An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing

Kaitai Liang[1], Man Ho Au[2], Willy Susilo[2,⋆], Duncan S. Wong[1,⋆⋆], Guomin Yang[2], and Yong Yu[2,⋆⋆⋆]

[1] Department of Computer Science, City University of Hong Kong, China
kliang4-c@my.cityu.edu.hk, duncan@cityu.edu.hk
[2] Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia
{aau,wsusilo,gyang,yyong}@uow.edu.au

Abstract. A Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) employs the PRE technology in the attribute-based encryption cryptographic setting, in which the proxy is allowed to convert an encryption under an access policy to another encryption under a new access policy. CP-ABPRE is applicable to many real world applications, such as network data sharing. The existing CP-ABPRE systems, however, leave how to achieve adaptive CCA security as an interesting open problem. This paper, for the first time, proposes a new CP-ABPRE to tackle the problem by integrating the dual system encryption technology with selective proof technique. The new scheme supports any monotonic access structures. Although our scheme is built in the composite order bilinear group, it is proven adaptively CCA secure in the standard model without jeopardizing the expressiveness of access policy.

Keywords: Ciphertext-Policy Attribute-Based Encryption, Ciphertext-Policy Attribute-Based Proxy Re-Encryption, Adaptive Chosen-Cipher text Security.

1 Introduction

Attribute-Based Encryption (ABE) [10,21], which is a generalization of Public Key Encryption (PKE), provides flexibility of data sharing for system users such that a data encryptor is allowed to specify some descriptive values x for an encryption and thus, the encryption can be decrypted successfully by a secret

⋆ W. Susilo is partially supported by the Australian Research Council Linkage Project LP120200052.
⋆⋆ D. S. Wong is supported by a grant from the RGC of the HKSAR, China (Project No. CityU 121512).
⋆⋆⋆ Y. Yu is supported by the Vice Chancellor's research fellowship of University of Wollongong and the NSFC of China under Grant 61003232.

X. Huang and J. Zhou (Eds.): ISPEC 2014, LNCS 8434, pp. 448–461, 2014.

key associated with some descriptive values y matching x. ABE has many applications, such as audit log applications [10]. It usually has two classifications: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In a KP-ABE system, ciphertexts are associated with attribute sets and secret keys are associated with access policies. However, CP-ABE is complementary. This paper deals with the case of CP-ABE.

In a cloud storage system, a user, say Alice, may encrypt a data under a specified access policy such that other system users satisfying this policy can access the data. She might encrypt her profile under a policy $AP_1 =$ ("*Department* : *Human Resource*" *and* "*Position* : *Team manager or above*") before uploading to the cloud. The system users satisfying AP_1 then can download the ciphertext from the cloud, and next access the data by using the corresponding secret keys. This data sharing pattern, nonetheless, does not scale well when the policy needs to be updated frequently. Suppose the policy above is updated as $AP_2 =$ ("*Department* : *Human Resource or Materials Storage*" *and* "*Position* : *Team manager only*"), Alice then should generate a new encryption accordingly. If Alice does not back up the data locally, she needs to download the ciphertext so as to recovers the data first. If the access policy is updated N times, Alice needs to construct N new encryptions. This might not be desirable as Alice's workload is linearly in N. Besides, if she is off-line or using some resource-limited devices which cannot afford such heavy computational cost, the data sharing might not be handled effectively.

To efficiently share data, we may leverage Proxy Re-Encryption (PRE). PRE is introduced by Mambo and Okamoto [19], and further studied by Blaze, Bleumer and Strauss [5]. It is an interesting extension of PKE providing the delegation of decryption rights. Specifically, it allows a *semi-trusted* proxy to transform a ciphertext intended for Alice into another ciphertext of the same plaintext intended for another system user, say Bob, without revealing knowledge of the secret keys and the underlying plaintext. It is applicable to many network applications, such as secure distributed files systems [1] and email forwarding [5].

To integrate PRE in the ABE cryptographic setting, Liang et al. [16] defined Ciphertext-Policy Attribute-Based PRE (CP-ABPRE), and proposed a concrete CP-ABPRE system enabling proxy to transform an encryption under a specified access policy into another encryption under a new access policy. We refer to this special functionality as *attribute-based re-encryption*. By using the technology of CP-ABPRE, Alice can share the data more efficiently. She first generates a re-encryption key from her own attribute set to a new access policy AP_2, and next uploads the key to the cloud such that the cloud server then can convert the original encryption under AP_1 to a new encryption under AP_2. The server, nevertheless, cannot learn the data during the conversion of cipehrtexts.

Although CP-ABPRE explores the applications of PRE, they leave us interesting open problems. All the existing CP-ABPRE schemes in the literature are secure against *selective chosen-plaintext attacks* (selective CPA) only except [15] which is *selective chosen-ciphertext attacks* (selective CCA) secure. We state that CPA security might not be sufficient enough in an open network as it only

guarantees the secrecy of data which only allows an encryption to be secure against "static" adversaries. Nevertheless, in a real network scenario, there might exist "active" adversaries trying to tamper an encryption in transit and next observing its decryption so as to obtain useful information related to the underlying data. Accordingly, a CP-ABPRE system being secure against CCA is needed as CCA security not only helps the system preclude the above subtle attacks but also enables the system to be further developed and next securely "embedded" to a large protocol/system implementing in arbitrary network environments. In addition, a CP-ABPRE system with selective security, which limits an adversary to choose an attack target before playing security game, might not scale in practice as well. This is so because a realistic adversary can adaptively choose his attack target upon attacking a cryptosystem. Therefore, an *adaptively CCA secure* CP-ABPRE scheme is needed in most of practical network applications.

