1-1-2013

A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security

Kaitai Liang
City University of Hong Kong

Liming Fang
Nanjing Aeronautics and Astronautics University

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Duncan S. Wong
City University of Hong Kong, dwong@uow.edu.au

A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security

Abstract

Cipher text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) extends the traditional Proxy Re-Encryption (PRE) by allowing a semi-trusted proxy to transform a cipher text under an access policy to the one with the same plaintext under another access policy (i.e. attribute-based re-encryption). The proxy, however, learns nothing about the underlying plaintext. CP-ABPRE has many real world applications, such as fine-grained access control in cloud storage systems and medical records sharing among different hospitals. Previous CP-ABPRE schemes leave how to be secure against Chosen-Cipher text Attacks (CCA) as an open problem. This paper, for the first time, proposes a new CP-ABPRE to tackle the problem. The new scheme supports attribute-based re-encryption with any monotonic access structures. Despite our scheme is constructed in the random oracle model, it can be proved CCA secure under the decisional q-parallel bilinear Diffie-Hellman exponent assumption.

Keywords

policy, ciphertext, attribute, proxy, security, re, encryption, chosen

Disciplines

Engineering | Science and Technology Studies

Publication Details

Liang, K., Fang, L., Susilo, W. & Wong, D. S. (2013). A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS-2013) (pp. 552-559). United States: IEEE Computer Society.

A Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Chosen-Ciphertext Security

Kaitai Liang*, Liming Fang†, Willy Susilo‡, and Duncan S. Wong*
*Department of Computer Science
City University of Hong Kong, Hong Kong
†Nanjing University of Aeronautics and Astronautics, Nanjing, China
‡School of Computer Science and Software Engineering
University of Wollongong, NSW, Australia

***Abstract*—Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) extends the traditional Proxy Re-Encryption (PRE) by allowing a semi-trusted proxy to transform a ciphertext under an access policy to the one with the same plaintext under another access policy (i.e.*attribute-based re-encryption*). The proxy, however, learns nothing about the underlying plaintext. CP-ABPRE has many real world applications, such as fine-grained access control in cloud storage systems and medical records sharing among different hospitals. Previous CP-ABPRE schemes leave how to be secure against Chosen-Ciphertext Attacks (CCA) as an open problem. This paper, for the first time, proposes a new CP-ABPRE to tackle the problem. The new scheme supports attribute-based re-encryption with any monotonic access structures. Despite our scheme is constructed in the random oracle model, it can be proved CCA secure under the decisional q-parallel bilinear Diffie-Hellman exponent assumption.**

***Keywords*-Proxy Re-Encryption, Ciphertext-Policy Attribute-Based Proxy Re-Encryption, Chosen-Ciphertext Security.**

I. Introduction

Introduced by Sahai and Waters [1], Attribute-Based Encryption (ABE), which is a generalization of Identity-Based Encryption (IBE), can effectively increase the flexibility of data sharing such that only parties satisfying specific policy are allowed to access the data. It comes in two flavors: one is the Key-Policy ABE (KP-ABE), and the other is the Ciphertext-Policy ABE (CP-ABE). In the former, ciphertexts are labeled with attribute sets and private keys are associated with access structures that specify which kinds of ciphertexts the receiver is able to decrypt. In the latter, however, the case is complementary. That is, ciphertexts are related to access structures, and attribute sets are assigned to private keys. ABE is applicable to many network applications, such as targeted broadcast and audit log applications [2].

We use medical data sharing as an example to illustrate the usage of CP-ABE and motivate our work. Suppose a heart-disease patient Alice would like to find a clinic for regular medical examination via an on-line medical service agent (e.g., healthgrades[1]). The clinic must be within 10 km of Campbelltown, the doctors (assigned to her) of the clinic must be the senior attending doctors and be expert at cardiology. For convenience, we denote the requirements as $I_1 = \{Cardiology \wedge Senior\ \ Attending\ \ Doctor \wedge Location: \ within\ 10\ km\ of\ Campbelltown\}$. Without loss of confidentiality, Alice prefers to encrypt the record under I_1 (i.e. $Enc(I_1, m_{Alice})$) before sending to the on-line agent. The agent (that knows I_1) then searches candidates satisfying I_1 in its database. Suppose there is a clinic matching I_1. The agent forwards the ciphertext to the clinic. Here the agent cannot access the medical data without knowledge of the private key corresponding to the ciphertext.

Upon receiving the ciphertext, the clinic satisfying I_1 can access Alice's record using its private key. To maintain the record, the clinic may back up the ciphertext locally. Suppose some medical cooperation is required in the process of the treatment, Alice's record has to be transferred to hospitals with the following requirements. The hospitals have to be within 15 km of Hurstville, and the doctors (assigned to the cooperation) of the hospitals should be the attending or chief doctors and must be expert at cardiology as well. Denote the requirements as $I_2 = \{Cardiology \wedge (Attending\ \ Doctor \vee Chief\ \ Doctor) \wedge Location: \ within\ 15\ km\ of\ Hurstville\}$. Suppose there are two hospitals, say A and B, which satisfy I_2.

Traditionally, sharing Alice's medical record with A and B (without losing confidentiality), the clinic has to first recover m_{Alice} and further encrypt the record under I_2 (i.e. $Enc(I_2, m_{Alice})$) before sending to hospitals. However, if there are N patients who need to be cooperatively treated, the clinic suffers from N pairs of encryption and decryption for the patients' records (See Fig. 1). This might be undesirable in practice due to high computational complexity.

To make data sharing be more efficiently, Proxy Re-Encryption (PRE) is proposed. Defined by Blaze, Bleumer and Strauss [3], PRE supports the delegation of decryption rights. It allows a *semi-trusted* party called *proxy* to transform a ciphertext intended for Alice into another ciphertext of the same plaintext intended for Bob. The proxy, however, learns neither the decryption keys nor the underlying plaintext. PRE is applicable to many applications, such as secure

[1]http://www.healthgrades.com/.

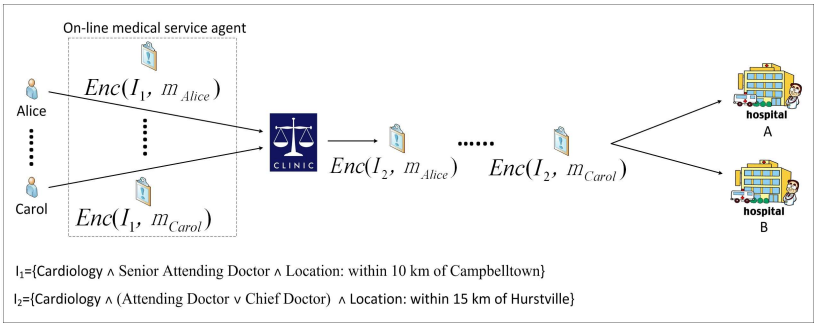

Figure 1. Traditional Attribute-Based Encryption Data Sharing

distributed files systems [4] and email forwarding [3].

