X_2\right)^\eta, \\ C' &= X_1X_2, \\ C_i &= \left(X_1X_2\right)^{\vec{M}_i^* \cdot \vec{u}'} \left(X_1X_2\right)^{-r_i' h_{\rho(i)}}, \\ D_i &= \left(X_1X_2\right)^{r_i'}, \end{aligned} \tag{18}$$

where $\theta \in \{0, 1\}$ is the random coin. We set $\vec{v} = a^{-1}s\vec{u}'$ and $\vec{u} = c\vec{u}'$, so s is shared in the subgroup G_{p_1} and $c \cdot a$ is shared in the subgroup G_{p_2}. It also sets $r_i = s \cdot r_i'$ and $\gamma_i = -c \cdot r_i'$. The values $z_{\rho(i)} = h_{\rho(i)}$ match those in the kth key if it is semifunctional of type 1.

Actually, if the kth key can be used to decrypt the challenge ciphertext, then $cd - bu_1 = cba - bca = 0$ modulo p_2 holds, so our key is either normal or nominally semifunctional. We must argue that this is hidden to A that cannot request any keys that can be used to decrypt the challenge ciphertext. Note that attributes are only used once in labeling the rows of the matrix. When attribute $x \notin S$, z_x only appeared in the kth key because all keys are semifunctional ones of type 2 except for the kth one. Because the kth key cannot be used, decrypting the challenge ciphertext, which implies the row space R formed by the rows of the matrix M whose attributes are in the key, does not include the vector $(1, 0, \ldots, 0)$. Thus, we denote a vector $\vec{\sigma}$ that is orthogonal to R and not orthogonal to vector $(1, 0, \ldots, 0)$. We set an equation that $\vec{u} = f\vec{\sigma} + \vec{u}''$ for $f \in Z_N$ and u'' is in the span of the basis elements not equal to $\vec{\sigma}$. We note that u'' is properly distributed and reveals nothing about f. Since $u_1 = \vec{u} \cdot (1, 0, 0, \ldots, 0) = f(1, 0, 0, \ldots, 0) \cdot \vec{\sigma} + (1, 0, 0, \ldots, 0) \cdot \vec{u}''$ and $(1, 0, 0, \ldots, 0) \cdot \vec{\sigma} \neq 0$, the item $\vec{u} \cdot (1, 0, 0, \ldots, 0)$ is correlated to f.

For $\rho(i) \in S$, the equation $\vec{M}_i \cdot \vec{u} = \vec{M}_i \cdot (f\vec{\sigma} + \vec{u}'') = \vec{M}_i \cdot \vec{u}''$ has nothing to do with f. And for $\rho(i) \notin S$, $f\vec{\sigma}$ can be obtained only in the equation $\vec{M}_i^* \cdot \vec{u} + \gamma_i z_{\rho(i)}$, where $\rho(i)$ is attribute which does not appear in the kth key. As long as each γ_i mod p_2 is not congruent to 0, each equation brings a new unknown factor $z_{\rho(i)}$ that appears nowhere else, and so the adversary A can get nothing about f. More precisely, for any value of u_1, there is the same number of solutions to these equations. Hence, as long as each γ_i is nonzero modulo p_2, the ciphertext and the kth key are properly distributed in the adversary's view with a probability negligibly close to 1.

Thus, if $T \in G_{p_1p_3}$, then B has simulated $\text{Game}_{k-1,2}$ with A. If $T \in G$ and γ_i is nonzero modulo p_2, then B has simulated $\text{Game}_{k,1}$. Hence, B can use the output result of A to distinguish between these possibilities for T. In other words, B can break Assumption 3 with advantage ε.