The expressiveness of access policy is another crucial factor for a practical CP-ABPRE system. An access policy should be embedded with AND, OR gates, and even more meaningful expression. For instance, Alice might choose to share her profile with some officials of the same company under the access policy $AP_3 = (\text{"}Department: \ allexcept \ Human \ Resource\text{"} \ and \ \text{"}Position: \ Project \ head \ or \ team \ manager\text{"})$. Nevertheless, most of the existing CP-ABPRE schemes only support access policy with AND gates operating over attributes. This limits their practical use. Thus it is desirable to propose a CP-ABPRE system supporting more expressive access policy.

1.1 Our Contributions

This work first formalizes the notion of adaptive CCA security for CP-ABPRE systems. Compared to the selective CPA security notion, our new notion enables an adversary to commit to a target access policy in the challenge phase, and to gain access to re-encryption and decryption oracles additionally. To tackle the open problems mentioned previously, this paper proposes a novel single-hop unidirectional CP-ABPRE system. In addition, the new system supports any monotonic access policy such that system users are allowed to fulfill more flexible delegation of decryption rights. Despite our scheme is built in the composite order bilinear group, it is proven adaptively CCA secure in the standard model by integrating the dual system encryption technology with the selective proof technique.

1.2 Related Work

Below we review some ABE systems related to this work. Following the introduction of ABE due to Sahai and Waters [21], Goyal et al. [10] proposed the first KP-ABE system. Later, Bethencourt, Sahai and Waters [4] defined a complementary notion, i.e. CP-ABE. After that there are some CP-ABE schemes (e.g. [7,9,22,2]) that have been proposed. Recently, Waters [23] proposed a deterministic finite automata-based functional encryption where policy is expressed by arbitrary-size regular language.

The aforementioned schemes, nonetheless, are only selective secure (except for [4] being proven in the generic group model). To convert one of the CP-ABE systems [22] to achieve fully security, Lewko et al. [13] leveraged the dual system encryption technology. But their conversion yields some loss of expressiveness. Later, Lewko and Waters [14] introduced a new method to guarantee the expressiveness by employing the selective proof technique into the dual system encryption technology. Inspired by [14,22], this paper focuses on constructing the first CP-ABPRE with adaptive CCA security in the standard model.

Decryption rights delegation is introduced in [19]. Later, Blaze, Bleumer and Strauss [5] defined PRE. PRE can be classified as: unidirectional and bidirectional PRE, and single-hop and multi-hop PRE [1]. This present work deals with the single-hop unidirectional case. Since its introduction many PRE systems have been proposed, e.g., [1,6,12,17,11,24,25,26].

To employ PRE in the context of ABE, Liang et al. [16] defined CP-ABPRE, and further extended [7] to support proxy re-encryption. Their work provides AND gates over positive and negative attributes. Luo et al. [18] proposed an extension of [16] supporting policy with AND gates on multi-valued and negative attributes. To combine ABE with IBE by using PRE technique, Mizuno and Doi [20] proposed a special type of CP-ABPRE scheme where encryptions in the form of ABE can be converted to the ones being decrypted in the context of IBE. The previously introduced systems, however, are selectively CPA secure, and their policies are lack of expressiveness due to supporting AND gates over attributes only. Thus an adaptively CCA-secure CP-ABPRE scheme with more expressive access policy remains open. This paper deals with this problem.

Below we compare this work with some CP-ABPRE schemes. We let p be the number of attributes used in an access policy, a be the number of attributes embedded in a user's secret key and u be the total number of attributes used in the system. In the worst case, an access policy and a user's secret key might be embedded with all system attributes, that is $p = a = u$. Thus we have $p, a \leq u$. We use c_e and c_p to denote the computational cost of an exponentiation and a bilinear pairing. To the best of our knowledge, our scheme is the first to achieve adaptive CCA security, and to support any monotonic access formula.

Table 1. Comparison with [16,18,20]

Schemes	Public/Secret Key Size	Ciphertext Size	Re-Encryption Cost	Adaptive Security	CCA Security
[16]	$\mathcal{O}(u)/\mathcal{O}(u)$	$\mathcal{O}(u)$	$\mathcal{O}(u) \cdot c_p$	✗	✗
[18]	$\mathcal{O}(u^2)/\mathcal{O}(u)$	$\mathcal{O}(u)$	$\mathcal{O}(u) \cdot c_p$	✗	✗
[20]	$\mathcal{O}(u)/\mathcal{O}(u)$	$\mathcal{O}(u)$	$\mathcal{O}(1) \cdot c_e + \mathcal{O}(u) \cdot c_p$	✗	✗
Ours	$\mathcal{O}(u)/\mathcal{O}(a)$	$\mathcal{O}(p)$	$\mathcal{O}(a) \cdot c_e + \mathcal{O}(a) \cdot c_p$	✓	✓

2 Definitions and Security Models

We review the definition of CP-ABPRE systems, and next define the adaptive CCA security notion. Due to limited space we refer the reader to [22] for the details of access structure and Linear Secret Sharing Schemes.

2.1 Definition of CP-ABPRE

We review the definition of single-hop unidirectional CP-ABPRE [16,18].

Definition 1. *A Single-Hop Unidirectional Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) scheme consists of the following algorithms:*