To date, PRE has been extended to adapt the context of ABE. Liang et al. [5] proposed the first Ciphertext-Policy Attribute-Based PRE (CP-ABPRE) scheme, in which a proxy is allowed to transform a ciphertext under a specified access policy into the one under another access policy (i.e. *attribute-based re-encryption*).

Using CP-ABPRE the medical records sharing can be efficiently fulfilled (See Fig. 2). The clinic, acting as a delegator, notifies a cloud server (acting as the proxy) that the hospitals satisfying I_2 (i.e., delegatees), should be granted the decryption rights of the ciphertexts under I_1. The server will then transform the ciphertexts under I_1 to the ones under I_2 using a re-encryption key (e.g., $rk_{I_1 \to I_2}$ generated by the clinic), such that A and B (satisfying I_2) can access the records. Note that the server does not learn the contents (of the medical records).

Previous CP-ABPRE schemes (e.g., [5], [6], [7]), however, are only secure against *Chosen-Plaintext Attacks* (CPA). CPA security might be not sufficient in practice as it only achieves the very basic security requirement, i.e. secrecy against "passive" eavesdroppers. When CP-ABPRE is implemented in a large system, a much wider array of attacks are possible. For example, an adversary may have control over ciphertexts so as to affect decryption values or learn some partial information from decryption. Therefore, it is desirable to propose CCA secure CP-ABPRE in practice. However, the existence of CP-ABPRE with *chosen-ciphertext security* has been open.

Another open problem left by previous CP-ABPRE schemes (such as [5]), which only support AND-gates over attributes, is how to support any monotonic access policy. In practical use, it is desirable to enable a CP-ABPRE to support expressive and flexible realization for access policy. This paper also deals with this problem.

A. Our Contributions

In this work we formalize the definition for CP-ABPRE. Specifically, in our definition an attribute set and an access structure are required as auxiliary input to the re-encryption key algorithm; meanwhile, an attribute set is required in the input to the private key generation and decryption algorithms.

Regarding to the security models, we propose the *selective access structure and chosen ciphertext security* (IND-sAS-CCA) notion for CP-ABPRE. Note that it is the first time to define chosen ciphertext security model for CP-ABPRE in the literature. We consider the IND-sAS-CCA game into two different aspects: one is to allow the adversary to achieve an original ciphertext as the challenge ciphertext; the other is to allow the adversary to achieve a re-encrypted ciphertext as challenge. We refer to the security of the former and the latter as *IND-sAS-CCA security at original ciphertext* (i.e. IND-sAS-CCA-Or) and *IND-sAS-CCA security at re-encrypted ciphertext* (i.e. IND-sAS-CCA-Re), respectively. We also show that the IND-sAS-CCA-Or security implies *selective collusion resistance*, which is also named as *selective master key security* in [6].

As previously mentioned, the construction of a CP-ABPRE with CCA security remains open. This paper proposes the first single-hop unidirectional CP-ABPRE to tackle the problem. It is worth mentioning that the existing CP-ABPRE schemes (e.g., [5]) *only* support AND-gates on (multi-valued) positive and negative attributes, while our scheme provides any monotonic access formula. Despite our scheme is constructed in the random oracle model, it can be proved collusion resistant and IND-sAS-CCA secure under the decisional q-parallel bilinear Diffie-Hellman exponent (q-parallel BDHE) assumption.

Difficulty of Converting Previous CPA-Secure CP-ABPRE to Be Secure against CCA. As stated in [5], the CCA security construction for CP-ABPRE is a challenging open problem. One might think that some cryptographic primitives could help, such as the CHK transformation [8]. Despite the well-known CHK transformation can be used to convert a CPA-secure PKE scheme to be secure against CCA, it cannot be trivially employed in the PRE setting. It is used to prevent ciphertext from being mutated, but meanwhile, PRE allows transformation among ciphertexts. If an encryptor uses the CHK transformation to guarantee the

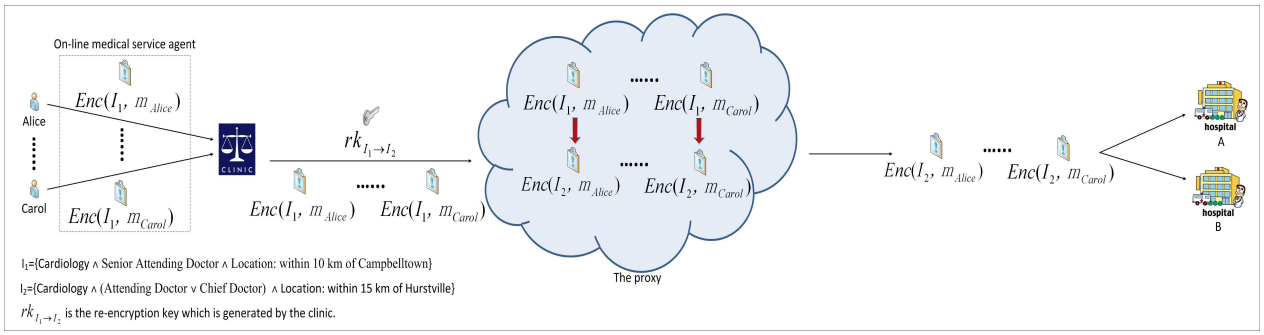

Figure 2. Ciphertext-policy attribute-based proxy re-encryption

validity of ciphertexts, it will easily incur that the validity of re-encryption results cannot be ensured. Thus, trivially employ the transformation in a PRE scheme that often results in Replayable CCA (RCCA) security [9]. The classic examples are [10], [11].

Therefore, using the CHK transformation as a black box to turn the existing CPA-secure CP-ABPRE schemes to be secure against CCA that is not trivial. In section IV, we show an efficient solution to address the difficulty.

B. Related Work

Please refer to our full paper [12] for the related work of ABE, PRE and CP-ABPRE.

We compare our scheme with [5], [6], [7] in terms of public/private key size, ciphertext/re-encryption key size, re-encryption cost and properties (see Table 1). Let f be the size of access formula, A be the number of attributes on user's private key, U be the number of all attributes used in system, $mv, +, -$ be multi-valued, positive and negative attribute, respectively. Besides, denote c_e and c_p as the computational cost of an exponentiation and a bilinear pairing. To the best of our knowledge, our scheme is the first of its kind to achieve CCA security and to support any monotonic access formula (over attributes).

C. Organization

The remaining paper is organized as follows. In section II, we introduce some basic definitions and security models for CP-ABPRE. In section III, we review some primitives and complexity assumption which are used in our scheme. In section IV we propose an efficient CCA-secure CP-ABPRE scheme. Finally, we conclude our work and discuss some open problems in section V.

