11-2013

Adaptable ciphertext-policy attribute-based encryption

Junzuo LAI
Jinan University - China

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Yanjiang YANG
Institute for InfoComm Research

Jian WENG
Institute for InfoComm Research

DOI: https://doi.org/10.1007/978-3-319-04873-4_12

Adaptable Ciphertext-Policy Attribute-Based Encryption

Conference Paper · January 2014

DOI: 10.1007/978-3-319-04873-4_12

CITATIONS
12

READS
232

4 authors, including:

Robert H. Deng
Singapore Management University
475 PUBLICATIONS **8,490** CITATIONS

SEE PROFILE

Yanjiang Yang
Agency for Science, Technology and Research (A*STAR)
73 PUBLICATIONS **1,301** CITATIONS

SEE PROFILE

Jian Weng
Jinan University (Guangzhou, China)
160 PUBLICATIONS **2,078** CITATIONS

SEE PROFILE

Adaptable Ciphertext-Policy Attribute-Based Encryption

Junzuo Lai[1,2], Robert H. Deng[2], Yanjiang Yang[3], and Jian Weng[1,2]

[1] Department of Computer Science, Jinan University, China
[2] School of Information Systems, Singapore Management University, Singapore
{junzuolai,robertdeng,jianweng}@smu.edu.sg
[3] Institute for Infocomm Research, Singapore
yyang@i2r.a-star.edu.sg

Abstract. In this paper, we introduce a new cryptographic primitive, called adaptable ciphertext-policy attribute-based encryption (CP-ABE). Adaptable CP-ABE extends the traditional CP-ABE by allowing a semi-trusted proxy to modify a ciphertext under one access policy into ciphertexts of the same plaintext under *any* other access policies; the proxy, however, learns nothing about the underlying plaintext. With such "adaptability" possessed by the proxy, adaptable CP-ABE has many real world applications, such as handling policy changes in CP-ABE encryption of cloud data and outsourcing of CP-ABE encryption.

Specifically, we first specify a formal model of adaptable CP-ABE; then, based on the CP-ABE scheme by Waters, we propose a concrete adaptable CP-ABE scheme and further prove its security under our security model.

Keywords: ciphertext-policy attribute-based encryption, adaptability, policy change.

1 Introduction

Attribute-based encryption (ABE), e.g., [25,9,3], has thus far received enormous attention, due to its ability in enforcing encryption/decryption capabilities defined over descriptive attributes. Unlike standard public key encryption, where encryption is performed under a public key and the ciphertext can be decrypted by a single private key, ABE is a one-to-many public key encryption primitive, allowing data to be encrypted with certain access policy/attributes while each decryption key is associated with certain attributes/policy; only when the attributes satisfy the access policy can a key decrypt the ciphertext successfully.

Two types of ABE are distinguished in the literature: ciphertext-policy ABE (CP-ABE) such as [3], and key-policy ABE (KP-ABE) such as [9]. The difference lies in that in the former, a ciphertext is generated under an access policy (also called access structure), and decryption keys are associated with attributes; while the latter is the other way around. While it is often possible to transform one type of ABE into the other [8], CP-ABE appears more aligned with practice

Z. Cao and F. Zhang (Eds.): Pairing 2013, LNCS 8365, pp. 199–214, 2014.

where the encryptor directly specifies the access policy under which a ciphertext can be decrypted.

In reality, a user's access privileges are often granted based on the functional role he/she assumes in an organization, where a role reduces to no more than a set of attributes. In this regard, CP-ABE enables a kind of cryptographic access control over data with respect to functional roles, rather than the usual notion of individuals inherent to the standard public key encryption. Thus CP-ABE represents a practically promising encryption primitive, and it has been an active research field in the past few years. Existing research on CP-ABE in the literature generally follows several lines. For example, since the earlier CP-ABE scheme [3] can only attain security in the generic group model, one direction of research is to propose CP-ABE constructions with security under a more solid ground (e.g., in the standard model) [5]. Another line of efforts is to enable CP-ABE schemes to accommodate more expressive and complex access policies [14,27,16,6,7]. Still, there are also many attempts to pursue more privacy-wise CP-ABE or variants that hide the associated access policies, besides encryption of the payload data [22,17,12,13,11,26,23,24].

In this work, we propose yet another new variant of CP-ABE, namely *adaptable CP-ABE*. We introduce a semi-trusted party, called *proxy*, into the setting of CP-ABE. Given a *trapdoor*, the proxy is entitled to transform a ciphertext under one access policy into ciphertexts of the same plaintext under any other access policies. The proxy, however, learns nothing about the plaintext during the process of transformation. We first formulate a model for adaptable CP-ABE, and then present a concrete construction. In fact, we can use the similar method to obtain adaptable KP-ABE. Due to space limitations, we do not discuss adaptable KP-ABE in this paper.

Comparison with PRE. To better understand the concept of adaptable CP-ABE, it is conducive to outline the distinctions between adaptable CP-ABE and proxy re-encryption (PRE), or more precisely ciphertext-policy attribute-based PRE (CP-ABPRE) [19,20,18]. PRE is a public key encryption primitive also incorporating a semi-trusted proxy which is capable of converting ciphertexts (Please refer to Section 2 for more details on the concept of PRE). Particularly, in CP-ABPRE [19,20,18], the proxy given a trapdoor (called re-encryption key in PRE) issued for a set S of attributes and an access policy $\mathbb{B}$, can transform a ciphertext under access policy $\mathbb{A}$ to a ciphertext under another access policy $\mathbb{B}$, if S satisfies $\mathbb{A}$.

The major differences between our adaptable CP-ABE and CP-ABPRE [19,20,18] can be summarized as follows. First, in adaptable CP-ABE the proxy is not restricted in its ability in converting ciphertexts, in that with a single trapdoor it can transform ciphertexts under any access policies and to the ones under any other policies. In comparison, each re-encryption key held by the proxy in CP-ABPRE is bound to a set of attributes and a destination access policy, and it is applicable only to the source ciphertexts whose access policies are satisfied by the set of attributes. Second, in adaptable CP-ABE the proxy's trapdoor is generated in a "centralized" manner by a trusted authority who is responsible for

establishing system parameters. In contrast, re-encryption keys in CP-ABPRE are generated in a "distributed" manner by individual users each holding a private key associated with a set of attributes. Lastly, in CP-ABPRE, a source ciphertext and its transformed version have different formats; the transformed ciphertext usually expands in size, compared to the ciphertext in the "source format" under the same access policy. This is not the case for adaptable CP-ABE, in which no discrepancy exists between "source format" and "destination format", and thus there is no ciphertext size expansion.