1. $(param, msk) \leftarrow Setup(1^k, \mathcal{U})$*: on input a security parameter* $k \in \mathbb{N}$ *and an attribute universe* $\mathcal{U}$*, output the public parameters* $param$ *and a master secret key* msk*.*
2. $sk_S \leftarrow KeyGen(param, msk, S)$*: on input* $param$*,* msk *and an attribute set* S *describing the key, output a secret key* sk_S *for* S*.*
3. $rk_{S\rightarrow(A',\rho')} \leftarrow ReKeyGen(param, sk_S, (A', \rho'))$*: on input* $param$*,* sk_S*, and an access structure* (A', ρ') *for attributes over* $\mathcal{U}$*, output a re-encryption key* $rk_{S\rightarrow(A',\rho')}$ *which can be used to transform a ciphertext under* (A, ρ) *to another ciphertext under* (A', ρ')*, where* $S \models (A, \rho)$*,* $S \not\models (A', \rho')$*,* (A, ρ) *and* (A', ρ') *are two disjoint access structures. Note by two disjoint access structures we mean for any attribute* x *satisfies* (A, ρ)*,* x *does not satisfy* (A', ρ')*.*
4. $C \leftarrow Encrypt(param, (A, \rho), m)$*: on input* $param$*,* (A, ρ)*, and a message* $m \in \{0,1\}^k$*, output an original ciphertext* C *which can be further re-encrypted. Note* (A, ρ) *is implicitly included in the ciphertext.*
5. $C_R \leftarrow ReEnc(param, rk_{S\rightarrow(A',\rho')}, C)$*: on input* $param$*,* $rk_{S\rightarrow(A',\rho')}$*, and a* C *under* (A, ρ)*, output a re-encrypted ciphertext* C_R *under* (A', ρ') *if* $S \models (A, \rho)$ *or a symbol* $\perp$ *indicating either* C *is invalid or* $S \not\models (A, \rho)$*. Note* C_R *cannot be further re-encrypted.*
6. $m \leftarrow Dec(param, sk_S, C)$*: on input* $param$*,* sk_S*, and a* C *under* (A, ρ)*, output a message* m *if* $S \models (A, \rho)$ *or a symbol* $\perp$ *indicating either* C *is invalid or* $S \not\models (A, \rho)$*.*
7. $m \leftarrow Dec_R(param, sk_S, C_R)$*: on input* $param$*,* sk_S*, and a* C_R *under* (A, ρ)*, output a message* m *if* $S \models (A, \rho)$ *or a symbol* $\perp$ *indicating either* C_R *is invalid or* $S \not\models (M, \rho)$*.*

2.2 Security Models

Definition 2. *A single-hop unidirectional CP-ABPRE scheme is IND-CCA secure at original ciphertext if no Probabilistic Polynomial Time (PPT) adversary* $\mathcal{A}$ *can win the game below with non-negligible advantage. Below* $\mathcal{C}$ *is the game challenger.*

1. ***Setup.*** $\mathcal{C}$ *runs* $Setup(1^k, \mathcal{U})$ *and sends* $param$ *to* $\mathcal{A}$*.*

2. ***Phase 1.***
   (a) *Secret key extraction oracle* $\mathcal{O}_{sk}(S)$*: on input an attribute set* S*,* $\mathcal{C}$ *runs* $sk_S \leftarrow KeyGen(param, msk, S)$ *and returns* sk_S *to* $\mathcal{A}$*.*
   (b) *Re-encryption key extraction oracle* $\mathcal{O}_{rk}(S, (A', \rho'))$*: on input* S*, and an access structure* (A', ρ')*,* $\mathcal{C}$ *outputs* $rk_{S\rightarrow(A',\rho')} \leftarrow ReKeyGen(param, sk_S, (A', \rho'))$*, where* $sk_S \leftarrow KeyGen(param, msk, S)$*.*
   (c) *Re-encryption oracle* $\mathcal{O}_{re}(S, (A', \rho'), C)$*: on input* S*,* (A', ρ')*, an original ciphertext* C *under* (A, ρ)*,* $\mathcal{C}$ *outputs* $C_R \leftarrow ReEnc(param, rk_{S\rightarrow(A',\rho')}, C)$*, where* $rk_{S\rightarrow(A',\rho')} \leftarrow ReKeyGen(param, sk_S, (A', \rho'))$*,* $sk_S \leftarrow KeyGen(param, msk, S)$ *and* $S \models (A, \rho)$*.*
   (d) *Original ciphertext decryption oracle* $\mathcal{O}_{dec}(S, C)$*: on input* S *and a* C *under* (A, ρ)*,* $\mathcal{C}$ *returns* $m \leftarrow Dec(param, sk_S, C)$ *to* $\mathcal{A}$*, where* $sk_S \leftarrow KeyGen(param, msk, S)$ *and* $S \models (A, \rho)$*.*
   (e) *Re-encrypted ciphertext decryption oracle* $\mathcal{O}_{dec_R}(S, C_R)$*: on input* S *and a* C_R *under* (A, ρ)*,* $\mathcal{C}$ *returns* $m \leftarrow Dec_R(param, sk_S, C_R)$*, where* $sk_S \leftarrow KeyGen(param, msk, S)$ *and* $S \models (A, \rho)$*.*

   If ciphertexts issued to $\mathcal{O}_{re}$*,* $\mathcal{O}_{dec}$ *and* $\mathcal{O}_{dec_R}$ *are invalid, outputs* $\perp$*.*
3. ***Challenge.*** $\mathcal{A}$ *outputs two equal length messages* m_0 *and* m_1*, and a challenge access structure* (A^*, ρ^*) *to* $\mathcal{C}$*. If the following queries*

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

   are never made, $\mathcal{C}$ *returns* $C^* = Encrypt(param, (A^*, \rho^*), m_b)$ *to* $\mathcal{A}$*, where* $b \in_R \{0, 1\}$*.*
4. ***Phase 2.*** $\mathcal{A}$ *continues making queries except the followings:*
   (a) $\mathcal{O}_{sk}(S)$ *for any* $S \models (A^*, \rho^*)$*;*
   (b) $\mathcal{O}_{rk}(S, (A', \rho'))$ *for any* $S \models (A^*, \rho^*)$*, and* $\mathcal{O}_{sk}(S')$ *for any* $S' \models (A', \rho')$*;*
   (c) $\mathcal{O}_{re}(S, (A', \rho'), C^*)$ *for any* $S \models (A^*, \rho^*)$*, and* $\mathcal{O}_{sk}(S')$ *for any* $S' \models (A', \rho')$*;*
   (d) $\mathcal{O}_{dec}(S, C^*)$ *for any* $S \models (A^*, \rho^*)$*; and*
   (e) $\mathcal{O}_{dec_R}(S, C_R)$ *for any* C_R *under* (A, ρ)*,* $S \models (A, \rho)$*, where* C_R *is a derivative of* C^**. As of [6], the derivative of* C^* *is defined as:*
      i. C^* *is a derivative of itself.*
      ii. *If* $\mathcal{A}$ *has issued a re-encryption key query on* $(S^*, (A', \rho'))$ *to get* $rk_{S^*\rightarrow(A',\rho')}$*, obtained* $C_R \leftarrow ReEnc(param, rk_{S^*\rightarrow(A',\rho')}, C^*)$ *such that* $Dec_R(param, sk_{S'}, C_R) \in \{m_0, m_1\}$*, then* C_R *is a derivative of* C^**, where* $S^* \models (A^*, \rho^*)$ *and* $S' \models (A', \rho')$*.*
      iii. *If* $\mathcal{A}$ *has issued a re-encryption query on* $(S, (A', \rho'), C^*)$ *and obtained the re-encrypted ciphertext* C_R*, then* C_R *is a derivative of* C^**, where* $S \models (A^*, \rho^*)$*.*
5. ***Guess.*** $\mathcal{A}$ *outputs a guess bit* $b' \in \{0, 1\}$*. If* $b' = b$*,* $\mathcal{A}$ *wins.*