II. Definitions and Security Models

Definition 1: Access Structure [13]. Let $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ be a set of parties. A collection $\mathbb{AS} \subseteq 2^{\mathcal{P}}$ is monotone if $\forall B, C$: if $B \in \mathbb{AS}$ and $B \subseteq C$ then $C \in \mathbb{AS}$. An access structure (resp., monotonic access structure) is a collection (resp., monotone collection) $\mathbb{AS}$ of non-empty subsets of $\mathcal{P}$, i.e., $\mathbb{AS} \subseteq 2^{\mathcal{P}} \setminus \{\emptyset\}$. The sets in $\mathbb{AS}$ are called the authorized sets, and the sets not in $\mathbb{AS}$ are called the unauthorized sets.

In this paper the role of the parties is taken by the attributes. The access structure $\mathbb{AS}$ contains all authorized sets of attributes. In this paper we work on monotone access structures. As shown in [13], any monotone access structure can be represented by a linear secret sharing scheme.

Definition 2: Linear Secret Sharing Schemes (LSSS) [14]. A secret-sharing scheme Π over a set of parties $\mathcal{P}$ is called linear (over $\mathbb{Z}_p$) if

- The shares for each party form a vector over $\mathbb{Z}_p$.
- There exists a matrix an M with l rows and n columns called the share-generating matrix for Π. For all $i = 1, ..., l$, the ith row of M is labeled by a party $\rho(i)$, where ρ is a function from $\{1, ..., l\}$ to $\mathcal{P}$. When we consider the column vector $v = (s, r_2, ..., r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, and $r_2, ..., r_n \in \mathbb{Z}_p$ are randomly chosen, then $M \cdot v$ is the vector of l shares of the secret s according to Π. The share $(M \cdot v)_i$ belongs to party $\rho(i)$. For any unauthorized set, no such constants exist. We use LSSS matrix (M, ρ) to represent an access policy in this paper.

Every LSSS according to the definition achieves the *linear reconstruction* property [13]. Suppose that Π is an LSSS for the access structure $\mathbb{AS}$. Let $S \in \mathbb{AS}$ (that is, S satisfies the access structure; we also denote this case as $S \models (M, \rho)$) be any authorized set, and let $I \subset \{1, 2, ..., l\}$ be defined as $I = \{i : \rho(i) \in S\}$. There will exist constants $\{w_i \in \mathbb{Z}_p\}_{i \in I}$ such that $\sum_{i \in I} w_i \cdot \lambda_i = s$ if $\{\lambda_i\}$ are valid shares of any secret s according to Π. Note that as shown in [13] $\{w_i\}$ can be found (with knowledge of M and I) in time polynomial in the size of the share-generating matrix M.

A. Definition of CP-ABPRE

Definition 3: A Single-Hop Unidirectional Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) scheme consists of the following seven algorithms:

1) $(param, msk) \leftarrow Setup(1^k, \mathcal{U})$: on input a security

Table I
COMPARISON WITH [5], [6], [7]

Schemes	Public/Private Key Size	Ciphertext/ ReKey Size	Re-Encryption Cost	Selective Model /CCA Security	Attributes Expression
CP-ABPRE [5]	$\mathcal{O}(U)/\mathcal{O}(U)$	$\mathcal{O}(U)/\mathcal{O}(U)$	$\mathcal{O}(U)\cdot c_p$	✓ /✗	AND gates on $+$ and $-$
CP-ABPRE [6]	$\mathcal{O}(U^2)/\mathcal{O}(U)$	$\mathcal{O}(U)/\mathcal{O}(U)$	$\mathcal{O}(U)\cdot c_p$	✓ /✗	AND gates on mv and $-$
CP-ABPRE [7]	$\mathcal{O}(U)/\mathcal{O}(U)$	$\mathcal{O}(U)/\mathcal{O}(U)$	$\mathcal{O}(1)\cdot c_e+\mathcal{O}(U)\cdot c_p$	✓ /✗	AND gates on $+$ and $-$
Our CP-ABPRE	$\mathcal{O}(1)/\mathcal{O}(A)$	$\mathcal{O}(f)/\mathcal{O}(A)$	$\mathcal{O}(A)\cdot c_e+\mathcal{O}(A)\cdot c_p$	✓ /✓	Any monotonic access formula

parameter $k\in\mathbb{N}$ and an attribute universe $\mathcal{U}$, output a public parameter $param$ and a master secret key msk.

2) $sk_S \leftarrow KeyGen(param, msk, S)$: on input $param$, msk and an attribute set S that describes the key, output a private key sk_S. Like traditional CP-ABE each private key sk_S is associated with an attribute set S.
3) $rk_{S\rightarrow(M',\rho')} \leftarrow ReKeyGen(param, sk_S, S, (M',\rho'))$: on input $param$, a private key sk_S and the corresponding attribute set S, and an access structure (M',ρ') for attributes over $\mathcal{U}$, output a re-encryption key $rk_{S\rightarrow(M',\rho')}$ that can be used to transform a ciphertext under (M,ρ) to the one under (M',ρ'), where $S\models(M,\rho)$, (M,ρ) and (M',ρ') are disjoint[2].
4) $C_{(M,\rho)} \leftarrow Enc(param,(M,\rho),m)$: on input $param$, an access structure (M,ρ) for attributes over $\mathcal{U}$, and a plaintext $m\in\{0,1\}^k$, output an original ciphertext $C_{(M,\rho)}$ which can be further re-encrypted. Suppose the access structure is implicitly included in the ciphertext.
5) $C^R_{(M',\rho')} \leftarrow ReEnc(param, rk_{S\rightarrow(M',\rho')}, C_{(M,\rho)})$: on input $param$, a re-encryption key $rk_{S\rightarrow(M',\rho')}$, and an original ciphertext $C_{(M,\rho)}$, output a re-encrypted ciphertext $C^R_{(M',\rho')}$ if $S\models(M,\rho)$ or a symbol $\perp$ indicating either $C_{(M,\rho)}$ is invalid or $S\not\models(M,\rho)$. Note that $C^R_{(M',\rho')}$ cannot be further re-encrypted.
6) $m \leftarrow Dec(param, S, sk_S, C_{(M,\rho)})$: on input $param$, an attribute set S and its corresponding private key sk_S, and an original ciphertext $C_{(M,\rho)}$, output a plaintext m if $S\models(M,\rho)$ or a symbol $\perp$ indicating either $C_{(M,\rho)}$ is invalid or $S\not\models(M,\rho)$.
7) $m \leftarrow Dec_R(param, S', sk_{S'}, C^R_{(M',\rho')})$: on input $param$, an attribute set S' and its corresponding private key $sk_{S'}$, and a re-encrypted ciphertext $C^R_{(M',\rho')}$, output a plaintext m if $S'\models(M',\rho')$ or a symbol $\perp$ indicating either $C^R_{(M',\rho')}$ is invalid or $S'\not\models(M',\rho')$.