1.1 Applications of Adaptable CP-ABE

Recall that, in CP-ABPRE, a proxy with a re-encryption key generated by a user, only can transform the ciphertexts whose access policies are satisfied by the user's attributes set. In some applications, the access polices associated with the ciphertexts *across many users* need to be modified; in these cases, CP-ABPRE is cumbersome to fulfill if not impossible and adaptable CP-ABE will show its capabilities. Below we give examples of applications that demonstrate the genuine applicability of adaptable CP-ABE. In view of the fact that cloud computing has been well accepted as a powerful platform for data sharing, we especially choose to consider the scenario where CP-ABE is used to encrypt the data outsourced to the cloud storage, to achieve confidentiality against the cloud.

Handling Policy Changes in CP-ABE Encryption of Cloud Data. Indeed, cloud computing enables users to outsource their data to the cloud, where massive storage capacity is available. However, a major concern over this data outsourcing paradigm is that the data owner who outsources his data (e.g., a company) may not want the cloud to see the data in cleartext. It is now basically accepted that in data critical applications, a user should only outsource encrypted data in order to ensure confidentiality against the cloud.

In practice, data accessing is often obliged to enforce fine-grained access control rules. For example, imagine that a hospital moves patient data to the cloud. Access control rules must guarantee that a patient's information is only allowed to be accessed by appropriate doctors/nurses from appropriate departments. Undoubtedly, CP-ABE is a nice tool for achieving this type of fine-grained cryptographic access control over cloud data.

In such applications where CP-ABE is used for encryption of cloud data, changes of access policies are not a rare phenomenon. For example, specifications on a new product might be only allowed access by the engineering department during the design and testing stage. As the product is ready to be launched in the market, access of the product specifications will need to be transferred from the engineering department to the marketing and sales departments. A straightforward application of CP-ABE would involve the data owner downloading the encrypted data from the cloud, decrypting it to obtain the original data, re-encrypting the data under the new access policies and uploading again. This is a daunting task if the quantity of data involved is massive.

Adaptable CP-ABE offers an effective solution by delegating the task of data re-encryption to the cloud. More specifically, the cloud is trusted as the proxy and is given the trapdoor for data transformation. As a result, the data owner simply needs to instruct the cloud to re-encrypt the data by providing the new access policies, while retaining data confidentiality against the cloud. We should point out that it is also possible to apply CP-ABPRE to accomplish the same task, but at a much higher price: for each old/new policy pair, the data owner must provide a seperate re-encryption key.

Outsourcing of CP-ABE Encryption. Consider again the above scenario of encryption of cloud data using CP-ABE, but now we focus on the situation where the data owner uses a resource-constrained device (e.g., tablet or smart phone) to do the data outsourcing. This is in accord with the current trend of growing use of such low-powered devices in our daily life. An example is that a user encrypts the photos taken with his smart phone, and uploads them to his personal account over the cloud for sharing with his friends.

We observe that in the existing CP-ABE schemes in the literature, the encryption function cannot be deemed efficient, and an encryption operation normally involves $\mathcal{O}(n)$ scalar exponentiations, where n is the number of attributes involved in the access policy. This is quite a burden for resource-limited devices. Adaptable CP-ABE would provide a good solution to this problem, inflicting fixed computation on the weak devices by delegating the majority of the computation to the cloud.

The basic idea is as follows. We first extend the original attributes of the system with an additional single-valued dummy attribute, but no one will be issued a private key corresponding to this dummy attribute. To generate the ciphertext for data to be outsourced to cloud, the data owner encrypts the data under a single-attribute access policy involving only the dummy attribute (i.e., only the dummy attribute satisfies the policy). The computation overhead for this is thus constant. The data owner then sends the ciphertext together with the intended access policy to the cloud, who then does the ciphertext conversion, generating the desired ciphertext. It goes without saying that using CP-ABPRE would require the data owner to provide a re-encryption key from the dummy attribute to each intended access policy.

1.2 Organization

This paper is organized as follows. In Section 2, we provide an overview of related work. In Section 3, some standard notations and cryptographic definitions are highlighted. In Section 4, we describe the formal model for adaptable CP-ABE, followed by a concrete construction together with its security analysis. Concluding remarks are contained in Section 5.

2 Related Work

ABE and proxy re-encryption (PRE) are of obvious relevance to our work, and we next give an overview of them, respectively.

ABE. The notion of ABE is introduced by Sahai and Waters as an application of their fuzzy identity-based encryption (IBE) scheme [25], where both ciphertexts and secrete keys are associated with sets of attributes. The decryption of a ciphertext is enabled if and only if the set of attributes for the ciphertext and the set of attributes for the secret key overlap by at least a fixed threshold value d. Goyal et al. [9] formulate two complementary forms of ABE: KP-ABE and CP-ABE. Our focus in this work is CP-ABE. In a CP-ABE scheme, decryption keys are associated with sets of attributes and ciphertexts are associated with access policies.

The first CP-ABE construction proposed by Bethencourt et al. [3] is proven secure under the generic group model. Later, Cheung and Newport [5] present a CP-ABE scheme that is secure under the standard model; however, the access policies in that scheme are restricted to be in the form of a AND combination of different attributes. Recently, secure and more expressive CP-ABE schemes [27,14,16,6,7] are proposed. In virtually all existing CP-ABE schemes, the size of a ciphertext in a CP-ABE scheme is proportional to the size of its associated access policy, and the decryption time is proportional to the number of attributes that have been used for decryption. This has motivated some work [1,10] to design CP-ABE schemes with faster decryption algorithms. Müller et al. [21] and Lewko et al. [15] led another line of research, considering CP-ABE schemes with multiple authorities, in an attempt to meet the need of a more general framework where data are shared according to policies defined over attributes or credentials issued across different trust domains and organizations.