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

Definition 3. *A single-hop unidirectional CP-ABPRE scheme is IND-CCA secure at re-encrypted ciphertext if the advantage* $Adv^{IND\text{-}CCA\text{-}Re}_{CP\text{-}ABPRE,\mathcal{A}}(1^k, \mathcal{U})$ *is negligible for any PPT adversary* $\mathcal{A}$ *in the following experiment. Set* $\mathcal{O} = \{\mathcal{O}_{sk}, \mathcal{O}_{rk}, \mathcal{O}_{dec}, \mathcal{O}_{dec_R}\}$.

$$Adv^{IND\text{-}CCA\text{-}Re}_{CP\text{-}ABPRE,\mathcal{A}}(1^k,\mathcal{U}) = |Pr[b' = b : (param, msk) \leftarrow Setup(1^k,\mathcal{U});$$
$$(m_0, m_1, (A^*, \rho^*), (A, \rho)) \leftarrow \mathcal{A}^{\mathcal{O}}(param); b \in_R \{0,1\};$$
$$C^*_R \leftarrow ReEnc(param, rk_{S\rightarrow(A^*,\rho^*)}, C); b' \leftarrow A^{\mathcal{O}}(C^*_R)] - \frac{1}{2}|,$$

where (A, ρ) *and* (A^*, ρ^*) *are disjoint,* (A^*, ρ^*) *is the challenge access structure,* $S \models (A, \rho)$, $rk_{S\rightarrow(A^*,\rho^*)} \leftarrow ReKeyGen(param, sk_S, (A^*, \rho^*))$, $C \leftarrow Encrypt(param, (A, \rho), m_b)$, $\mathcal{O}_{sk}, \mathcal{O}_{rk}, \mathcal{O}_{dec}, \mathcal{O}_{dec_R}$ *are the oracles defined in Definition 2. However, these oracles are restricted by the following constraints. For* $\mathcal{O}_{sk}$*, any query* $S \models (A^*, \rho^*)$ *is rejected. There is no restriction to* $\mathcal{O}_{rk}$ *and* $\mathcal{O}_{dec}$ *(note invalid ciphertexts issued to* $\mathcal{O}_{dec}$ *are rejected). If* $\mathcal{A}$ *queries to* $\mathcal{O}_{dec_R}$ *on either* (S, C^*_R) *in which* $S \models (A^*, \rho^*)$ *or any invalid re-encrypted ciphertext, the oracle outputs* $\perp$.

Remarks. Definition 3 implies collusion resistance. If $\mathcal{A}$ can compromise sk_{S^*} from either $rk_{S^*\rightarrow(A,\rho)}$ or $rk_{S\rightarrow(A^*,\rho^*)}$, $\mathcal{A}$ wins the game with non-negligible probability, where $S \models (A, \rho)$, $S^* \models (A^*, \rho^*)$ and sk_S is given.

3 An Adaptively CCA-Secure CP-ABPRE

3.1 Construction

Due to limited space we review composite order bilinear groups, complexity assumptions, and one-time symmetric encryption in Appendix A.

1. **Setup**$(1^k,\mathcal{U})$. Run $(N, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(1^k)$, where $N = p_1p_2p_3$ is the order of group $\mathbb{G}$ and p_1, p_2, p_3 are distinct primes. Let $\mathbb{G}_{p_i}$ denote the subgroup of order p_i in group $\mathbb{G}$. Choose $a, \alpha, \kappa, \beta, \epsilon \in_R \mathbb{Z}_N$, $g, \hat{g}_1 \in_R \mathbb{G}_{p_1}$, two Target Collision Resistance hash functions [8] $TCR_1 : \mathbb{G}_T \rightarrow \mathbb{Z}_N$, $TCR_2 : \mathbb{G}_T \rightarrow \{0,1\}^{poly(1^k)}$, a CCA-secure one-time symmetric encryption system SYM and a strongly existential unforgeable one-time signature system [3] OTS. For each attribute $i \in \mathcal{U}$, choose $h_i \in_R \mathbb{Z}_N$. The $param$ is $(N, g, \hat{g}_1, g^a, g^\kappa, g^\beta, g^\epsilon, e(g,g)^\alpha, \forall i \in \mathcal{U}\ H_i = g^{h_i}, TCR_1, TCR_2, SYM, OTS)$, and the msk is (g^α, g_3), where g_3 is a generator of $\mathbb{G}_{p_3}$.
2. **KeyGen**$(param, msk, S)$. Choose $t, u \in_R \mathbb{Z}_N, R, R', R'', \{R_i\}_{i\in S} \in_R \mathbb{G}_{p_3}$, and set the secret key sk_S as
$$(S, K = g^\alpha g^{at} g^{\kappa u} R, K' = g^u R', K'' = g^t R'', \forall i \in S\ K_i = H_i^t R_i).$$
3. **Encrypt**$(param, (A, \rho), m)$. Given an LSSS access structure (A, ρ) and a message $m \in \mathbb{G}_T$ in which A is an $l \times n$ matrix and ρ is a map from each row A_j to an attribute $\rho(j)$,

