2018

Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes

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

Guomin Yang
University of Wollongong, gyang@uow.edu.au

Fuchun Guo
University of Wollongong, fuchun@uow.edu.au

Qiong Huang
South China Agricultural University, csqhuang@alumni.cityu.edu.hk

Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes

Abstract

Attribute-based encryption (ABE) is an augmentation of public key encryption that allows users to encrypt and decrypt messages based on users' attributes. In a (t, s) threshold ABE, users who can decrypt a ciphertext must hold at least t attributes among the s attributes specified by the encryptor. At PKC 2010, Herranz, Laguillaumie and Ràfols proposed the first threshold ABE with constant-size ciphertexts. In order to ensure the encryptor can flexibly select the attribute set and a threshold value, they use dummy attributes to satisfy the decryption requirement. The advantage of their scheme is that any addition or removal of the attributes will not require any change to users' private keys or public parameters. Unfortunately, the need for dummy attributes makes their scheme inefficient, since the computational cost of encryption is linear to the size of selected attribute set and dummy attribute set. In this work, we improve Herranz et al.'s work, and propose a new threshold ABE scheme which does not use any dummy attribute . Our scheme not only retains the nice feature of Herranz et al.'s scheme, but also offers two improvements in comparison to the previous work. Firstly, the computational costs of encryption and decryption are only linear in the size of the selected attribute set. Secondly, without any dummy attribute, most of the computations can be conducted without the knowledge of the threshold t . Hence, threshold change in the encryption phase does not require complete recomputation of the ciphertext.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Susilo, W., Yang, G., Guo, F. & Huang, Q. (2018). Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes. Information Sciences, 429 349-360.

Constant-Size Ciphertexts in Threshold Attribute-Based Encryption without Dummy Attributes

Willy Susilo[a], Guomin Yang[a], Fuchun Guo[a], Qiong Huang[b]

[a] *School of Computing and Information Technology*
University of Wollongong, NSW 2500, Australia
[b] *College of Mathematics and Informatics*
South China Agricultural University, China

Abstract

Attribute-based encryption (ABE) is an augmentation of public key encryption that allows users to encrypt and decrypt messages based on users' attributes. In a (t, s) threshold ABE, users who can decrypt a ciphertext must hold at least t attributes among the s attributes specified by the encryptor. At PKC 2010, Herranz, Laguillaumie and Ràfols proposed the first threshold ABE with constant-size ciphertexts. In order to ensure the encryptor can flexibly select the attribute set and a threshold value, they use dummy attributes to satisfy the decryption requirement. The advantage of their scheme is that any addition or removal of the attributes will not require any change to users' private keys or public parameters. Unfortunately, the need for dummy attributes makes their scheme inefficient, since the computational cost of encryption is linear to the size of selected attribute set and dummy attribute set. In this work, we improve Herranz et al.'s work, and propose a new threshold ABE scheme which *does not use any dummy attribute*. Our scheme not only retains the nice feature of Herranz et al.'s scheme, but also offers two improvements in comparison to the previous work. Firstly, the computational costs of encryption and decryption are only linear in the size of the selected attribute set. Secondly, without any dummy attribute, most of the computations can be conducted without the knowledge of the threshold t. Hence, threshold change in the encryption phase does not require complete recomputation of the ciphertext.

Keywords: threshold attribute-based encryption, constant size, dummy attributes, provable security

1. Introduction

As an extension of public key encryption, Attribute-based encryption (ABE) [24, 15, 3] has been an active area of research recently, since it supports fine-grained access control of the encrypted data. ABE allows users to encrypt and decrypt messages based on user attributes. It is useful in providing anonymous access control, which is a desirable property in many applications, such as encrypted storage in distributed environments. In ciphertext-policy ABE (CP-ABE), a user's private key is generated by the central authority according to his/her attributes. When someone encrypts a message, it selects a policy indicating what attributes the decryptor should hold. Unfortunately, this fascinating functionality comes at a cost. In a typical implementation, the size of a ciphertext is usually proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption.

The first CP-ABE scheme with constant-size ciphertexts under AND-gate access structure was proposed in [7]. Subsequently, Herranz, Laguillaumie and Ràfols [16][1] presented the first threshold ABE scheme with constant-size ciphertexts, which supports a more expressive access structure compared to [7]. Their construction works for the (t, s) threshold case, in which a user who is authorized to decrypt should hold at least t attributes among the s attributes selected by the encryptor. Due to the ability of the encryptor to select any threshold value t and attribute set during the encryption phase, their scheme is practical. Their scheme is inspired by the technique introduced by Delerablée and Pointcheval [9] in achieiving dynamic threshold identity-based encryption. Herranz et al.'s scheme is proven secure in the standard model based on the hardness of the augmented multi-sequence of exponents decisional Diffie-Hellman (aMSE-DDH) problem [16].