Proxy Re-Encryption (PRE). Proxy re-encryption (PRE), first introduced in [4], involves a set of users (each holding a public/private key pair for standard public-key encryption), and a semi-trusted proxy. Let pk_A and pk_B be the public keys of Alice and Bob, respectively. The proxy is given a re-encryption key $rk_{A\to B}$ from Alice to Bob, and can transform ciphertexts under Alice's public key into ciphertexts under Bob's public key, where the procedure is intuitively depicted as $Enc(pk_A, m) \xrightarrow{rk_{A\to B}} Enc(pk_B, m)$. The proxy does not learn anything about the messages m encrypted under either key.

Later, the concept of conditional proxy re-encryption(CPRE) [28] emerged, which strengthens PRE in such a way that a ciphertext under Alice's public key is generated under a condition $\mathbb{C}$, and the re-encryption key from Alice to Bob is associated with certain properties $\mathbb{P}$ (denoted as $rk_{A\xrightarrow{\mathbb{P}}B}$). A ciphertext for Alice can be transferred to one for Bob, if and only if $\mathbb{P}$ satisfies $\mathbb{C}$. Intuitively, the procedure is $Enc(pk_A, m, \mathbb{C}) \xrightarrow{rk_{A\xrightarrow{\mathbb{P}}B}} Enc(pk_B, m)$. Most of the existing CPRE schemes such as [28,29] can only handle keyword-based conditions, where both $\mathbb{C}$ and $\mathbb{P}$ are a keyword. The scheme in [30] is an exception, and it manages to process attribute-based conditions.

To implement PRE in the attribute-based cryptographic setting, Liang et al. [19] introduce ciphertext-policy attribute-based PRE (CP-ABPRE), in which a proxy is allowed to transform a ciphertext under a source access policy into another ciphertext under a destination policy. At the mean time, CP-ABPRE has

the flavor of CPRE, in the sense that a re-encryption key is bounded with a set S of attributes as well as a destination access policy, and ciphertext transformation is *conditioned* upon the satisfaction of S to the source access policy. Liang et al. [19] propose a concrete construction of CP-ABPRE based on a CP-ABE scheme [5] in which access policy is only represented as AND gates on positive and negative attributes. Luo et al. [20] propose a CP-ABPRE scheme which supports AND gates on multi-valued and negative attributes. Recently, Liang et al. [18] present a CP-ABPRE scheme supporting any monotonic access policy.

Adaptable CP-ABE is similar to CP-ABPRE, in terms of the concept of ciphertext transformation among source/destination access policies, but they also differ in delicate ways as shown earlier. Adaptable CP-ABE has no implication of "conditional" transformation, and the trapdoor for ciphertext conversion is independent of specific attributes and access policies, and entitles to transform ciphertext under any source access policy and to any destination policy.

3 Preliminaries

If S is a set, then $s \xleftarrow{\$} S$ denotes the operation of picking an element s uniformly at random from S. Let $z \leftarrow \mathsf{A}(x, y, \ldots)$ denote the operation of running an algorithm A with inputs $(x, y, \ldots)$ and output z. A function $f(\lambda)$ is *negligible* if for every $c > 0$ there exists a λ_c such that $f(\lambda) < 1/\lambda^c$ for all $\lambda > \lambda_c$.

3.1 Access Structures

Definition 1 (Access Structure [2]). *Let $\{P_1, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1,\ldots,P_n\}}$ is monotone for $\forall B$ and C, if $B \in \mathbb{A}, B \subseteq C$, then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, \ldots, P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1,\ldots,P_n\}} \backslash \{\emptyset\}$. The sets in $\mathbb{A}$ are called authorized sets, and the sets not in $\mathbb{A}$ are called unauthorized sets.*

In our context, attributes play the role of parties and we restrict our attention to monotone access structures. It is possible to (inefficiently) realize general access structures using our techniques by treating the negation of an attribute as a separate attribute.

3.2 Linear Secret Sharing Schemes

Our construction will employ linear secret-sharing schemes. We use the definition adapted from [2].

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

1. *The shares for each party form a vector over $\mathbb{Z}_p$.*

2. *There exists a matrix* $\mathbf{A}$ *with* ℓ *rows and* n *columns called the share-generating matrix for* Π. *For all* $i = 1, \ldots, \ell$, *the* i^{th} *row of* $\mathbf{A}$ *is labeled by a party* $\rho(i)$ *(*ρ *is a function from* $\{1, \ldots, \ell\}$ *to* $\mathcal{P}$*). When we consider the column vector* $v = (s, r_2, \ldots, r_n)$, *where* $s \in \mathbb{Z}_p$ *is the secret to be shared, and* $r_2, \ldots, r_n \in \mathbb{Z}_p$ *are randomly chosen, then* $\mathbf{A}v$ *is the vector of* ℓ *shares of the secret* s *according to* Π. *The share* $(\mathbf{A}v)_i$ *belongs to party* $\rho(i)$.

It is shown in [2] that every linear secret-sharing scheme according to the above definition also enjoys the linear reconstruction property, defined as follows. Suppose that Π is an LSSS for the access structure $\mathbb{A}$. Let $S \in \mathbb{A}$ be any authorized set, and let $I \subset \{1, \ldots, \ell\}$ be defined as $I = \{i | \rho(i) \in S\}$. Then there exist constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ such that, if $\{\lambda_i\}$ are valid shares of any secret s according to Π, then $\sum_{i \in I} \omega_i \lambda_i = s$. Let A_i denotes the i^{th} row of $\mathbb{A}$, we have $\sum_{i \in I} \omega_i A_i = (1, 0, \ldots, 0)$. These constants $\{\omega_i\}$ can be found in time polynomial in the size of the share-generation matrix $\mathbf{A}$ [2]. Note that, for unauthorized sets, no such constants $\{\omega_i\}$ exist.