(a) Choose a random vector $v = (s, v_2, ..., v_n) \in_R \mathbb{Z}_N^n$.
(b) For each A_j, choose $r_j \in_R \mathbb{Z}_N$, run $(ssk, svk) \leftarrow OTS.KeyGen(1^k)$ and set

$$B_0 = m \cdot e(g,g)^{\alpha s}, B_1 = g^s, B_2 = (g^\kappa)^s, B_3 = (\hat{g}_1^{svk} g^\beta)^s, B_4 = (g^\epsilon)^s,$$
$$\forall j \in [1,l](C_j = (g^a)^{A_j v} H_{\rho(j)}{}^{-r_j}, D_j = g^{r_j}),$$
$$E = OTS.Sign(ssk, (B_0, B_1, B_3, \forall j \in [1,l]\ (C_j, D_j))).$$

(c) Output $C = (svk,\ B_0,\ B_1,\ B_2,\ B_3,\ B_4,\ \forall j \in [1,l]\ (C_j, D_j),\ E)$. Note $\{\rho(j) | 1 \le j \le l\}$ are the attributes used in (A, ρ).

4. **ReKeyGen**$(param, sk_S, (A', \rho'))$. Given $sk_S = (S, K, K', K'', \forall i \in S\ K_i)$ and an LSSS access structure (A', ρ'),
(a) Choose $\theta_1, \theta_2, \theta_3 \in_R \mathbb{Z}_N, \delta \in_R \mathbb{G}_T$, set $rk_1 = (Kg^{\kappa\theta_1} g^{a\theta_2})^{TCR_1(\delta)} g^{\epsilon\theta_3}$, $rk_2 = (K' g^{\theta_1})^{TCR_1(\delta)}$, $rk_3 = (K'' g^{\theta_2})^{TCR_1(\delta)}$, $rk_4 = g^{\theta_3}$, $\forall i \in S\ rk_{5,i} = (K_i H_i^{\theta_2})^{TCR_1(\delta)}$.
(b) Choose a random vector $v^{(rk)} = (s^{(rk)}, v_2^{(rk)}, ..., v_n^{(rk)}) \in_R \mathbb{Z}_N^n$. For each row A'_j of A', choose $r_j^{(rk)} \in_R \mathbb{Z}_N$, run $(ssk^{(rk)}, svk^{(rk)}) \leftarrow OTS.KeyGen(1^k)$ and set rk_6 as

$$svk^{(rk)}, B_0^{(rk)} = \delta \cdot e(g,g)^{\alpha s^{(rk)}}, B_1^{(rk)} = g^{s^{(rk)}}, B_2^{(rk)} = (g^\kappa)^{s^{(rk)}},$$
$$B_3^{(rk)} = (\hat{g}_1^{svk^{(rk)}} g^\beta)^{s^{(rk)}}, \forall j \in [1,l]\ (C_j^{(rk)} = (g^a)^{A'_j v^{(rk)}} H_{\rho'(j)}{}^{-r_j^{(rk)}},$$
$$D_j^{(rk)} = g^{r_j^{(rk)}}), E^{(rk)} = OTS.Sign(ssk^{(rk)}, (B_0^{(rk)}, B_1^{(rk)}, B_3^{(rk)},$$
$$\forall j \in [1,l]\ (C_j^{(rk)}, D_j^{(rk)}))).$$

(c) Output $rk_{S \to (A', \rho')} = (rk_1,\ rk_2,\ rk_3,\ rk_4,\ \forall i \in S\ rk_{5,i},\ rk_6)$.

5. **ReEnc**$(param, rk_{S \to (A', \rho')}, C)$. Parse the original ciphertext C under (A, ρ) as $(svk,\ B_0,\ B_1,\ B_2,\ B_3,\ B_4,\ \forall j \in [1,l]\ (C_j,\ D_j),\ E)$, and the re-encryption key $rk_{S \to (A', \rho')}$ as $(rk_1,\ rk_2,\ rk_3,\ rk_4,\ \forall i \in S\ rk_{5,i},\ rk_6)$.
(a) Check the validity of the original ciphertext C as

$$e(B_1, g^\kappa) \stackrel{?}{=} e(B_2, g), e(B_1, \hat{g}_1^{svk} g^\beta) \stackrel{?}{=} e(B_3, g), e(B_1, g^\epsilon) \stackrel{?}{=} e(B_4, g),$$
$$e(\prod_{\rho(j) \in S} C_j^{w_j}, g) \stackrel{?}{=} e(B_1, g^a) \cdot \prod_{\rho(j) \in S} (e(D_j^{-1}, H_{\rho(j)}^{w_j})), S \stackrel{?}{\models} (A, \rho),$$
$$OTS.Verify(svk, (E, (B_0, B_1, B_3, \forall j \in [1,l]\ (C_j, D_j)))) \stackrel{?}{=} 1, \qquad (1)$$

where w_j are chosen by the proxy so that $\sum_{\rho(j) \in S} w_j A_j = (1, 0, ..., 0)$. If Eq. (1) does not hold, output $\perp$. Otherwise, proceed.
(b) Compute $F = \frac{e(B_1, rk_1) e(B_2, rk_2)^{-1} e(B_4, rk_4)^{-1}}{(\prod_{\rho(j) \in S} (e(C_j, rk_3) e(D_j, rk_{5,j}))^{w_j})}$, run $\sigma_1 = SYM.Enc(TCR_2(key), G)$, where $G = (C || rk_6 || F)$ and $key \in_R \mathbb{G}_T$.
(c) Choose a random vector $v^{(re)} = (s^{(re)}, v_2^{(re)}, ..., v_n^{(re)}) \in_R \mathbb{Z}_N^n$. For each row A'_j of A', choose $r_j^{(re)} \in_R \mathbb{Z}_N$, run $(ssk^{(re)}, svk^{(re)}) \leftarrow$