Hence, if the adversary A has a nonnegligible advantage ε to distinguish $\text{Game}_{k-1,2}$ and $\text{Game}_{k,1}$, B can also distinguish element on $G_{p_1p_3}$ and G with a nonnegligible advantage ε. □

Lemma 13. *Suppose that there is a polynomial time adversary A such that $\text{Game}_{k,1}Adv_A - \text{Game}_{k,2}Adv_A = \varepsilon$. Then, another polynomial time algorithm B, which breaks Assumption 3 with a nonnegligible advantage ε, can be constructed.*

Proof. B receives $\{g, X_1X_2, X_3, Y_2Y_3, T\}$ to simulate either $\text{Game}_{k,1}$ or $\text{Game}_{k,2}$ with the adversary A depending on whether $T \in G$ or $T \in G_{p_1p_3}$. This proof is very similar to that of Lemma 12, so here we only describe Phases 1 and 2.

Phase 1. The first $(k-1)$ semifunctional keys of type 2 and the last $(Q-k)$ normal keys are constructed exactly as in Lemma 12. To answer the kth query, B randomly chooses an exponent $h \in Z_N$ and then computes

$$\begin{aligned} K &= g^\eta T^a R_0 \left(Y_2Y_3\right)^h, \\ L &= TR_0', \\ K_x &= T^{h_x} R_x \quad \forall x \in S. \end{aligned} \tag{19}$$

The only difference from Lemma 12 here is adding a term $(Y_2Y_3)^h$ which randomizes the G_{p_2} part of K, so the kth key is no longer a semifunctional one. It would be failed if we try to use it to decrypt the semifunctional ciphertext, because condition $cd - bu_1 \equiv 0 \bmod p_2$ is no longer established.

Phase 2. Phase 1 is repeated.

Hence, if $T \in G_{p_1p_3}$, the kth key is a properly distributed semifunctional key of type 2 and therefore B simulates $\text{Game}_{k,2}$ for A. If $T \in G$, the kth key is a properly distributed semifunctional key of type 1 and therefore B simulates $\text{Game}_{k,1}$ for A. As a result, if A has a nonnegligible advantage ε to distinguish $\text{Game}_{k,2}$ and $\text{Game}_{k,1}$, B also has a nonnegligible advantage ε to distinguish element in $G_{p_1p_3}$ and G. □

Lemma 14. *Assume that there is a polynomial time adversary A such that $\text{Game}_{Q,2}Adv_A - \text{Game}_{Final}Adv_A = \varepsilon$. Then, we can construct a polynomial time algorithm B, which can break Assumption 5 with a nonnegligible advantage ε, which can be constructed.*

Proof. The proof is similar to those of Lemmas 11–13. B receives $\{g, g^\alpha X_2, X_3, g^s Y_2, Z_2, T\}$ to simulate $\text{Game}_{Q,2}$ or $\text{Game}_{\text{Final}}$ with A based on whether $T = e(g, g)^{\eta s}$ or T is a random element of G_T.

Setup. B chooses random values $a, h_x \in Z_N$ $(\forall x \in U)$ and sends the public key $\text{PK} = (N, g, g_0, e(g, g)^\eta = e(g, g^\eta X_2), g^a, H_x = g^{h_x}\ \forall x)$ to A. Note that B does not know η.

Table 1: Property comparisons.

Schemes	Access structure	Adaptive security	Complexity assumption	Supported policy
Liang et al.'s [6]	AND gate between two-value attributes	N	ADBDH CTDH	And
Luo et al.'s [7]	AND gate among multivalue attributes	N	DBDH	And
Seo and Kim's [8]	AND gate between two-value attributes	N	ADBDH CTDH	And
Li's [9]	LSSS matrix	N	DPBDHE	Any monotonic access formula
Liang et al.'s [11]	LSSS matrix	N	DPBDHE	Any monotonic access formula
Liang et al.'s [14]	LSSS matrix	Y	DPBDHE	Any monotonic access formula
Backes et al.'s [15]	LSSS matrix	Y	DPBDHE	And
Our scheme	LSSS matrix	Y	3P-SDP	Any monotonic access formula

DBDH: Decisional Bilinear Diffie-Hellman, CTDH: Complex Triple Diffie-Hellman, ADBDH: Augment Decisional Bilinear Diffie-Hellman, 3P-SDP: subgroup decision problem for 3 primes, and DPBDHE: Decisional q-Parallel Bilinear Diffie-Hellman Exponent.