1.1. Motivation

The technique used by Delerablée and Pointcheval [9] is to incorporate some "dummy information" (or, *dummy users* in their identity-based encryption scheme [9]) as part of the computation in order to satisfy the decryption requirement. This technique was then used to construct threshold ABE in [16]. However, the incorporation of dummy attributes in [16] brings efficiency loss in both encryption and decryption, linear in the size of selected attribute

[1]The expanded version of this paper appeared in [1].

set and dummy attribute set. To illustrate the efficiency lost, consider the following parameters used in [16]. Let s be the number of attributes in the chosen attribute set S, t be the threshold and m be the upper bound of the number of attributes in S. The costs for encryption and decryption in [16] are mainly dominated by $m+t+1$ exponentiations and $O(t^2+m)$ exponentiations, respectively. It means, with the choice of small parameters in s and t, we will still require a large computation effort, since m is typically large.

One of the possible application scenarios is the case which usually appears in a Massively Multiplayer Online Game (MMOG). As shown in [25], the recent global epic combat strategy mobile game Clash-of-Clans®[2] is an example of such games which will require an access control mechanism as described in this paper. In this game, each player has multiple attributes which will elevate after gaining more experience in the gameplay. The attributes are the possible *features* in the game, such as {"dragon", "canon", "bomb", $\cdots$}. There is a large set of possible features that a player can acquire during the game, as the set of the possible features is very large. If a player acquires a new feature in the game, it means that this feature has been *authorized* by the central server, otherwise people can just simply cheat by creating the new feature themselves. Occasionally, the central server would like to broadcast a special feature (such as an advanced *weapon* in this game), which will only be available to people who have gained a particular level, which is measured by the number of *features* that this player has acquired. This "offer" will be broadcast to all players, but only players that satisfy the requirement can read this broadcast message. Therefore, this message needs to be sent in an encrypted form. Only players who have satisfied some certain level can decrypt this broadcast message. This certain level is determined by a minimum number of attributes that this player has, and hence, the notion of *threshold* requirement of attributes, t. Referring to the notation that was introduced earlier, the number of possible attributes, S, is typically very large, but a player only has a subset of this set, which is referred to as s. As an example, the set $S = \{$"dragon", "snake", "canon", "bomb", "air trap", $\cdots\}$, where typically the total maximum available in S (which is m in the above notation) are around 10,000 features in a single game. A user who has played for a reasonable amount of time will gain approximately 100 features, and hence $s = 100$. If the threshold t is set to something like 30, then a user who holds

[2]http://www.supercell.net/games/view/clash-of-clans

at least 30 out of the possible features will be able to decrypt the broadcast ciphertext. Nevertheless, if the scheme in [16] is used, then each eligible user will still have to conduct a large computation, since m is large. This will make the scheme impractical, especially in the case where the application will be run in a mobile device. We note that in other scenarios, it would be typical to have a large m as well, even the value of s is small.

Although Herranz et al.'s scheme [16] is not very computationally efficient, their construction enjoys a nice feature. Namely, any addition or removal of the attributes will not require any change to users' private keys or public parameters. We note that there are some subsequent works that achieve threshold ABE but do not have this feature. These works will be reviewed in the related work.

1.2. Summary of Our Contributions

The contributions of this paper are twofold:

- We improve Herranz et al.'s work and propose a threshold ABE scheme which achieves constant-size ciphertexts *without using dummy attributes*. Let s be the number of attributes in the chosen attribute set S, t be the corresponding threshold and m be the upper bound of the number of attributes in S. Compared to our scheme, the major computational cost of encryption of Herranz et al.'s scheme includes $m + t + 1$ exponentiations whereas ours requires only $s + 3$ exponentiations, and the major computational cost of decryption of Herranz et al.'s scheme includes $O(t^2 + m)$ exponentiations, but ours only needs $O(t^s + s)$ exponentiations.

- Another fascinating feature of our scheme is that it supports an efficient threshold change during the encryption process. The impact of using dummy attributes is that the threshold t must be known in the beginning of the encryption process, as this value determines how the ciphertext is being formed. While in our scheme, the value of t only affects one or two operations during the encryption, but not the overall computation, and therefore, the encryptor can change the threshold t without having to recompute the overall ciphertext.

1.3. Technical Contributions

In the following we describe an overview of our technique. Following [16], let A be the set of attributes held by a user, and S be the set of attributes

specified by the encryptor. Let $A_S = A \cap S$ and $F(\gamma)$ be the polynomial defined as

$$F(\gamma) = \frac{\prod_{\mathsf{at} \in S}(\gamma + \tau(\mathsf{at})) \prod_{d \in \mathcal{D}_{m+t-1-s}}(\gamma + d)}{\prod_{\mathsf{at} \in A_S}(\gamma + \tau(\mathsf{at}))},$$

which has degree $m+t-1-|A_S|$. Here, $|A_S|$ denotes the number of attributes in A_S and $\mathcal{D}_{m+t-1-s}$ denotes a dummy attribute set with $m+t-1-s$ dummy attributes.