$OTS.KeyGen(1^k)$ and set σ_2 as

$$svk^{(re)}, B_0^{(re)} = key \cdot e(g,g)^{\alpha s^{(re)}}, B_1^{(re)} = g^{s^{(re)}}, B_2^{(re)} = (g^{\kappa})^{s^{(re)}},$$
$$B_3^{(re)} = (\hat{g}_1^{svk^{(re)}} g^{\beta})^{s^{(re)}}, \forall j \in [1,l]\ (C_j^{(re)} = (g^a)^{A'_j v^{(re)}} H_{\rho'(j)}{}^{-r_j^{(re)}},$$
$$D_j^{(re)} = g^{r_j^{(re)}}), E^{(re)} = OTS.Sign(ssk^{(re)}, (B_0^{(re)}, B_1^{(re)}, B_3^{(re)},$$
$$\forall j \in [1,l]\ (C_j^{(re)}, D_j^{(re)}))).$$

(d) Output $C_R = (\sigma_1, \sigma_2)$ under (A', ρ').

6. **Dec**$(param, sk_S, C)$. Parse the original ciphertext C under (A, ρ) as $(svk,\ B_0,\ B_1,\ B_2,\ B_3,\ B_4,\ \forall j \in [1,l]\ (C_j,\ D_j),\ E)$, and the secret key sk_S as $(S, K, K', K'', \forall i \in S\ K_i)$. The decryption algorithm chooses a set of constants $w_j \in_R \mathbb{Z}_N$ such that $\sum_{\rho(j)\in S} w_j A_j = (1, 0, ..., 0)$, and next recovers the message as follows.
   (a) If Eq. (1) does not hold, output $\perp$. Otherwise, proceed.
   (b) Compute $e(B_1, K)e(B_2, K')^{-1}/(\prod_{\rho(j)\in S}(e(C_j, K'')e(D_j, K_{\rho(j)}))^{w_j})$ $= e(g,g)^{\alpha s}$, and output the message $m = B_0/e(g,g)^{\alpha s}$.
7. **Dec**$_R(param, sk_S, C_R)$. Parse the re-encrypted ciphertext C_R under (A', ρ') as (σ_1, σ_2), and the secret key sk_S as $(S, K, K', K'', \forall i \in S\ K_i)$.
   (a) Check the validity of σ_2 as

$$e(B_1^{(re)}, g^{\kappa}) \stackrel{?}{=} e(B_2^{(re)}, g), e(B_1^{(re)}, \hat{g}_1^{svk^{(re)}} g^{\beta}) \stackrel{?}{=} e(B_3^{(re)}, g),$$
$$e(\prod_{\rho'(j)\in S} (C_j^{(re)})^{w_j^{(re)}}, g) \stackrel{?}{=} e(B_1^{(re)}, g^a) \cdot \prod_{\rho'(j)\in S} (e((D_j^{(re)})^{-1}, H_{\rho'(j)}^{w_j^{(re)}})),$$
$$OTS.Verify(svk^{(re)}, (E^{(re)}, (B_0^{(re)}, B_1^{(re)}, B_3^{(re)},$$
$$\forall j \in [1,l]\ (C_j^{(re)}, D_j^{(re)})))) \stackrel{?}{=} 1, S \stackrel{?}{\models} (A', \rho'), \tag{2}$$

   where $w_j^{(re)}$ are chosen by the decryptor so that $\sum_{\rho'(j)\in S} w_j^{(re)} A'_j = (1, 0, ..., 0)$. If Eq. (2) does not hold, output $\perp$. Otherwise, proceed.
   (b) Compute $e(B_1^{(re)}, K)e(B_2^{(re)}, K')^{-1}/(\prod_{\rho'(j)\in S}(e(C_j^{(re)}, K'')e(D_j^{(re)},$ $K_{\rho'(j)}))^{w_j^{(re)}}) = e(g,g)^{\alpha s^{(re)}}$, and output $key = B_0^{(re)}/e(g,g)^{\alpha s^{(re)}}$.
   (c) Run $G = SYM.Dec(TCR_2(key), \sigma_1)$.
   (d) Parse G as (C, rk_6, F). If either Eq. (1) or the following verification for rk_6 does not hold, output $\perp$. Otherwise, proceed.

$$e(B_1^{(rk)}, g^{\kappa}) \stackrel{?}{=} e(B_2^{(rk)}, g), e(B_1^{(rk)}, \hat{g}_1^{svk^{(rk)}} g^{\beta}) \stackrel{?}{=} e(B_3^{(rk)}, g),$$
$$e(\prod_{\rho'(j)\in S} (C_j^{(rk)})^{w_j^{(rk)}}, g) \stackrel{?}{=} e(B_1^{(rk)}, g^a) \cdot \prod_{\rho'(j)\in S} (e((D_j^{(rk)})^{-1}, H_{\rho'(j)}^{w_j^{(rk)}})),$$
$$OTS.Verify(svk^{(rk)}, (E^{(rk)}, (B_0^{(rk)}, B_1^{(rk)}, B_3^{(rk)},$$
$$\forall j \in [1,l]\ (C_j^{(rk)}, D_j^{(rk)})))) \stackrel{?}{=} 1, S \stackrel{?}{\models} (A', \rho'), \tag{3}$$

where $w_j^{(rk)}$ are chosen by the decryptor so that $\sum_{\rho'(j)\in S} w_j^{(rk)} A'_j = (1, 0, ..., 0)$.