For simplicity, we omit $param$ in the expression of the algorithm inputs in the rest of the paper.

Correctness: For any $k\in\mathbb{N}$, any attribute set S ($S\subseteq\mathcal{U}$) with its cardinality polynomial to k, any access structure (M,ρ) for attributes over $\mathcal{U}$ and any message $m\in\{0,1\}^k$, if $(param, msk)\leftarrow Setup(1^k,\mathcal{U})$, $sk_S\leftarrow KeyGen(msk,S)$, for all S used in the system, we have

$$Dec(S, sk_S, Enc((M,\rho),m)) = m;$$
$$Dec_R(S', sk_{S'}, ReEnc(ReKeyGen(sk_S, S, (M',\rho')), Enc((M,\rho),m))) = m,$$

where $S\models(M,\rho)$ and $S'\models(M',\rho')$.

B. Security Models

Definition 4: A single-hop unidirectional CP-ABPRE scheme is IND-sAS-CCA secure at original ciphertext if no probabilistic polynomial time (PPT) adversary $\mathcal{A}$ can win the game below with non-negligible advantage. In the game, $\mathcal{C}$ is the game challenger, k and $\mathcal{U}$ are the security parameter and attribute universe.

1) **Initialization.** $\mathcal{A}$ outputs a challenge access structure (M^*,ρ^*) to $\mathcal{C}$.
2) **Setup.** $\mathcal{C}$ runs $Setup(1^k,\mathcal{U})$ and sends $param$ to $\mathcal{A}$.
3) **Phase I.** $\mathcal{A}$ is given access to the following oracles.
   a) Private key extraction oracle $\mathcal{O}_{sk}(S)$: on input an attribute set S, $\mathcal{C}$ returns $sk_S\leftarrow KeyGen(msk,S)$ to $\mathcal{A}$.
   b) Re-encryption key extraction oracle $\mathcal{O}_{rk}(S,(M',\rho'))$: on input an attribute set S, and an access structure (M',ρ'), $\mathcal{C}$ returns $rk_{S\rightarrow(M',\rho')}\leftarrow ReKeyGen(sk_S, S, (M',\rho'))$ to $\mathcal{A}$, where $sk_S\leftarrow KeyGen(msk, S)$.
   c) Re-encryption oracle $\mathcal{O}_{re}(S,(M',\rho'),C_{(M,\rho)})$: on input an attribute set S, an access structure (M',ρ'), and an original ciphertext $C_{(M,\rho)}$, $\mathcal{C}$ returns $C^R_{(M',\rho')}\leftarrow ReEnc(rk_{S\rightarrow(M',\rho')}, C_{(M,\rho)})$ to $\mathcal{A}$, where $rk_{S\rightarrow(M',\rho')}\leftarrow ReKeyGen(sk_S,S,(M',\rho'))$, $sk_S\leftarrow KeyGen(msk,S)$ and $S\models(M,\rho)$.
   d) Original ciphertext decryption oracle $\mathcal{O}_{d2}(S,C_{(M,\rho)})$: on input an attribute set S and an original ciphertext $C_{(M,\rho)}$, $\mathcal{C}$ returns $m\leftarrow Dec(S, sk_S, C_{(M,\rho)})$ to $\mathcal{A}$, where $sk_S\leftarrow KeyGen(msk,S)$ and $S\models(M,\rho)$.
   e) Re-encrypted ciphertext decryption oracle $\mathcal{O}_{d1}(S', C^R_{(M',\rho')})$: on input an attribute set S' and

[2]Suppose (M,ρ) and (M',ρ') are two access structures. For any attribute x satisfies (M,ρ), x does not satisfy (M',ρ'). For such a case, from now on, we say that (M,ρ) and (M',ρ') are disjoint.

a re-encrypted ciphertext $C^R_{(M',\rho')}$, $\mathcal{C}$ returns $m \leftarrow Dec_R(S', sk_{S'}, C^R_{(M',\rho')})$, where $sk_{S'} \leftarrow KeyGen(msk, S')$ and $S' \models (M', \rho')$.

Note that if the ciphertexts queried to oracles $\mathcal{O}_{re}$, $\mathcal{O}_{d2}$ and $\mathcal{O}_{d1}$ are invalid, $\mathcal{C}$ simply outputs $\perp$. In this phase the following queries are forbidden to issue:

- $\mathcal{O}_{sk}(S)$ for any $S \models (M^*, \rho^*)$; and
- $\mathcal{O}_{rk}(S, (M', \rho'))$ for any $S \models (M^*, \rho^*)$, and $\mathcal{O}_{sk}(S')$ for any $S' \models (M', \rho')$.

4) **Challenge.** $\mathcal{A}$ outputs two equal length messages m_0 and m_1 to $\mathcal{C}$. $\mathcal{C}$ returns $C^*_{(M^*,\rho^*)} \leftarrow Enc((M^*, \rho^*), m_b)$ to $\mathcal{A}$, where $b \in_R \{0, 1\}$.
5) **Phase II.** $\mathcal{A}$ makes further queries except the following:
   a) $\mathcal{O}_{sk}(S)$ for any $S \models (M^*, \rho^*)$;
   b) $\mathcal{O}_{rk}(S, (M', \rho'))$ for any $S \models (M^*, \rho^*)$, and $\mathcal{O}_{sk}(S')$ for any $S' \models (M', \rho')$;
   c) $\mathcal{O}_{re}(S, (M', \rho'), C^*_{(M^*,\rho^*)})$ for any $S \models (M^*, \rho^*)$, and $\mathcal{O}_{sk}(S')$ for any $S' \models (M', \rho')$;
   d) $\mathcal{O}_{d2}(S, C^*_{(M^*,\rho^*)})$ for any $S \models (M^*, \rho^*)$; and
   e) $\mathcal{O}_{d1}(S', C^R_{(M',\rho')})$ for any $C^R_{(M',\rho')}$, $S' \models (M', \rho')$, where $C^R_{(M',\rho')}$ is a derivative of $C^*_{(M^*,\rho^*)}$. As of [15], the derivative of $C^*_{(M^*,\rho^*)}$ is defined below.
      i. $C^*_{(M^*,\rho^*)}$ is a derivative of itself.
      ii. If $\mathcal{A}$ has issued a re-encryption key query on $(S, (M', \rho'))$ to obtain the re-encryption key $rk_{S\rightarrow(M',\rho')}$, and achieved $C^R_{(M',\rho')} \leftarrow ReEnc(rk_{S\rightarrow(M',\rho')}, C^*_{(M^*,\rho^*)})$, then $C^R_{(M',\rho')}$ is a derivative of $C^*_{(M^*,\rho^*)}$, where $S \models (M^*, \rho^*)$.
      iii. If $\mathcal{A}$ has issued a re-encryption query on $(S, (M', \rho'), C^*_{(M^*,\rho^*)})$ and obtained the re-encrypted ciphertext $C^R_{(M',\rho')}$, then $C^R_{(M',\rho')}$ is a derivative of $C^*_{(M^*,\rho^*)}$, where $S \models (M^*, \rho^*)$.
6) **Guess.** $\mathcal{A}$ outputs a guess bit $b' \in \{0, 1\}$.