Boolean Formulas. Access structures might also be described in terms of monotonic boolean formulas. Using standard techniques one can convert any monotonic boolean formula into an LSSS representation. We can represent the boolean formula as an access tree. An access tree of ℓ nodes will result in an LSSS matrix of ℓ rows. We refer the reader to the appendix of [15] for a discussion on how to perform this conversion.

3.3 Bilinear Groups

Let $\mathcal{G}$ be an algorithm that takes as input a security parameter λ and outputs a tuple $(p, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative cyclic groups of prime order p, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map such that:

1. **Bilinearity:** $e(g^a, h^b) = e(g, h)^{ab}$ for all $g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$.
2. **Non-degeneracy:** $e(g, h) \neq 1$ whenever $g, h \neq 1_{\mathbb{G}}$.
3. **Computable:** efficient computability for any input pair.

We refer to the tuple $(p, \mathbb{G}, \mathbb{G}_T, e)$ as a bilinear group.

3.4 Complexity Assumption

Definition 3 (DBDH Problem). *Given a group* $\mathbb{G}$ *of prime order* p *with generator* g *and elements* $g^a, g^b, g^c \in \mathbb{G}$, $e(g, g)^z \in \mathbb{G}_T$ *where* a, b, c, z *are selected uniformly at random from* $\mathbb{Z}_p^*$. *A fair binary coin* $\beta \in \{0, 1\}$ *is flipped. If* $\beta = 1$, *it outputs the tuple* $(g, g^a, g^b, g^c, T = e(g, g)^{abc})$. *If* $\beta = 0$, *it outputs the tuple* $(g, g^a, g^b, g^c, T = e(g, g)^z)$. *The Decisional Bilinear Diffie-Hellman (DBDH) problem is to guess the value of* β.

The advantage of an adversary $\mathcal{A}$ in solving the DBDH problem is defined as

$$|\mathsf{Pr}[\mathcal{A}(g, g^a, g^b, g^c, T = e(g, g)^{abc}) = 1] - \mathsf{Pr}[\mathcal{A}(g, g^a, g^b, g^c, T = e(g, g)^z) = 1]|$$

where the probability is over the randomly chosen a, b, c, z and the random bits consumed by $\mathcal{A}$. We refer to the distribution on the left-hand size as $\mathcal{P}_{BDH}$ and the one on the right as $\mathcal{R}_{BDH}$.

Definition 4 (DBDH assumption). *We say that DBDH assumption holds if all probabilistic polynomial time (PPT) adversaries have at most a negligible advantage in solving the DBDH problem.*

4 Adaptable Ciphertext-Policy Attribute-Based Encryption

In this section, we give the formal definition of adaptable CP-ABE firstly. Then, we present the formal security model for adaptable CP-ABE. Finally, drawing on the CP-ABE scheme proposed by Waters [27], we propose a concrete construction of adaptable CP-ABE and prove that it is secure in our security model.

4.1 Formal Definition of Adaptable CP-ABE

Besides Setup, KeyGen, Encrypt and Decrypt algorithms as in a traditional CP-ABE scheme, an adaptable CP-ABE scheme also includes two additional algorithms: TrapdoorGen and PolicyAdp. The authority runs the algorithm TrapdoorGen to generate a trapdoor. Given the trapdoor, a proxy can transform a ciphertext under an access policy into another ciphertext of the same plaintext under *any* access policy using the algorithm PolicyAdp.

Formally, an adaptable CP-ABE scheme consists of the following six algorithms:

- $\mathsf{Setup}(\lambda, U)$ takes as input a security parameter λ and an attribute universe description U. It outputs the public parameters PK and a master secret key MSK. This algorithm is run by a trusted authority.
- $\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S)$ takes as input the public parameters PK, the master secret key MSK and a set of attributes S. It outputs a private key SK_S corresponding to S. This algorithm is run by a trusted authority.
- $\mathsf{TrapdoorGen}(\mathsf{PK}, \mathsf{MSK})$ takes as input the public parameters PK and the master secret key MSK. It outputs a trapdoor TK. This algorithm is run by a trusted authority and the trapdoor TK is sent to a semi-trusted proxy.
- $\mathsf{Encrypt}(\mathsf{PK}, M, \mathbb{A})$ takes as input the public parameters PK, a message M and an access structure $\mathbb{A}$. It outputs a ciphertext CT.
- $\mathsf{PolicyAdp}(\mathsf{PK}, \mathsf{TK}, CT, \mathbb{A}')$ takes as input the public parameters PK, a trapdoor TK, a ciphertext CT which contains an access policy $\mathbb{A}$, and a new access policy $\mathbb{A}'$. It outputs a new ciphertext CT' associated with the access policy $\mathbb{A}'$, without changing the underlying plaintext message of CT. This algorithm is run by a semi-trusted proxy.
- $\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, CT)$ takes as input the public parameters PK, a private key SK_S, and a ciphertext CT associated with an access policy $\mathbb{A}$. If the set S of attributes satisfies the access structure $\mathbb{A}$, then the algorithm will decrypt the ciphertext and return a message M; otherwise, it outputs $\perp$.

Let $(\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(\lambda, U)$, $\mathsf{SK}_S \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S)$, $\mathsf{TK} \leftarrow \mathsf{TrapdoorGen}(\mathsf{PK}, \mathsf{MSK})$, $CT \leftarrow \mathsf{Encrypt}(\mathsf{PK}, M, \mathbb{A})$ and $CT' \leftarrow \mathsf{PolicyAdp}(\mathsf{PK}, \mathsf{TK}, CT, \mathbb{A}')$. For correctness, we require the following to hold:

1. If the set S of attributes satisfies the access structure $\mathbb{A}$, then $M \leftarrow \mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, CT)$;
2. The distributions of CT' and $\mathsf{Encrypt}(\mathsf{PK}, M, \mathbb{A}')$ are identical.

4.2 Security Model for Adaptable CP-ABE

Given the formal definition for adaptable CP-ABE, we are now in a position to define its security specification. We consider two types of adversaries. Type 1 adversaries who are allowed to query for any private keys that cannot be used to decrypt the challenge ciphertext, model adversaries in a traditional CP-ABE scheme. We also want to consider Type 2 adversaries who are equipped with a transformation trapdoor, in order to model security against an eavesdropping proxy. We assume that the proxy in an adaptable CP-ABE scheme is semi-trusted. That is to say, the proxy does not collude with any user. Thus, Type 2 adversaries are not allowed to query for any private keys.