Phase 1. To form semifunctional keys of type 2, B responds to each A's key query by randomly choosing elements $t \in Z_N$ and $R_0, R_0', R_x \in G_{p_3}$ and sets

$$K = g^{\eta} g^{at} Z_2^t R_0,$$
$$L = g^t R_0', \tag{20}$$
$$K_x = H_x^t R_x \quad \forall x \in S$$

which is similar as in the previous lemmas.

Challenge. A submits two messages M_0 and M_1 with equal length and a matrix (M^*, ρ) to B. B then takes s from the assumption term $g^s Y_2$. It randomly chooses values $u_2, u_3, \ldots, u_n \in Z_N$ to define a vector $u' = (a, u_2, u_3, \ldots, u_n)$ and randomly chooses an exponent $r_i' \in Z_N$. B chooses a random message M_θ from M_0 and M_1 and generates the challenge ciphertext C^* as

$$C = M_\theta T,$$
$$C' = g^s Y_2,$$
$$C_i = \left(g^s Y_2\right)^{\overrightarrow{M}_i^* \overrightarrow{u}'} \left(g^s Y_2\right)^{-r_i' h_{\rho(i)}}, \tag{21}$$
$$D_i = \left(g^s Y_2\right)^{r_i'},$$

where $\theta \in \{0, 1\}$ is the random coin. We note that there exists $v = a^{-1} s u'$ and $u = c u'$, so s is being shared in the subgroup G_{p_1} and ca is being shared in the subgroup G_{p_2}. At the same time, set $r_i = s r_i'$ and $\gamma_i = -c r_i'$.

Phase 2. Repeat Phase 1.

Guess. A outputs its guess result θ' of θ.

If $T = e(g, g)^{\eta s}$, then this is a properly distributed semifunctional ciphertext with message M_θ. Otherwise, this is a semifunctional ciphertext of a random message and will not give anything about θ to the attacker.

Hence, if A can distinguish $\text{Game}_{Q,2}$ and $\text{Game}_{\text{Final}}$ with a nonnegligible advantage ε, B can distinguish the element $e(g, g)^{\eta s}$ and a random element in G_T with a nonnegligible advantage ε. □

Theorem 15. *If Assumptions 1, 3, and 5 hold, our CP-ABPRE scheme is adaptively secure.*

Proof. If Assumptions 1, 3, and 5 hold, we have proved that the real CP-ABPRE security game $\text{Game}_{\text{real}}$ is indistinguishable from $\text{Game}_{\text{Final}}$ by previous Lemmas 11–14. And because the challenger in $\text{Game}_{\text{Final}}$ chooses a random message M_θ to encrypt, the adversary could not get any information on θ. In other words, the advantage of adversary in $\text{Game}_{\text{Final}}$ can be negligible, so the advantage of the adversary in $\text{Game}_{\text{real}}$ can be also negligible. Hence, our CP-ABPRE scheme is secure. □

5.3. Analyses and Discussions

5.3.1. Security Analysis. The reencryption control, which allows the encryptor to decide whether the ciphertext can be reencrypted, was first put forward by Luo et al. in [7]. In our CP-ABPRE scheme, we can see that the element $C'' = g_0^s$ is of no use in the original ciphertext decryption phase, and it is only used in the reencrypted ciphertext decryption phase. If the encryptor does not provide the factor g_0^s, it is impossible for the decryption of reencrypted ciphertext. So in our scheme, the encryptor can control whether the ciphertext can be reencrypted (in fact he can decide whether the reencrypted ciphertext can be decrypted). In addition, our scheme overcomes the restriction on the attacker in a selective security model in the existing schemes [6–9, 11] and is proven adaptively secure in the standard model without jeopardizing the expressiveness of access policy.