The advantage of $\mathcal{A}$ is defined as $\epsilon_1 = Adv^{IND-sAS-CCA-Or}_{CP-ABPRE,\mathcal{A}}(1^k, \mathcal{U}) = |Pr[b' = b] - \frac{1}{2}|$.

Definition 5: A single-hop unidirectional CP-ABPRE scheme is IND-sAS-CCA secure at re-encrypted ciphertext if the advantage $\epsilon_2 = Adv^{IND-sAS-CCA-Re}_{CP-ABPRE,\mathcal{A}}(1^k, \mathcal{U})$ is negligible for any PPT adversary $\mathcal{A}$ in the following experiment. Set $O_1 = \{\mathcal{O}_{sk}, \mathcal{O}_{rk}, \mathcal{O}_{re}, \mathcal{O}_{d2}, \mathcal{O}_{d1}\}$.

$$\epsilon_2 = |Pr[b' = b : ((M^*, \rho^*), State_1) \leftarrow \mathcal{A}(1^k); (param, msk) \leftarrow Setup(1^k, \mathcal{U}); (m_0, m_1, (M, \rho), State_2) \leftarrow \mathcal{A}^{O_1}(param, State_1); b \in_R \{0, 1\}; C^{R*}_{(M^*,\rho^*)} \leftarrow ReEnc(rk_{S\rightarrow(M^*,\rho^*)}, C_{(M,\rho)}); b' \leftarrow A^{O_1}(C^{R*}_{(M^*,\rho^*)}, State_2)] - \frac{1}{2}|,$$

where $State_1$ and $State_2$ are the state information, (M, ρ) and (M^*, ρ^*) are disjoint, (M^*, ρ^*) is the challenge access structure, $S \models (M, \rho)$, $rk_{S\rightarrow(M^*,\rho^*)} \leftarrow ReKeyGen(sk_S, S, (M^*, \rho^*))$, $C_{(M,\rho)} \leftarrow Enc((M, \rho), m_b)$, $\mathcal{O}_{sk}, \mathcal{O}_{rk}, \mathcal{O}_{re}, \mathcal{O}_{d2}, \mathcal{O}_{d1}$ are the oracles defined in Definition 4 (but) with the following constraints. For $\mathcal{O}_{sk}$, the query on S is forbidden to issue for any $S \models (M^*, \rho^*)$. For $\mathcal{O}_{rk}$, it works as in the IND-sAS-CCA-Or game. $\mathcal{O}_{re}$ will output $\perp$ if $\mathcal{A}$ queries invalid original ciphertexts or re-encrypted ciphertexts. There is no restriction for $\mathcal{O}_{d2}$ except that the oracle will reject invalid original ciphertexts. If $\mathcal{A}$ queries to $\mathcal{O}_{d1}$ on $(S, C^{R*}_{(M^*,\rho^*)})$ or invalid re-encrypted ciphertexts, the oracle outputs $\perp$, where $S \models (M^*, \rho^*)$.

We now proceed to the *selective* collusion resistance for CP-ABPRE. Like collusion resistance defined in traditional PRE, this security notion also guarantees that a dishonest proxy cannot compromise the entire private key of the delegator even it colludes with the corresponding delegatee. However, an adversary is required to output an attribute set that it wishes to attack before the setup phase. The selective collusion resistance model can be defined via the identical manner introduced in [5], [6], we hence omit the details. Instead, we prefer to show that the IND-sAS-CCA-Or security already implies selective collusion resistance.

Theorem 1: Suppose a single-hop unidirectional CP-ABPRE scheme is IND-sAS-CCA-Or secure, then it is selective collusion resistant as well.

Please refer to [12] for the proof of Theorem 1.

III. Preliminaries

Bilinear Maps. Let $BSetup$ denote an algorithm that, on input the security parameter 1^k, outputs the parameters for a bilinear map as $(p, g, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative cyclic groups with prime order $p \in \Theta(2^k)$ and g is a generator of $\mathbb{G}$. The efficient mapping $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ has three properties: (1) *Bilinearity*: for all $g \in \mathbb{G}$ and $a, b \in_R \mathbb{Z}^*_p$, $e(g^a, g^b) = e(g, g)^{ab}$; (2) *Non-degeneracy*: $e(g, g) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ is the unit of $\mathbb{G}_T$; (3) *Computability*: e can be efficiently computed.

Complexity Assumption.

Definition 6: Decisional q-parallel BDHE Assumption [14]. Given a tuple y=

$$g, g^s, g^a, ..., g^{a^q}, g^{a^{q+2}}, ..., g^{a^{2q}}$$
$$\forall_{1\leq j\leq q}\ g^{s\cdot b_j}, g^{a/b_j}, ..., g^{a^q/b_j}, g^{a^{q+2}/b_j}, ..., g^{a^{2q}/b_j}$$
$$\forall_{1\leq j,k\leq q, k\neq j}\ g^{a\cdot s\cdot b_k/b_j}, ..., g^{a^q\cdot s\cdot b_k/b_j},$$

the decisional q-parallel BDHE problem is to decide whether $T = e(g, g)^{a^{q+1}\cdot s}$, where $a, s, b_1, ..., b_q \in_R \mathbb{Z}_p, T \in_R \mathbb{G}_T$ and g is a generator of $\mathbb{G}$. Define $Adv^{D-q-parallelBDHE}_{\mathcal{A}} = |Pr[\mathcal{A}(y, e(g, g)^{a^{q+1}\cdot s}) = 0] - Pr[\mathcal{A}(y, T) = 0]|$ as the advantage of adversary $\mathcal{A}$ in winning the decisional q-parallel BDHE problem. We say that the decisional q-parallel BDHE assumption holds in $(\mathbb{G}, \mathbb{G}_T)$ if no PPT algorithm has non-negligible advantage.

Target Collision Resistant (TCR) Hash Function. The definition of TCR hash function can be found in [16] we hence omit the details.

IV. A New CP-ABPRE with CCA Security

In this section we propose a new CP-ABPRE in the random oracle model with CCA security. Prior to describing the scheme, we introduce some intuition behind our construction. We choose Waters ABE [14] as a basic building block due to the following reasons. Waters ABE utilizes LSSS to support any monotonic access formula that is a desirable and practical property for our system. Besides, the construction technique for ciphertexts, which ensures ciphertext size to be linear in the size of formula other than all system attributes, enables us to relieve the communication cost incurred by re-encrypted ciphertext and re-encryption key.