We now give the security model against Type 1 adversaries for adaptable CP-ABE, described as a security game between a challenger and a Type 1 adversary. The game proceeds as follows:

Setup. The challenger runs Setup to obtain the public parameters PK and a master secret key MSK. It gives the public parameters PK to the adversary and keeps MSK to itself.

Query Phase 1. The adversary adaptively queries the challenger for secret keys corresponding to sets of attributes $S_1, \ldots, S_q$. In response, the challenger runs $\mathsf{SK}_{S_i} \leftarrow \mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S_i)$ and gives the secret key SK_{S_i} to the adversary, for $1 \leq i \leq q$.

Challenge. The adversary submits two (equal length) messages M_0, M_1 and an access structures $\mathbb{A}$, subject to the restriction that $\mathbb{A}$ cannot be satisfied by any of the queried sets of attributes in Query phase 1. The challenger selects a random bit $\beta \in \{0, 1\}$, sets $CT = \mathsf{Encrypt}(\mathsf{PK}, M_\beta, \mathbb{A})$ and sends CT to the adversary as the challenge ciphertext.

Query Phase 2. The adversary continues to adaptively query the challenger for secret keys corresponding to sets of attributes with the restriction that none of these satisfies $\mathbb{A}$.

Guess. The adversary outputs its guess $\beta' \in \{0, 1\}$ for β.

The advantage of the Type 1 adversary in this game is defined as $|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}|$ where the probability is taken over the random bits used by the challenger and the Type 1 adversary.

Note that, a Type 1 adversary of adaptable CP-ABE can see the transformed ciphertexts CT' of the challenge ciphertext $CT \leftarrow \mathsf{Encrypt}(\mathsf{PK}, M_\beta, \mathbb{A})$. The challenger does not provide the information for the adversary in the above game, since CT' does not leak any additional information about M_β.

We give a brief explanation. One can easily prove that, if $C \leftarrow \mathsf{Encrypt}(\mathsf{PK}, M, \mathbb{A}), C' \leftarrow \mathsf{Encrypt}(\mathsf{PK}, M, \mathbb{A}')$ are the ciphertexts of a secure CP-ABE, then given $C \| C'$ simultaneously, the adversary also can not obtain any information about M. On the other hand, adaptable CP-ABE requires that the distributions of CT' and $\mathsf{Encrypt}(\mathsf{PK}, M_\beta, \mathbb{A}')$ should be identical, hence CT' does not leak any additional information about M_β.

Definition 5. *An adaptable CP-ABE scheme is secure against Type 1 adversaries if all PPT adversaries have at most a negligible advantage in the above game.*

We say that an adaptable CP-ABE scheme is *selectively* secure against Type 1 adversaries if we add an **Init** stage before **Setup** where the adversary commits to the challenge access structure $\mathbb{A}$.

The security model against Type 2 adversaries for adaptable CP-ABE is also described as a security game between a challenger and a Type 2 adversary. The game proceeds as follows:

Setup. The challenger runs Setup to generate a public parameters/master secret key pair (PK, MSK) firstly. Then, it runs $\mathsf{TrapdoorGen}(\mathsf{PK},\mathsf{MSK})$ to obtain a trapdoor TK. Finally, it sends (PK, TK) to the adversary and keeps MSK to itself.

Challenge. The adversary submits two (equal length) messages M_0, M_1 and an access structures $\mathbb{A}$. The challenger selects a random bit $\beta \in \{0, 1\}$, sets $CT = \mathsf{Encrypt}(\mathsf{PK}, M_\beta, \mathbb{A})$ and sends CT to the adversary as the challenge ciphertext.

Guess. The adversary outputs its guess $\beta' \in \{0, 1\}$ for β.

The advantage of the Type 2 adversary in this game is defined as $|\mathsf{Pr}[\beta = \beta'] - \frac{1}{2}|$ where the probability is taken over the random bits used by the challenger and the Type 2 adversary.

Definition 6. *An adaptable CP-ABE scheme is secure against Type 2 adversaries if all PPT adversaries have at most a negligible advantage in the above game.*

4.3 Proposed Adaptable CP-ABE Scheme

Based on the CP-ABE scheme proposed by Waters [27], we propose a concrete construction of adaptable CP-ABE scheme. Inheriting from the underlying Waters CP-ABE scheme [27], our proposed adaptable CP-ABE is only *selectively* secure against Type 1 adversaries and the size of the public parameters is linear in the number of attributes in the universe.

Recently, the first CP-ABE scheme that achieved full security was proposed by Lewko et al. [14]. Since the underlying structure of the CP-ABE scheme presented by Lewko et al. [14] is almost identical to the underlying Waters CP-ABE scheme [27] we use, one can adapt our construction techniques to the

CP-ABE scheme proposed in [14] to achieve a new adaptable CP-ABE scheme, which is (*fully*) secure against Type 1 adversaries. On the other hand, it is also possible to adapt our techniques to obtain a large universe construction. In a large universe construction, we could use all elements of $\mathbb{Z}_p$ as attributes. To obtain a large universe construction, we could replace the group elements h_i associated with attribute i with a function $h : \mathbb{Z}_p \to \mathbb{G}$ based on a polynomial, as shown in [27].

Concretely, the proposed adaptable CP-ABE scheme is as follows:

$\mathsf{Setup}(\lambda, U)$ The setup algorithm takes as input a security parameter λ and a small universe description $U = \{1, 2, \ldots, |U|\}$. It first runs $\mathcal{G}(\lambda)$ to obtain a bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of prime order p. It then chooses $g, h_1, \ldots, h_{|U|} \in \mathbb{G}$, and $\alpha, \beta \in \mathbb{Z}_p$ uniformly at random. The public parameters are published as $\mathsf{PK} = (\mathbb{G}, \mathbb{G}_T, e, g, g^\beta, e(g,g)^\alpha, h_1, \ldots, h_{|U|})$. The master secret key is $\mathsf{MSK} = (\alpha, \beta)$.