5.3.2. Performance Analyses. In this part, we will make some comparisons of different CP-ABPRE schemes, and the results are summarized in Tables 1–3. A comparison of access expression and some properties is given in Table 1. In addition, we

Table 2: Performance comparisons (I).

Schemes	PK	MK	SK	Ciphertext
Liang et al.'s [6]	$(6n+2)L_G + L_{G_T}$	$(3n+1)L_{Z_q}$	$(2n+1)L_G$	$(n+2)L_G + L_{G_T}$
Luo et al.'s [7]	$(N'+2n+4)L_G + L_{G_T}$	$(N'+2n+1)L_{Zq}$	$(4n+1)L_G$	$(n+2)L_G + L_{G_T}$
Seo and Kim's [8]	$(3n+2)L_G + L_{G_T} + 3nL_{Z_q}$	$(3n+3)L_{Z_q}$	$(n+1)L_G + L_{Z_q}$	$(n+2)L_G + L_{G_T}$
Li's [9]	$(n+2)L_G + L_{G_T}$	L_G	$(\lvert A_U\rvert + 2)L_G$	$(2\lvert A_C\rvert + 2)L_G + L_{G_T}$
Liang et al.'s [11]	$3L_G + L_{G_T}$ + 6Hash	L_G	$(\lvert A_U\rvert + 2)L_G$	$(2\lvert A_C\rvert + 3)L_G + L_{\{0,1\}^{2k}}$
Liang et al.'s [14]	$(n+6)L_G + L_{G_T}$	$2L_G$	$(\lvert A_U\rvert + 3)L_G$	$(2\lvert A_C\rvert + 5)L_G + L_{G_T}$
Backes et al.'s [15]	$(n+2)L_G + L_{G_T}$	$L_G + (1+n)L_{Z_q}$	$(n+1)L_G$	$3L_G + L_{G_T} + nL_{Z_q}$
Our scheme	$(n+2)L_G + L_{G_T}$	$L_G + L_{Z_q}$	$(\lvert A_U\rvert + 2)L_G$	$(2\lvert A_C\rvert + 2)L_G + L_{G_T}$

Table 3: Performance comparisons (II).

Schemes	Encryption	Decryption	Reencryption	Reencrypted decryption
Liang et al.'s [6]	$(n+2)G + 2G_T$	$(n+2)P + 2G_T$	$(n+1)P + G_T$	$(n+3)P + 4G_T$
Luo et al.'s [7]	$(n+2)G + 2G_T$	$2nP + 3G_T$	$(2n+1)P + (n+1)G_T$	$(2n+1)P + 5G_T$
Seo and Kim's [8]	$(n+2)G + 2G_T$	$2P + (3n+2)G + 2G_T$	$2P + 3nG + G_T$	$3P + 3nG + 4G_T$
Li's [9]	$(4\lvert A_C\rvert + 2)G + 2G_T$	$(2\lvert A_U\rvert + 1)P + 3G_T$	$(2\lvert A_C\rvert + 1)P + 4\lvert A_C\rvert G + 3\lvert A_C\rvert G_T$	$(2\lvert A_U\rvert + 1)P + (3\lvert A_U\rvert + 2)G_T$
Liang et al.'s [11]	$(4\lvert A_C\rvert + 2)G + G_T$	$(2\lvert A_U\rvert + 1)P + 3\lvert A_U\rvert G_T$	$(2\lvert A_U\rvert + 2)P + (3\lvert A_U\rvert + 1)G_T$	$(2\lvert A_U\rvert + 2)P + 3\lvert A_U\rvert G_T$
Liang et al.'s [14]	$(4\lvert A_C\rvert + 4)G + 2G_T$	$(2\lvert A_U\rvert + 1)P + (2\lvert A_U\rvert + 1)G_T$	$(2\lvert A_U\rvert + 2)P + (2\lvert A_U\rvert + 2)G_T$	$(2\lvert A_U\rvert + 3)P + (2\lvert A_U\rvert + 4)G_T$
Backes et al.'s [15]	$(n+3)G + 2G_T$	$2P + nG$	$nP + (n-1)G$	$nP + 2G + G_T$
Our scheme	$(4\lvert A_C\rvert + 2)G + 2G_T$	$2P + (4\lvert A_U\rvert - 1)G + 2G_T$	$2P + (4\lvert A_U\rvert - 1)G + 2G_T$	$3P + (4\lvert A_U\rvert - 1)G + 4G_T$