(e) Compute $e(B_1^{(rk)}, K)e(B_2^{(rk)}, K')^{-1}/(\prod_{\rho'(j)\in S}(e(C_j^{(rk)}, K'')e(D_j^{(rk)}, K_{\rho'(j)}))^{w_j^{(rk)}}) = e(g,g)^{\alpha s^{(rk)}}$, and then $B_0^{(rk)}/e(g,g)^{\alpha s^{(rk)}} = \delta$. Compute $F^{TCR_1(\delta)^{-1}} = e(g,g)^{\alpha s}$, and finally output $m = B_0/e(g,g)^{\alpha s}$.

3.2 Security Analysis

Theorem 1. *Suppose Assumption 1, the general subgroup decision assumption, the three party Diffie-Hellman assumption in a subgroup, and the source q-parallel BDHE assumption in a subgroup hold, SYM is a CCA-secure one-time symmetric encryption, OTS is a strongly existential unforgeable one-time signature, and TCR_1, TCR_2 are the TCR hash functions, our system is IND-CCA secure in the standard model.*

We prove our scheme by following [14]. Due to limited space, we present our construction for semi-functional ciphertexts and semi-functional keys in the full version.

We will prove Theorem 1 in a hybrid argument over a sequence of games. We let the total number of queries be $q = q_{sk}+q_{rk}+q_{re}+q_{dec}$, where $q_{sk}, q_{rk}, q_{re}, q_{dec}$ denote the number of the secret key, re-encryption key, re-encryption and decryption queries, respectively. $Game_{real}$ is the first game that is the IND-CCA security game for CP-ABPRE systems in which the challenge ciphertext (original ciphertext/re-encrypted ciphertext) is normal. Here, $\mathcal{C}$ will use normal secret keys to respond secret key extraction queries. Besides, $\mathcal{C}$ will first generate normal secret keys, and next leverage these keys to respond the re-encryption key, re-encryption and decryption queries, namely, the re-encryption keys, re-encryption results and decryption results are indirectly computed from the normal secret keys. $Game_0$ is the second game which is identical to $Game_{real}$ except that the challenge ciphertext is semi-functional.

Hereafter by "keys" (resp. "key") we mean the secret key(s) (constructed by $\mathcal{C}$) used to respond the secret key extraction, re-encryption key extraction, re-encryption and decryption queries. In the following, we will convert the "keys" to be semi-functional one by one. But for clarity we first turn the "keys" for the secret key extraction queries, and then convert the "keys" for the re-encryption key queries, the re-encryption queries and the decryption queries in sequence. Besides, $\mathcal{A}$ issues one query in each of the following games. We define $Game_i$ as follows, where $i \in [1, q]$. We let $j_\tau \in [1, q_\tau]$, where $\tau \in \{sk, rk, re, dec\}$. In $Game_{j_\tau}$ we define two sub-games $Game_{j_\tau}^N$ and $Game_{j_\tau}^T$ in which the challenge ciphertext is semi-functional. In $Game_{j_\tau}^N$ the first $(j-1)_\tau$ "keys" are semi-functional, the j_τ-th "key" is nominal semi-functional, and the rest of "keys" are normal. In $Game_{j_\tau}^T$ the first $(j-1)_\tau$ "keys" are semi-functional, the j_τ-th "key" is temporary semi-functional, and the remaining "keys" are normal.

To transform $Game_{(j-1)_\tau}$ (where j_τ-th "key" is normal) to $Game_{j_\tau}$ (where j_τ-th "key" is semi-functional) , we first convert $Game_{(j-1)_\tau}$ to $Game_{j_\tau}^N$, then

to $Game^T_{j_\tau}$, and finally to $Game_{j_\tau}$. To get from $Game^N_{j_\tau}$ to $Game^T_{j_\tau}$, we treat the simulations for the queries of Phase 1 and that of Phase 2 differently: the former is based on the three party Diffie-Hellman assumption, and the latter is based on the source group q-parallel BDHE assumption. In $Game_q = Game_{q_{dec}}$ all "keys" are semi-functional, and the challenge ciphertext is semi-functional for one of the given messages. $Game_{final}$ is the final game where all "keys" are semi-functional and the challenge ciphertext is semi-functional for a random message, independent of the two message given by $\mathcal{A}$. We will prove the above games to be indistinguishable by the following lemmas. Note we implicitly assume SYM is a CCA-secure one-time symmetric encryption, OTS is a strongly existential unforgeable one-time signature, TCR_1, TCR_2 are TCR hash functions and it is hard to find a non-trivial factor of N (for Lemma 3 and Lemma 4).

Lemma 1. *If there is an algorithm $\mathcal{A}$ such that $Game_{real}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} - Game_0Adv^{CP\text{-}ABPRE}_{\mathcal{A}} = \varphi$, we build an algorithm $\mathcal{C}$ that breaks the general subgroup decision assumption with advantage φ.*

Lemma 2. *If there is an algorithm $\mathcal{A}$ such that $Game_{(j-1)_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} - Game^N_{j_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} = \varphi$ (for any $j_\tau \in [1, q_\tau]$), we build an algorithm $\mathcal{C}$ that breaks the general subgroup decision assumption with advantage φ.*

Lemma 3. *If there is an algorithm $\mathcal{A}$ such that $Game^N_{j_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} - Game^T_{j_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} = \varphi$ for a j_τ belonging to the Phase 1 queries, we build an algorithm $\mathcal{C}$ that breaks the three party Diffie-Hellman assumption in a subgroup with advantage φ.*

Lemma 4. *If there is an algorithm $\mathcal{A}$ such that $Game^N_{j_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} - Game^T_{j_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} = \varphi$ for a j_τ belonging to the Phase 2 queries, we build an algorithm $\mathcal{C}$ that breaks the source group q-parallel BDHE assumption in a subgroup with advantage φ.*

Lemma 5. *If there is an algorithm $\mathcal{A}$ such that $Game^T_{j_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} - Game_{j_\tau}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} = \varphi$ (for any $j_\tau \in [1, q_\tau]$), we build an algorithm $\mathcal{C}$ that breaks the general subgroup decision assumption with advantage φ.*

Lemma 6. *If there is an algorithm $\mathcal{A}$ such that $Game_qAdv^{CP\text{-}ABPRE}_{\mathcal{A}} - Game_{final}Adv^{CP\text{-}ABPRE}_{\mathcal{A}} = \varphi$, we can build a reduction algorithm $\mathcal{C}$ that breaks Assumption 1 with advantage φ.*

Due to limited space, we will provide the proofs of the lemmas in the full version of this paper.