$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, S)$ The key generation algorithm takes as input the public parameters, the master secret key and a set S of attributes. The algorithm first randomly picks $t \in \mathbb{Z}_p$. Then, the secret key $\mathsf{SK}_S = (S,\ K, K_0, K_i)$ is computed as $K = g^\alpha g^{\beta t},\ K_0 = g^t,\ K_i = h_i^t\ \forall i \in S$.

$\mathsf{TrapdoorGen}(\mathsf{PK}, \mathsf{MSK} = (\alpha, \beta))$ The trapdoor generation algorithm takes as input the public parameters and the master secret key. It creates the trapdoor as $\mathsf{TK} = \beta$.

$\mathsf{Encrypt}(\mathsf{PK}, M \in \mathbb{G}_T, \mathbb{A})$ The encryption algorithm takes as input the public parameters PK, a message $M \in \mathbb{G}_T$ to encrypt and an LSSS access structure $\mathbb{A} = (\mathbf{A}, \rho)$, where $\mathbf{A}$ is an $\ell \times n$ matrix and ρ is a map from each row A_i of $\mathbf{A}$ to an attribute $\rho(i)$.

The algorithm first chooses a random vector $\boldsymbol{v} = (s, v_2, \ldots, v_n) \in \mathbb{Z}_p^n$. These values will be used to share the encryption exponent s. Then, for each row A_i of $\mathbf{A}$, it chooses $r_i \in \mathbb{Z}_p$ uniformly at random. The ciphertext is $CT = ((\mathbf{A}, \rho),\ C, C', C_i, D_i)$, where $C = M \cdot e(g,g)^{\alpha s},\ C' = g^s,\ C_i = g^{\beta A_i \cdot \boldsymbol{v}} h_{\rho(i)}^{-r_i},\ D_i = g^{r_i}\ \forall i \in \{1, 2, \ldots, \ell\}$.

$\mathsf{PolicyAdp}(\mathsf{PK}, \mathsf{TK} = \beta, CT, \mathbb{A}' = (\mathbf{A}', \rho'))$ The policy adaptation algorithm takes as input the public parameters PK, the trapdoor TK, a ciphertext $CT = (\mathbb{A} = (\mathbf{A}, \rho),\ C, C', C_i, D_i)$ and an access structure $\mathbb{A}' = (\mathbf{A}', \rho')$. With the help of the trapdoor TK, this algorithm transforms the ciphertext CT into a ciphertext CT' associated with the access structure $\mathbb{A}' = (\mathbf{A}', \rho')$, without changing the underlying message of CT.

Let $CT = ((\mathbf{A}, \rho),\ C = M \cdot e(g,g)^{\alpha s},\ C' = g^s,\ C_i = g^{\beta A_i \cdot \boldsymbol{v}} h_{\rho(i)}^{-r_i},\ D_i = g^{r_i}\ \forall i \in \{1, 2, \ldots, \ell\})$, where $\mathbf{A}$ is an $\ell \times n$ matrix and $\boldsymbol{v} = (s, v_2, \ldots, v_n) \in \mathbb{Z}_p^n$ is a random vector.

Let $\mathbf{A}'$ be an $\ell' \times n'$ matrix. The algorithm proceeds as follows. First choose a random vector $\tilde{\boldsymbol{v}} = (\tilde{s}, \tilde{v}_2, \ldots, \tilde{v}_{n'}) \in \mathbb{Z}_p^{n'}$. Then, for each row A'_i of $\mathbf{A}'$, choose $r'_i \in \mathbb{Z}_p$ uniformly at random. Let $\boldsymbol{v'} = (s', \tilde{v}_2, \ldots, \tilde{v}_{n'})$, where

$s' = s + \tilde{s}$. The new ciphertext $CT' = ((\mathbf{A}', \rho'), \tilde{C}, \tilde{C}', \tilde{C}_i, \tilde{D}_i)$ is computed as

$$\begin{aligned} CT' = ((\mathbf{A}', \rho'),\ \tilde{C} &= C \cdot (e(g,g)^{\alpha})^{\tilde{s}} = M \cdot e(g,g)^{\alpha s'}, \\ \tilde{C}' &= C' \cdot g^{\tilde{s}} = g^{s+\tilde{s}} = g^{s'}, \\ \forall i \in \{1, 2, \ldots, \ell'\} &: \tilde{C}_i = g^{\beta A'_i \cdot \boldsymbol{v}'} h_{\rho'(i)}^{-r'_i},\ \tilde{D}_i = g^{r'_i}). \end{aligned}$$

It can see that the distribution of CT' is the same as that generated directly from $\mathsf{Encrypt}(\mathsf{PK}, M, \mathbb{A}' = (\mathbf{A}', \rho'))$.

Comment: Note that, although s is unknown, we show how exactly $\tilde{C}_i$ are computed. Let the row vector $A'_i = (a_{i,1}, \ldots, a_{i,n'})$. Then,

$$\begin{aligned} g^{\beta A'_i \cdot \boldsymbol{v}'} &= g^{\beta(a_{i,1}s' + a_{i,2}\tilde{v}_2 + \cdots + a_{i,n'}\tilde{v}_{n'})} \\ &= (g^{s'})^{\beta a_{i,1}} \cdot g^{\beta(a_{i,2}\tilde{v}_2 + \cdots + a_{i,n'}\tilde{v}_{n'})} = (\tilde{C}')^{\beta a_{i,1}} \cdot g^{\beta(a_{i,2}\tilde{v}_2 + \cdots + a_{i,n'}\tilde{v}_{n'})}. \end{aligned}$$

Thus, $\tilde{C}_i$ can be computed from β, $\tilde{C}'$, the LSSS access structure $\mathbb{A}' = (\mathbf{A}', \rho')$, the randomness $\tilde{v}_2, \ldots, \tilde{v}_{n'}$ and r'_i, and the public parameters.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_S, CT)$ The decryption algorithm takes as input the public parameters PK, a private key $\mathsf{SK}_S = (S,\ K,\ K_0, K_i)$ for a set of attributes S and a ciphertext $CT = ((\mathbf{A}, \rho),\ C, C', C_i, D_i)$ for an access structure $\mathbb{A} = (\mathbf{A}, \rho)$, where $\mathbf{A}$ is an $\ell \times n$ matrix. If S does not satisfy the access structure $\mathbb{A}$, it outputs $\perp$. Suppose that S satisfies the access structure $\mathbb{A}$ and let $I \subset \{1, 2, \ldots, \ell\}$ be defined as $I = \{i : \rho(i) \in S\}$. It computes constant $\omega_i \in \mathbb{Z}_p$ such that $\sum_{i \in I} \omega_i A_i = (1, 0, \ldots, 0)$.