shall compare the performance and efficiency of our proposal with the existing ones in Tables 2 and 3. We use $|A_U|$, $|A_C|$, and n to denote the attributes held by user U, the attributes required by the ciphertext, and the number of attributes in systems, respectively. We use G to denote the operation in group G, G_T for the operation in group G_T, and P for the bilinear pairing operation. We use symbol L_* to denote the bit length of element in $*$. At last, we use $N' = \sum_{i=1}^{n} n_i$ to denote the total number of possible values of attributes, where n_i is the number of possible values for attribute i.

From Tables 1–3, we can draw the following conclusions. Liang et al. [6], Luo et al. [7], Seo and Kim [8], and Backes et al. [15], respectively, proposed their schemes based on the CP-ABE in which the ciphertext is associated with AND gates access structure. However, the access policy in these four schemes is not flexible enough; it can only support AND operation on attributes. The ciphertext policy realized in Li's [9], Liang et al.'s [11, 14], and our scheme is LSSS matrix access structure which supports any monotonic access formula including what the AND gate access structure supports. Different from Li's [9] and Liang et al.'s [11] schemes, our scheme is adaptively secure. And, what is more, our scheme needs only a constant number of paring operations in Reencryption and Decryption phase when compared with Liang et al.'s scheme [14]. That is, our scheme greatly reduces the computational overhead.

From the above analysis, we can conclude that our scheme is more efficient and secure than previous CP-ABPRE schemes.

6. Conclusions

CP-ABPRE employs the PRE technology in the ABE cryptographic setting and could be applicable to many real world applications, such as email forwarding. The existing CP-ABPRE systems, however, were proven secure only in the selective security model which causes attacker to behave differently from real environment. So an efficient and adaptively secure Attribute-Based Proxy Reencryption scheme is proposed in this paper. By using the dual system encryption, the proposed scheme can be proven to be adaptively secure rather than selectively secure which is much less practical. Meantime, our scheme supports any monotone access formulas including what the AND gate access structure supports. And compared with the existing schemes, our scheme needs only a constant number of paring operations in Reencryption and Decryption phase, which greatly reduces the computational overhead.

Notations

p_i: Large prime number ($i = 1, 2, 3$)
N: Order of composite order linear groups
G: Additive group of order p
G_{p_i}: The subgroup of order p_i in G ($i = 1, 2, 3$)
λ: Security parameter
U: System attribute set
Z_N: The set of positive integers which are less than N
g: Generator of G_{p_1}
X_3: Generator of G_{p_3}
e: Bilinear mapping, that is, $e : G \times G \to G_T$
PK: The private key
MSK: The master secret key
S: User attribute set
SK: The secret key
W: An access policy
M: An $l \times n$ matrix

ρ: The rows of M to attributes
m: Message to sign
s: The encryption exponent
RK: The reencryption key.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

Acknowledgments

This work was supported by Natural Science Foundation of China under Grant no. 61103178, Natural Science Basic Research Plan in Shaanxi Province of China under Grants nos. 2015JM6294 and 2016JM6002, and the Fundamental Research Funds for the Central Universities under Grant no. 3102015JSJ0003.

References

[1] D. G. Feng and C. Chen, "Research on attribute-based cryptography," *Journal of Cryptologic Research*, vol. 1, no. 1, pp. 1–12, 2014.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, Alexandria, Va, USA, October 2006.

[3] Q. Y. Li and F. L. Zhang, "A fully secure attribute based broadcast encryption scheme," *International Journal of Network Security*, vol. 17, no. 3, pp. 263–271, 2015.