Our CP-ABPRE works as follows. Unless stated otherwise, we let $\mathcal{U}$ be the attribute universe in the system, and S be an attribute set, $S \subseteq \mathcal{U}$.

1) $Setup(1^k, \mathcal{U})$. Given a security parameter k and the attribute universe $\mathcal{U}$, run $(p, g, \mathbb{G}, \mathbb{G}_T, e) \leftarrow BSetup(1^k)$. Choose two random values $a, \alpha \in \mathbb{Z}_p^*$, a random generator $g_1 \in \mathbb{G}$, and set the following TCR hash functions $H_1 : \{0,1\}^{2k} \rightarrow \mathbb{Z}_p^*$, $H_2 : \mathbb{G}_T \rightarrow \{0,1\}^{2k}$, $H_3 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_4 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_5 : \{0,1\}^k \rightarrow \mathbb{Z}_p^*$, $H_6 : \{0,1\}^* \rightarrow \mathbb{G}$. The public parameters are $param = (p,\ g,\ \mathbb{G},\ \mathbb{G}_T,\ e,\ g_1,\ g^a,\ e(g,g)^\alpha,\ H_1,\ H_2,\ H_3,\ H_4,\ H_5,\ H_6)$, and the master secret key is $msk = g^\alpha$.
2) $KeyGen(msk, S)$. Given a master secret key msk and an attribute set S, choose $t \in_R \mathbb{Z}_p^*$, and set the private key sk_S as

$$K = g^{a \cdot t} \cdot g^\alpha, L = g^t, \forall x \in S\ K_x = H_3(x)^t.$$

3) $Enc((M, \rho), m)$. Taking an LSSS access structure (M, ρ) (M is an $l \times n$ matrix, and the function ρ associates rows of M to attributes) and a message $m \in \{0,1\}^k$ as input, the encryption algorithm works as follows.
   a) Choose $\beta \in_R \{0,1\}^k$, set $s = H_1(m, \beta)$ and a random vector $v = (s, y_2, ..., y_n)$, where $y_2, ..., y_n \in_R \mathbb{Z}_p^*$.
   b) For $i = 1$ to l, set $\lambda_i = v \cdot M_i$, where M_i is the vector corresponding to the ith row of M.
   c) Choose $r_1, ..., r_l \in_R \mathbb{Z}_p^*$, set $A_1 = (m||\beta) \oplus H_2(e(g,g)^{\alpha \cdot s})$, $A_2 = g^s$, $A_3 = g_1^s$, $B_1 = (g^a)^{\lambda_1} \cdot H_3(\rho(1))^{-r_1}$, $C_1 = g^{r_1}$, ..., $B_l = (g^a)^{\lambda_l} \cdot H_3(\rho(l))^{-r_l}$, $C_l = g^{r_l}$, $D = H_4(A_1, A_3, (B_1, C_1), ..., (B_l, C_l), (M, \rho))^s$, and output the original ciphertext $C_{(M,\rho)} = ((M, \rho),\ A_1,\ A_2,\ A_3,\ (B_1, C_1),\ ...,\ (B_l, C_l),\ D)$. Note that $\{\rho(i) | 1 \le i \le l\}$ are the attributes used in the access structure (M, ρ). Like [14], we allow an attribute to be associated with multiple rows of matrix M, i.e. the function ρ is not injective.
4) $ReKeyGen(sk_S, S, (M', \rho'))$. Given a private key $sk_S = (K, L, K_x)$ and the corresponding attribute set S, and an LSSS access structure (M', ρ'), the re-encryption key is generated as follows, where $x \in S$, M' is an $l' \times n'$ matrix, and the function ρ' associates rows of M' to attributes.
   a) Choose $\beta', \delta \in_R \{0,1\}^k$, set $s' = H_1(\delta, \beta')$ and a random vector $v' = (s', y'_2, ..., y'_{n'})$, where $y'_2, ..., y'_{n'} \in_R \mathbb{Z}_p^*$.
   b) For $i = 1$ to l', set $\lambda'_i = v' \cdot M'_i$, where M'_i is the vector corresponding to the ith row of M'.
   c) Choose $r'_1, ..., r'_{l'} \in_R \mathbb{Z}_p^*$, compute $A'_1 = (\delta||\beta') \oplus H_2(e(g,g)^{\alpha \cdot s'})$, $A'_2 = g^{s'}$, $B'_1 = (g^a)^{\lambda'_1} \cdot H_3(\rho'(1))^{-r'_1}$, $C'_1 = g^{r'_1}$, ..., $B'_{l'} = (g^a)^{\lambda'_{l'}} \cdot H_3(\rho'(l'))^{-r'_{l'}}$, $C'_{l'} = g^{r'_{l'}}$, $D' = H_6(A'_1, A'_2, (B'_1, C'_1), ..., (B'_{l'}, C'_{l'}), S, (M', \rho'))^{s'}$, and output $C_{(M',\rho')} = ((M', \rho'),\ A'_1,\ A'_2,\ (B'_1, C'_1),\ ...,\ (B'_{l'}, C'_{l'}),\ D')$.
   d) Choose $\theta \in_R \mathbb{Z}_p^*$, and set $rk_1 = K^{H_5(\delta)} \cdot g_1^\theta, rk_2 = g^\theta, rk_3 = L^{H_5(\delta)}$, $\forall x \in S\ R_x = K_x^{H_5(\delta)}, rk_4 = C_{(M',\rho')}$, and output the re-encryption key $rk_{S \rightarrow (M',\rho')} = (S, rk_1, rk_2, rk_3, rk_4, R_x)$.
5) $ReEnc(rk_{S \rightarrow (M',\rho')}, C_{(M,\rho)})$. Parse the original ciphertext $C_{(M,\rho)}$ as $((M, \rho),\ A_1,\ A_2,\ A_3,\ (B_1, C_1),\ ...,\ (B_l, C_l),\ D)$, and the re-encryption key $rk_{S \rightarrow (M',\rho')}$ as $(S, rk_1, rk_2, rk_3, rk_4, R_x)$. Recall that M is an $l \times n$ matrix. Let $I \subset \{1, ..., l\}$ be defined as $I = \{i : \rho(i) \in S\}$, $\{w_i \in \mathbb{Z}_p^*\}_{i \in I}$ be a set of constants such that $\sum_{i \in I} w_i \cdot \lambda_i = s$ if $\{\lambda_i\}$ are valid shares of any secret s according to M and $S \models (M, \rho)$[3].
   a) Verify whether the re-encryption key $rk_{S \rightarrow (M',\rho')}$ contains valid S and (M', ρ') or not

$$e(A'_2, H_6(A'_1, A'_2, (B'_1, C'_1), ..., (B'_{l'}, C'_{l'}), S, (M', \rho'))) \stackrel{?}{=} e(g, D').$$

   b) Verify the validity of the original ciphertext

$$\begin{aligned} &e(A_2, g_1) \stackrel{?}{=} e(g, A_3), e(A_3, H_4(A_1, A_3, (B_1, C_1), ..., \\ &(B_l, C_l), (M, \rho))) \stackrel{?}{=} e(g_1, D), S \stackrel{?}{\models} (M, \rho), \\ &e(\prod_{i \in I} B_i^{w_i}, g) \stackrel{?}{=} e(A_2, g^a) \cdot \prod_{i \in I} (e(C_i^{-1}, H_3(\rho(i))^{w_i})). \end{aligned} \quad (1)$$