The decryption algorithm first computes:

$$\frac{e(C', K)}{\prod_{i \in I}(e(C_i, K_0) \cdot e(K_{\rho(i)}, D_i))^{\omega_i}} = \frac{e(g,g)^{\alpha s} e(g,g)^{\beta t s}}{\prod_{i \in I} e(g,g)^{\beta t A_i \cdot \boldsymbol{v} \cdot \omega_i}} = e(g,g)^{\alpha s}.$$

The decryption algorithm can then divide out this value from C and obtain the message M.

Obviously, the above scheme satisfies the correctness of adaptable CP-ABE. We now state the security theorems of our adaptable CP-ABE scheme.

Theorem 1. *If the CP-ABE scheme proposed in [27] is selectively secure, then our proposed adaptable CP-ABE scheme is selectively secure against Type 1 adversaries.*

Proof. Recall that, Type 1 adversaries in an adaptable CP-ABE scheme, which model adversaries in a traditional CP-ABE scheme, are allowed to possess any private keys that cannot be used to decrypt the challenge ciphertext. Observe that, the algorithms Setup, KeyGen, $\mathsf{Encrypt}$ and $\mathsf{Decrypt}$ constitute a traditional CP-ABE scheme, and the scheme is same as the CP-ABE scheme proposed by Waters [27]. Since Waters [27] has proved that the CP-ABE scheme is selectively secure, thus, our proposed adaptable CP-ABE scheme is also selectively secure against Type 1 adversaries. □

Theorem 2. *If DBDH assumption holds, then our proposed adaptable CP-ABE is secure against Type 2 adversaries.*

Proof. Suppose there exists a Type 2 adversary $\mathcal{A}$ against our proposed adaptable CP-ABE scheme with non-negligible advantage. We are going to construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the DBDH problem with non-negligible probability.

$\mathcal{B}$ is given as input a random 5-tuple (g, g^a, g^b, g^c, T) that is either sampled from $\mathcal{P}_{BDH}$ (where $T = e(g,g)^{abc}$) or from $\mathcal{R}_{BDH}$ (where T is uniform and independent in $\mathbb{G}_T$). Algorithm $\mathcal{B}$'s goal is to output 1 if $T = e(g,g)^{abc}$ and 0 otherwise. Algorithm $\mathcal{B}$, playing the role of challenger, runs $\mathcal{A}$ executing the following steps.

Setup. $\mathcal{B}$ chooses random exponents $\beta, \gamma_1, \ldots, \gamma_{|U|} \in \mathbb{Z}_p^*$. The public parameters $\mathsf{PK} = (\mathbb{G}, g, g^\beta, e(g^a, g^b), h_1 = g^{\gamma_1}, \ldots, h_{|U|} = g^{\gamma_{|U|}})$ and the trapdoor $\mathsf{TK} = \beta$ are passed to $\mathcal{A}$. It sets $\alpha = ab$ implicitly, which is unknown to $\mathcal{B}$.

Challenge. The adversary $\mathcal{A}$ outputs two equal-length messages (M_0, M_1) and an access structure $\mathbb{A} = (\mathbf{A}, \rho)$, where $\mathbf{A}$ is an $\ell \times n$ matrix and ρ is a map from each row A_i of $\mathbf{A}$ to an attribute $\rho(i)$.

$\mathcal{B}$ flips a fair coin $\sigma \in \{0,1\}$ firstly. Then, for each row A_i of $\mathbf{A}$, $\mathcal{B}$ chooses $r_i \in \mathbb{Z}_p$ uniformly at random. $\mathcal{B}$ also chooses random $v_2, \ldots, v_n \in \mathbb{Z}_p$ and sets $\boldsymbol{v} = (c, v_2, \ldots, v_n)$. $\mathcal{B}$ computes the ciphertext CT as $((\mathbf{A}, \rho), C = M_\beta \cdot T,\ C' = g^c,\ C_i = g^{\beta A_i \cdot \boldsymbol{v}} h_{\rho(i)}^{-r_i},\ D_i = g^{r_i}\ \forall i \in \{1, 2, \ldots, \ell\})$, Note that, although c is unknown to $\mathcal{B}$, it can compute C_i from g^c, β, the LSSS access structure $\mathbb{A} = (\mathbf{A}, \rho)$, the randomness $v_2, \ldots, v_n$ and r_i, and the public parameters, as in the $\mathsf{PolicyAdp}$ algorithm.

Finally, $\mathcal{B}$ sets CT as the challenge ciphertext and sends it to $\mathcal{A}$. Obviously, the challenge ciphertext is a valid encryption of M_β with the correct distribution whenever $T = e(g,g)^{abc} = e(g^a, g^b)^c = e(g,g)^{\alpha c}$ (as is the case when the input 5-tuple is sampled from $\mathcal{P}_{BDH}$). On the other hand, when T is uniform and independent in $\mathbb{G}_T$ (which occurs when the input 5-tuple is sampled from $\mathcal{R}_{BDH}$) the challenge ciphertext CT is independent of σ in the adversary's view.

Guess. The adversary $\mathcal{A}$ outputs a bit σ'. If $\sigma' = \sigma$ then $\mathcal{B}$ outputs 1 meaning $T = e(g,g)^{abc}$. Otherwise, it outputs 0 meaning $T \neq e(g,g)^{abc}$.