[4] K. T. Liang, L. M. Fang, D. S. Wong, and W. Susilo, "A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 8, pp. 2004–2027, 2014.

[5] C.-C. Chang, C.-Y. Sun, and T.-F. Cheng, "A dependable storage service system in cloud environment," *Security and Communication Networks*, vol. 8, no. 4, pp. 574–588, 2015.

[6] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (ASIACCS '09)*, pp. 276–286, ACM, March 2009.

[7] S. Luo, J. Hu, and Z. Chen, "Ciphertext policy attribute-based proxy re-encryption," in *Information and Communications Security*, M. Soriano, S. Qing, and J. López, Eds., vol. 6476 of *Lecture Notes in Computer Science*, pp. 401–415, Springer, Berlin, Germany, 2010.

[8] H. Seo and H. Kim, "Attribute-based proxy re-encryption with a constant number of pairing operations," *International Journal of Information and Communication Engineering*, vol. 10, no. 1, pp. 53–60, 2012.

[9] K. Y. Li, "Matrix access structure policyused in attribute-based proxy re-encryption," http://arxiv.org/abs/1302.6428.

[10] P.-S. Chung, C.-W. Liu, and M.-S. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13, 2014.

[11] K. T. Liang, L. M. Fang, D. S. Wong, and W. Susilo, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," Tech. Rep. 2013/236, IACR Cryptology ePrint Archive, 2013.

[12] Y. Kawai, "Outsourcing the re-encryption key generation: flexible ciphertext-policy attribute-based proxy re-encryption," in *Information Security Practice and Experience*, vol. 9065 of *Lecture Notes in Computer Science*, pp. 301–315, Springer, Berlin, Germany, 2015.

[13] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology—EUROCRYPT 2010*, H. Gilbert, Ed., vol. 6110 of *Lecture Notes in Computer Science*, pp. 62–91, Springer, Berlin, Germany, 2010.

[14] K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang, and Y. Yu, "An adaptively CCA-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," in *Information Security Practice and Experience: 10th International Conference, ISPEC 2014, Fuzhou, China, May 5–8, 2014. Proceedings*, vol. 8434 of *Lecture Notes in Computer Science*, pp. 448–461, Springer, Berlin, Germany, 2014.

[15] M. Backes, M. Gagné, and S. A. Krishnan Thyagarajan, "Fully secure inner-product proxy re-encryption with constant size ciphertext," in *Proceedings of the 3rd International Workshop on Security in Cloud Computing (SCC '15)*, pp. 31–40, Singapore, April 2015.

[16] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005. Proceedings*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 457–473, Springer, Berlin, Germany, 2005.

[17] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Advances in Cryptology (CRYPTO '84)*, pp. 47–53, Springer, Berlin, Germany, 1985.

[18] L. J. Pang, J. Yang, and Z. T. Jiang, "A survey of research progress and development tendency of attribute-based encryption," *The Scientific World Journal*, vol. 2014, Article ID 193426, 13 pages, 2014.

[19] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 456–465, November 2007.

[20] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Applied Cryptography and Network Security (ACNS 2008)*, pp. 111–129, Springer, Berlin, Germany, 2008.

[21] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, IEEE Computer Society, Berkeley, Calif, USA, May 2007.

[22] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proceedings of the International Colloquium Automata, Languages and Programming (ICALP '08)*, pp. 579–591, Springer, Berlin, Germany, 2008.

[23] X. H. Liang, Z. F. Cao, H. Lin, and D. S. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ICCS '09)*, pp. 343–352, Sydney, Australia, March 2009.

[24] L. Ibraim, Q. Tang, P. Hartel, and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," in *International Conference on Information Security Practice and Experience (ISPEC '09)*, pp. 1–12, Springer, 2009.

[25] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Public Key Cryptography (PKC 2011)*, pp. 53–70, Springer, Berlin, Germany, 2011.

[26] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), Warsaw, Poland, May 2003*, Springer, 2003.