4 Conclusions

This paper defined the IND-CCA security notion for CP-ABPRE systems, and proposed the first adaptively CCA-secure CP-ABPRE scheme without loss of expressiveness on access policy by integrating the dual system encryption technology with selective proof technique. Following the proof framework introduced

by Lewko and Waters, our scheme was proved in the standard model. This paper also motivates interesting open problems, such as, converting our system in the prime order bilinear group.

References

1. Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur. 9(1), 1–30 (2006)
2. Attrapadung, N., Herranz, J., Laguillaumie, F., Libert, B., de Panafieu, E., Rafols, C.: Attribute-based encryption schemes with constant-size ciphertexts. Theoretical Computer Science 422, 15–38 (2012)
3. Bellare, M., Shoup, S.: Two-tier signatures, strongly unforgeable signatures, and fiat-shamir without random oracles. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 201–216. Springer, Heidelberg (2007)
4. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Computer Society (2007)
5. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144. Springer, Heidelberg (1998)
6. Canetti, R., Hohenberger, S.: Chosen-ciphertext secure proxy re-encryption. In: Ning, P., di Vimercati, S.D.C., Syverson, P.F. (eds.) ACM Conference on Computer and Communications Security, pp. 185–194. ACM (2007)
7. Cheung, L., Newport, C.C.: Provably secure ciphertext policy ABE. In: Ning, P., di Vimercati, S.D.C., Syverson, P.F. (eds.) ACM Conference on Computer and Communications Security, pp. 456–465. ACM (2007)
8. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. 33(1), 167–226 (2004)
9. Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attribute based encryption. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 579–591. Springer, Heidelberg (2008)
10. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Juels, A., Wright, R.N., di Vimercati, S.D.C. (eds.) ACM Conference on Computer and Communications Security, pp. 89–98. ACM (2006)
11. Hanaoka, G., Kawai, Y., Kunihiro, N., Matsuda, T., Weng, J., Zhang, R., Zhao, Y.: Generic construction of chosen ciphertext secure proxy re-encryption. In: Dunkelman, O. (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 349–364. Springer, Heidelberg (2012)
12. Isshiki, T., Nguyen, M.H., Tanaka, K.: Proxy re-encryption in a stronger security model extended from CT-RSA2012. In: Dawson, E. (ed.) CT-RSA 2013. LNCS, vol. 7779, pp. 277–292. Springer, Heidelberg (2013)
13. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010)

14. Lewko, A., Waters, B.: New proof methods for attribute-based encryption: Achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012)
15. Liang, K., Fang, L., Susilo, W., Wong, D.S.: A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. In: INCoS, pp. 552–559. IEEE (2013)
16. Liang, X., Cao, Z., Lin, H., Shao, J.: Attribute based proxy re-encryption with delegating capabilities. In: Li, W., Susilo, W., Tupakula, U.K., Safavi-Naini, R., Varadharajan, V. (eds.) ASIACCS, pp. 276–286. ACM (2009)
17. Libert, B., Vergnaud, D.: Unidirectional chosen-ciphertext secure proxy re-encryption. In: Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 360–379. Springer, Heidelberg (2008)
18. Luo, S., Hu, J., Chen, Z.: Ciphertext policy attribute-based proxy re-encryption. In: Soriano, M., Qing, S., López, J. (eds.) ICICS 2010. LNCS, vol. 6476, pp. 401–415. Springer, Heidelberg (2010)
19. Mambo, M., Okamoto, E.: Proxy cryptosystems: Delegation of the power to decrypt ciphertexts. IEICE Transactions E80-A(1), 54–63 (1997)
20. Mizuno, T., Doi, H.: Hybrid proxy re-encryption scheme for attribute-based encryption. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Inscrypt 2009. LNCS, vol. 6151, pp. 288–302. Springer, Heidelberg (2010)
21. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
22. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011)
23. Waters, B.: Functional encryption for regular languages. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 218–235. Springer, Heidelberg (2012)
24. Weng, J., Chen, M., Yang, Y., Deng, R.H., Chen, K., Bao, F.: CCA-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles. Science China Information Sciences 53(3), 593–606 (2010)
25. Weng, J., Yang, Y., Tang, Q., Deng, R.H., Bao, F.: Efficient conditional proxy re-encryption with chosen-ciphertext security. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) ISC 2009. LNCS, vol. 5735, pp. 151–166. Springer, Heidelberg (2009)
26. Weng, J., Zhao, Y., Hanaoka, G.: On the security of a bidirectional proxy re-encryption scheme from PKC 2010. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 284–295. Springer, Heidelberg (2011)

A Preliminaries

Due to limited space, we refer the reader to [14] for the definition of composite order bilinear groups, assumption 1, the general subgroup decision assumption, the three party Diffie-Hellman assumption in a subgroup, the source group q-parallel BDHE assumption in a subgroup. We here review the one-time symmetric encryption system.

One-time Symmetric Encryption. A one-time symmetric encryption [8] consists of the following algorithms. Note let $\mathcal{K}_D$ be the key space $\{0,1\}^{poly(1^k)}$, and SYM be a symmetric encryption scheme, where $poly(1^k)$ is the fixed polynomial size (bound) with respect to the security parameter k. The encryption algorithm $SYM.Enc$ intakes a key $K \in \mathcal{K}_D$ and a message M, outputs a ciphertext C. The decryption algorithm $SYM.Dec$ intakes K and C, outputs M or a symbol $\perp$. The CCA security model for SYM systems is given in [12], we hence omit the details.