   If Eq. (1) does not hold, output $\perp$. Otherwise, proceed.
   c) Compute $A_4 = \frac{e(A_2, rk_1)/e(A_3, rk_2)}{(\prod_{i \in I}(e(B_i, rk_3) \cdot e(C_i, R_{\rho(i)}))^{w_i})}$, and output the re-encrypted ciphertext $C^R_{(M',\rho')} = (S,\ (M, \rho),\ A_1,\ A_3,\ (B_1, C_1),\ ...,\ (B_l, C_l),\ D,\ A_4,\ rk_4)$.
6) $Dec(S, sk_S, C_{(M,\rho)})$. Parse the original ciphertext $C_{(M,\rho)}$ as $((M, \rho),\ A_1,\ A_2,\ A_3,\ (B_1, C_1),\ ...,\ (B_l, C_l),$

[3] As stated in [13], [14], with knowledge of M and I one can find the values w_i satisfying $\sum_{i \in I} w_i \cdot \lambda_i = s$.

D), and the private key sk_S (for an attribute set S) as (K, L, K_x) ($x \in S$). Note that let $I \subset \{1, ..., l\}$ be defined as $I = \{i : \rho(i) \in S\}$, $\{w_i \in \mathbb{Z}_p^*\}_{i \in I}$ be a set of constants such that $\sum_{i \in I} w_i \cdot \lambda_i = s$.

a) Verify Eq. (1). If Eq. (1) does not hold, output $\perp$. Otherwise, proceed.

b) Compute $Z = e(A_2, K)/(\prod_{i \in I}(e(B_i, L) \cdot e(C_i, K_{\rho(i)}))^{w_i})$ and $m||\beta = H_2(Z) \oplus A_1$, output m if $A_3 = g_1^{H_1(m,\beta)}$, and output $\perp$ otherwise.

7) $Dec_R(S', sk_{S'}, C^R_{(M',\rho')})$. Parse the re-encrypted ciphertext $C^R_{(M',\rho')}$ as $(S, (M, \rho), A_1, A_3, (B_1, C_1), ..., (B_l, C_l), D, A_4, rk_4)$, and the private key $sk_{S'}$ (for an attribute set S') as (K', L', K'_x) ($x \in S'$).

a) Recover $\delta||\beta'$ as follows. Let $I' \subset \{1, ..., l'\}$ be defined as $I' = \{i : \rho'(i) \in S'\}$, $\{w'_i \in \mathbb{Z}_p^*\}_{i \in I'}$ be a set of constants such that $\sum_{i \in I'} w'_i \cdot \lambda'_i = s'$ if $\{\lambda'_i\}$ are valid shares of any secret s' according to M' and $S' \models (M', \rho')$.

i) Verify the validity of rk_4

$$e(A'_2, H_6(A'_1, A'_2, (B'_1, C'_1), ..., (B'_{l'}, C'_{l'}), S, (M', \rho'))) \stackrel{?}{=} e(g, D'), S' \stackrel{?}{\models} (M', \rho'). \quad (2)$$

If Eq. (2) does not hold, output $\perp$. Otherwise, proceed.

ii) Compute $Z' = e(A'_2, K')/(\prod_{i \in I'}(e(B'_i, L') \cdot e(C'_i, K'_{\rho'(i)}))^{w'_i})$ and $\delta||\beta' = H_2(Z') \oplus A'_1$, proceed if $A'_2 = g^{H_1(\delta,\beta')}$, and output $\perp$ otherwise.

b) Compute $m||\beta = H_2(A_4^{\frac{1}{H_5(\delta)}}) \oplus A_1$, output m if $A_3 = g_1^{H_1(m,\beta)}$, $D = H_4(A_1, A_3, (B_1, C_1), ..., (B_l, C_l), (M, \rho))^{H_1(m,\beta)}$ and $S \models (M, \rho)$, and output $\perp$ otherwise.

- **Correctness for Original Ciphertext.**

$$Z = e(A_2, K)/(\prod_{i \in I}(e(B_i, L) \cdot e(C_i, K_{\rho(i)}))^{w_i})$$
$$= \frac{e(g^s, g^{a \cdot t} \cdot g^{\alpha})}{(\prod_{i \in I}(e(g^{a \cdot \lambda_i} \cdot H_3(\rho(i))^{-r_i}, g^t) \cdot e(g^{r_i}, H_3(\rho(i))^t))^{w_i})}$$
$$= \frac{e(g^s, g^{a \cdot t} \cdot g^{\alpha})}{e(g, g^{a \cdot t})^{\sum_{i \in I} \lambda_i \cdot w_i}} = e(g^s, g^{\alpha}),$$

then $H_2(Z) \oplus A_1 = H_2(e(g^s, g^{\alpha})) \oplus (m||\beta) \oplus H_2(e(g, g)^{\alpha \cdot s}) = m||\beta$.

- **Correctness for Re-Encrypted Ciphertext.**

$$A_4 = \frac{e(A_2, rk_1)/e(A_3, rk_2)}{(\prod_{i \in I}(e(B_i, rk_3) \cdot e(C_i, R_{\rho(i)}))^{w_i})}$$
$$= \frac{e(g^s, g^{\alpha \cdot H_5(\delta)}) \cdot e(g^s, g^{a \cdot t \cdot H_5(\delta)})}{e(g, g^{a \cdot t \cdot H_5(\delta)})^{\sum_{i \in I} \lambda_i \cdot w_i}} = e(g^s, g^{\alpha \cdot H_5(\delta)}),$$

then $H_2(A_4^{\frac{1}{H_5(\delta)}}) \oplus A_1 = H_2(e(g, g)^{\alpha \cdot s \cdot H_5(\delta)})^{\frac{1}{H_5(\delta)}} \oplus (m||\beta) \oplus H_2(e(g, g)^{\alpha \cdot s}) = m||\beta$.