[27] B. Waters, "Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology—CRYPTO 2009*, S. Halevi, Ed., vol. 5677 of *Lecture Notes in Computer Science*, pp. 619–636, Springer, Berlin, Germany, 2009.

[28] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: achieving full security through selective techniques," in *Advances in Cryptology—CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2012. Proceedings*, vol. 7417 of *Lecture Notes in Computer Science*, pp. 180–198, Springer, Berlin, Germany, 2012.

[29] S. Garg, C. Gentry, S. Halevi, and M. Zhandry, "Fully secure attribute based encryption from multilinear maps," Cryptology ePrint Archive Report 2014/622, 2014.

[30] Z. B. Ying, H. Li, J. F. Ma, J. W. Zhang, and J. T. Cui, "Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating," *Science China Information Sciences*, no. 4, pp. 1–16, 2016.

[31] T. Kitagawa, H. Kojima, N. Attrapadung, and H. Imai, "Efficient and fully secure forward secure ciphertext-policy attribute-based encryption," in *Information Security*, Y. Desmedt, Ed., vol. 7807 of *Lecture Notes in Computer Science*, pp. 87–99, Springer, Berlin, Germany, 2015.

[32] M. Mambo and E. Okamoto, "Proxy cryptosystems: delegation of the power to decrypt ciphertexts," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 80, no. 1, pp. 54–63, 1997.

[33] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology—EUROCRYPT '98: International Conference on the Theory and Application of Cryptographic Techniques Espoo, Finland, May 31–June 4, 1998 Proceedings*, vol. 1403 of *Lecture Notes in Computer Science*, pp. 127–144, Springer, Berlin, Germany, 1998.

[34] P. Xu, T. F. Jiao, Q. H. Wu, W. Wang, and 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.

[35] X. Zhao and H. Li, "Achieving dynamic privileges in secure data sharing on cloud storage," *Security and Communication Networks*, vol. 7, no. 11, pp. 2211–2224, 2014.

[36] L. Barolli, X. F. Chen, and F. Xhafa, "Advances on cloud services and cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 8, pp. 1985–1987, 2015.

[37] J. Shao, Z. Cao, and P. Liu, "SCCR: a generic approach to simultaneously achieve CCA security and collusion-resistance in proxy re-encryption," *Security and Communication Networks*, vol. 4, no. 2, pp. 122–135, 2011.

[38] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K.-K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," *Pervasive and Mobile Computing*, vol. 28, pp. 122–134, 2016.

[39] J. Shao, R. Lu, X. Lin, and K. Liang, "Secure bidirectional proxy re-encryption for cryptographic cloud storage," *Pervasive and Mobile Computing*, vol. 28, pp. 113–121, 2016.

[40] S. Guo, Y. Zeng, J. Wei, and Q. Xu, "Attribute-based re-encryption scheme in the standard model," *Wuhan University. Journal of Natural Sciences*, vol. 13, no. 5, pp. 621–625, 2008.

[41] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Theory of Cryptography*, J. Kilian, Ed., vol. 3378 of *Lecture Notes in Computer Science*, pp. 325–341, Springer, Berlin, Germany, 2005.

[42] A. Beimel, *Secure schemes for secret sharing and key distribution [Ph.D. thesis]*, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[43] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, 2006.

[44] S. Luo, Q. Shen, and Z. Chen, "Fully secure unidirectional identity-based proxy re-encryption," in *Information Security and Cryptology—ICISC 2011: 14th International Conference, Seoul, Korea, November 30–December 2, 2011. Revised Selected Papers*, vol. 7259 of *Lecture Notes in Computer Science*, pp. 109–126, Springer, Berlin, Germany, 2011.

[45] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *Proceedings of the 7th Theory of Cryptography Conference (TCC '10), Zurich, Switzerland, February 2010*, pp. 455–479, Springer, Berlin, Germany, 2010.

[46] N. Doshi and D. C. Jinwala, "Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption," *Security and Communication Networks*, vol. 7, no. 11, pp. 1988–2002, 2014.