Observe that, when the input 5-tuple is sampled from $\mathcal{P}_{BDH}$ (where $T = e(g,g)^{abc}$) then $\mathcal{A}$'s view is identical to its view in a real attack game. On the other hand, when the input 5-tuple is sampled from $\mathcal{R}_{BDH}$ (where T is uniform in $\mathbb{G}_T$) then the value of σ is information-theoretically hidden from the adversary $\mathcal{A}$. Thus, if $\mathcal{A}$ breaks our proposed adaptable CP-ABE scheme with non-negligible advantage, then $\mathcal{B}$ will solve the DBDH problem with non-negligible probability. □

5 Conclusions

In this paper, we introduced a new cryptographic primitive, called adaptable CP-ABE, which enables a *semi-trusted* proxy, given a trapdoor, to transform

a ciphertext under one access policy into ciphertexts under any other access policies. We showed that adaptable CP-ABE has many interesting real world applications. We gave the formal model of adaptable CP-ABE and proposed a concrete construction.

In our construction, since a proxy with the trapdoor can transform a ciphertext under one access policy into ciphertexts under *any* other access policies, then the proxy colluding with *any* user can decrypt all ciphertexts in the system. Hence, we require that the proxy should be *semi-trusted*, i.e., it does not collude with any user in the system. On the one hand, the assumption that a proxy is semi-trusted is reasonable and is used in many related works, such as PREs. On the other hand, a future research direction is to construct adaptable CP-ABE schemes, where the "adaptability" capability of the semi-trusted proxy could be controlled *flexibly*, called controlled adaptable CP-ABE. In a controlled adaptable CP-ABE, the semi-trusted proxy with a trapdoor only can transform a ciphertext associated with an access policy $\mathbb{A}_1 \in \mathcal{AS}_1$ into a ciphertext of the same plaintext under the access policy $\mathbb{A}_2 \in \mathcal{AS}_2$, where the access policies sets $\mathcal{AS}_1, \mathcal{AS}_2$ are specified by the trusted authority who setups the system and generates the trapdoor. Our proposed scheme can be viewed as of a special case of controlled adaptable CP-ABE, where $\mathcal{AS}_1, \mathcal{AS}_2$ are the sets of *all* access polices. Observe that, since the authority also can generate the re-encryption keys which is generated by the users in CP-ABPRE, one can easily construct a special case of controlled adaptable CP-ABE, which has the same functionality of CP-ABPRE.

Acknowledgment. The research effort of Robert H. Deng was funded through a research grant 13-C220-SMU-005 from Singapore MOE's AcRF Tier 1 funding support through Singapore Management University. The work of Junzuo Lai was supported by the National Natural Science Foundation of China (Nos. 61300226, 61272534, 61272453), the Research Fund for the Doctoral Program of Higher Education of China (No. 20134401120017), the Guangdong Provincial Natural Science Foundation (No. S2013040014826), and the Fundamental Research Funds for the Central Universities. The work of Jian Weng was supported by the National Natural Science Foundation of China under Grant Nos. 61272413, 61005049, 61373158, 61133014, 61070249, 61272415, the Fok Ying Tung Education Foundation under Grant No. 131066, the Program for New Century Excellent Talents in University under Grant No. NCET-12-0680, the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security under Grand No. AGK2011003, and the R&D Foundation of Shenzhen Basic Research Project under Grant No. JC201105170617A.

References

1. Attrapadung, N., Herranz, J., Laguillaumie, F., Libert, B., de Panafieu, E., Ràfols, C.: Attribute-based encryption schemes with constant-size ciphertexts. Theor. Comput. Sci. 422, 15–38 (2012)

2. Beimel, A.: Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology (1996)
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334 (2007)
4. 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)
5. Cheung, L., Newport, C.C.: Provably secure ciphertext policy ABE. In: ACM Conference on Computer and Communications Security, pp. 456–465 (2007)
6. Garg, S., Gentry, C., Halevi, S., Sahai, A., Waters, B.: Attribute-based encryption for circuits from multilinear maps. IACR Cryptology ePrint Archive, 2013:128 (2013)
7. Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: STOC, pp. 545–554 (2013)
8. 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)
9. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communications Security, pp. 89–98 (2006)
10. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 162–179. Springer, Heidelberg (2013)
11. Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)
12. Lai, J., Deng, R.H., Li, Y.: Fully secure cipertext-policy hiding CP-ABE. In: Bao, F., Weng, J. (eds.) ISPEC 2011. LNCS, vol. 6672, pp. 24–39. Springer, Heidelberg (2011)
13. Lai, J., Deng, R.H., Li, Y.: Expressive cp-abe with partially hidden access structures. In: ASIACCS, pp. 18–19 (2012)
14. 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)
15. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011)
16. 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)
17. Li, J., Ren, K., Zhu, B., Wan, Z.: Privacy-aware attribute-based encryption with user accountability. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) ISC 2009. LNCS, vol. 5735, pp. 347–362. Springer, Heidelberg (2009)
18. Liang, K., Fang, L., Wong, D.S., Susilo, W.: A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. IACR Cryptology ePrint Archive, 2013:236 (2013)
19. Liang, X., Cao, Z., Lin, H., Shao, J.: Attribute-based proxy re-encrytpion with delegating capabilities. In: ACM ASIACCS, pp. 276–286 (2009)

20. 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)
21. Müller, S., Katzenbeisser, S., Eckert, C.: Distributed attribute-based encryption. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 20–36. Springer, Heidelberg (2009)
22. Nishide, T., Yoneyama, K., Ohta, K.: Attribute-based encryption with partially hidden encryptor-specified access structures. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 111–129. Springer, Heidelberg (2008)
23. Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009)
24. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010)
25. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
26. Shen, E., Shi, E., Waters, B.: Predicate privacy in encryption systems. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 457–473. Springer, Heidelberg (2009)
27. 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)
28. Weng, J., Deng, R.H., Ding, X., Chu, C.K., Lai, J.: Conditional proxy re-encryption secure against chosen-ciphertext attack. In: ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009, pp. 322–332 (2009)
29. 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)
30. Zhao, J., Feng, D., Zhang, Z.: Attribute-based conditional proxy re-encryption with chosen-ciphertext security. In: IEEE GLOBECOM 2010, pp. 1–6 (2010)