Before giving the formal security analysis, we first give some intuition as to why the scheme is secure against CCA. For the CCA security of original ciphertext, we let $C^*_{(M^*,\rho^*)} = ((M^*, \rho^*), A_1^*, A_2^*, A_3^*, (B_1^*, C_1^*), ..., (B_l^*, C_l^*), D^*)$ be the challenge ciphertext of m_b. Suppose an adversary $\mathcal{A}$ who follows the constraints defined in Definition 4 will try to get extra advantage in guessing b by using $\mathcal{O}_{re}$ and $\mathcal{O}_{d2}$. Specifically, $\mathcal{A}$ might mutate the challenge ciphertext, and submit the resulting ciphertext to $\mathcal{O}_{re}$ and $\mathcal{O}_{d2}$. From Eq. (1), the challenger can tell the change. This is so because A_1^*, A_3^*, (B_1^*, C_1^*), ..., (B_l^*, C_l^*) are bound by D^* as well as the description of (M^*, ρ^*), where D^* is a "signature" for the components. Besides, the integrity of A_2^* is bound by A_3^*. If the ciphertext is mutated, Eq. (1) will not hold. Therefore, no extra advantage in guessing b leaks to $\mathcal{A}$.

For the CCA security of re-encrypted ciphertext, we let $C^{R*}_{(M^*,\rho^*)} = (S, (M, \rho), A_1^*, A_3^*, (B_1^*, C_1^*), ..., (B_l^*, C_l^*), D^*, A_4^*, rk_4^*)$ be the challenge ciphertext of m_b. Following Definition 5, $\mathcal{A}$ will try to gain extra advantage in winning the game with the help of $\mathcal{O}_{d1}$. Note that here given $\mathcal{O}_{re}$ $\mathcal{A}$ cannot achieve extra advantage as our scheme is single-hop, i.e. re-encrypted ciphertexts cannot be further converted.

Given $C^{R*}_{(M^*,\rho^*)}$ $\mathcal{A}$ cannot mutate the ciphertext and issue the resulting ciphertext to $\mathcal{O}_{d1}$ such that the oracle outputs a valid decryption value without any rejection. This is because A_1^*, A_3^*, (B_1^*, C_1^*), ..., (B_l^*, C_l^*) and (M, ρ) are bound by D^*; meanwhile, S and (M^*, ρ^*) are bound by rk_4^*, where rk_4^* is secure against CCA[4]. The only consideration left is the integrity of A_4^*. We state that if A_4^* is mutated, the challenger can tell the change with non-negligible probability. Please refer to the proof for details. Hence $\mathcal{A}$ cannot acquire extra advantage by using $\mathcal{O}_{d1}$.

Therefore we have the following theorems.

Theorem 2: Suppose the decisional q-parallel BDHE assumption holds in $(\mathbb{G}, \mathbb{G}_T)$, and H_1, H_2, H_3, H_4, H_5, H_6 are the TCR hash functions, our CP-ABPRE scheme is IND-sAS-CCA-Or secure in the random oracle model.

Theorem 3: Suppose the decisional q-parallel BDHE assumption holds in $(\mathbb{G}, \mathbb{G}_T)$, and H_1, H_2, H_3, H_4, H_5, H_6 are the TCR hash functions, our CP-ABPRE scheme is IND-sAS-CCA-Re secure in the random oracle model.

Please refer to [12] for the proof of Theorem 2 and Theorem 3.

V. Conclusion

In this work we proposed a new single-hop unidirectional CP-ABPRE scheme, which supports attribute-based re-encryption with any monotonic access structure, to tackle the open problems left by the existing CP-ABPRE schemes. We also proved our scheme to be collusion resistant and IND-sAS-CCA secure in the random oracle model assuming the decisional q-parallel BDHE assumption holds.

[4]It can be seen that D' is a "signature" for all the components contained in rk_4^* (except D' itself) and S, and A'_2 is the "verification key".

Removing the ROM. The technique introduced in [17], [18] might be a possible approach to remove random oracles. We leave this as our future work.

This paper also motivates some interesting open problems, for example, how to construct a CCA secure CP-ABPRE scheme in the adaptive access structure model, i.e. achieving IND-aAS-CCA security.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their insightful comments and helpful suggestions.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *EUROCRYPT*, Lecture Notes in Computer Science, R. Cramer, Ed., vol. 3494. Springer, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, A. Juels, R. N. Wright, and S. D. C. di Vimercati, Eds. ACM, 2006, pp. 89–98.

[3] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *EUROCRYPT*, Lecture Notes in Computer Science, K. Nyberg, Ed., vol. 1403. Springer, 1998, pp. 127–144.

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, 2006.

[5] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *ASI-ACCS*, W. Li, W. Susilo, U. K. Tupakula, R. Safavi-Naini, and V. Varadharajan, Eds. ACM, 2009, pp. 276–286.

[6] S. Luo, J. bin Hu, and Z. Chen, "Ciphertext policy attribute-based proxy re-encryption," in *ICICS*, Lecture Notes in Computer Science, M. Soriano, S. Qing, and J. López, Eds., vol. 6476. Springer, 2010, pp. 401–415.

[7] T. Mizuno and H. Doi, "Hybrid proxy re-encryption scheme for attribute-based encryption," in *Inscrypt*, Lecture Notes in Computer Science, F. Bao, M. Yung, D. Lin, and J. Jing, Eds., vol. 6151. Springer, 2009, pp. 288–302.

[8] D. Boneh, R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," *SIAM J. Comput.*, vol. 36, no. 5, pp. 1301–1328, 2007.

[9] R. Canetti, H. Krawczyk, and J. B. Nielsen, "Relaxing chosen-ciphertext security," in *CRYPTO*, Lecture Notes in Computer Science, D. Boneh, Ed., vol. 2729. Springer, 2003, pp. 565–582.

[10] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1786–1802, 2011.

[11] K. Emura, A. Miyaji, and K. Omote, "A timed-release proxy re-encryption scheme," *IEICE Transactions*, vol. 94-A, no. 8, pp. 1682–1695, 2011.

[12] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," Cryptology ePrint Archive.

[13] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[14] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography*, Lecture Notes in Computer Science, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds., vol. 6571. Springer, 2011, pp. 53–70.

[15] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *ACM Conference on Computer and Communications Security*, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 185–194.

[16] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," *SIAM J. Comput.*, vol. 33, no. 1, pp. 167–226, January 2004.

[17] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A cca-secure identity-based conditional proxy re-encryption without random oracles," in *ICISC*, Lecture Notes in Computer Science, T. Kwon, M.-K. Lee, and D. Kwon, Eds., vol. 7839. Springer, 2012, pp. 231–246.

[18] J. Weng, M. Chen, Y. Yang, R. H. Deng, K. Chen, and F. Bao, "CCA-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles," *Science China Information Sciences*, vol. 53, no. 3, pp. 593–606, 2010.