Given the ciphertext, any user (whose $A_S \neq \emptyset$) can compute

$$e(g^{\alpha}, h)^{-\kappa} e(g^{\alpha}, h)^{r\kappa}, \quad \forall i \in [1, m-1], e(g^{\alpha}, \ h)^{r\kappa\gamma^i} \ \text{ and } \ e(g^{\alpha}, h)^{r\kappa F(\gamma)}.$$

According to the setting, all redundant group elements $e(g^{\alpha}, h)^{r\kappa\gamma^i}$ must be removed in order to extract the encryption key $e(g^{\alpha}, h)^{-\kappa}$ from $e(g^{\alpha}, h)^{r\kappa F(\gamma)}$. Therefore, the user will successfully decrypt the ciphertext if and only if $F(\gamma)$ is of degree $m-1$ at most, which requires $|A_S| \geq t$. If dummy attributes are not embedded in $F(\gamma)$, the degree of $F(\gamma)$ will be always less than $m-1$, such that the user can decrypt the ciphertext even its attribute number does not satisfy the threshold requirement.

We notice that the required degree of $F(\gamma)$ in the construction is mainly dominated by group elements $e(g^{\alpha}, h)^{r\kappa\gamma^i}$, which can be computed by all users. Since all users can compute $e(g^{\alpha}, h)^{r\kappa\gamma^i}$ for all i up to $m-1$, the security requires that $e(g^{\alpha}, h)^{r\kappa F(\gamma)}$ with an $(m-1)$-degree polynomial can only be generated by valid users.

In our scheme we take a different approach. We avoid to use dummy attributes by setting the way that all users can only compute $e(g^{\alpha}, h)^{r\kappa\gamma^i}$ for all i up to $s-t-1$, instead of $m-1$. Let $A_S \subseteq A \cap S$ be the attribute set with t attributes at most and $F(\gamma)$ be the polynomial defined as

$$F(\gamma) = \frac{\prod_{\mathsf{at} \in S}(\gamma + \tau(\mathsf{at}))}{\prod_{\mathsf{at} \in A_S}(\gamma + \tau(\mathsf{at}))},$$

where $F(\gamma)$ is a polynomial in γ with degree $s - |A_s|$.

Given the ciphertext, any private key user ($A \cap S \neq \emptyset$) can compute

$$e(g^{\beta}, h^{\alpha\gamma^{s-t}})^{-\kappa} e(g^{\alpha}, h)^{r\kappa\gamma^{s-t}}, \forall i \in [1-m, -1], e(g^{\alpha}, h)^{r\kappa\gamma^{s-t+i}} \text{and } e(g^{\alpha}, h)^{r\kappa F(\gamma)}.$$

The user will successfully decrypt the ciphertext if and only if $F(\gamma)$ has degree $s-t$. That is, $|A_S| = t$. If $|A_S| < t$, we have that the degree of $F(\gamma)$ is larger than $s-t$ such that all redundancy (that is $e(g^{\alpha}, h)^{r\kappa\gamma^i}$) cannot be removed for extracting the encryption key $e(g^{\beta}, h^{\alpha\gamma^{s-t}})^{-\kappa}$ from $e(g^{\alpha}, h)^{r\kappa F(\gamma)}$.

	Structures of Private Key and Ciphertext
Private Key in [16]	$sk_A = \left\{ \left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}} \right\}_{\mathsf{at}\in A},\ \left\{ h^{r\gamma^i} \right\}_{i\in[0,m-2]},\ h^{\frac{r-1}{\gamma}} \right\}$
Ciphertext in [16]	$\left(g^{\kappa\cdot\alpha\gamma},\ h^{\kappa\cdot\alpha\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))\prod_{d\in\mathcal{D}_{m+t-1-s}}(\gamma+d)},\ e(g^\alpha,h)^\kappa\cdot M \right)$
Our Private Key	$sk_A = \left\{ \left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}} \right\}_{\mathsf{at}\in A},\ \left\{ h^{r\gamma^i} \right\}_{i\in[1,m-1]},\ h^{(r-\beta)\gamma^m} \right\}$
Our Ciphertext	$\left(g^{\kappa\cdot\alpha\gamma^{s-t-m}},\ h^{\kappa\cdot\alpha\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))},\ e(g^\beta,h^{\alpha\gamma^{s-t}})^\kappa\cdot M \right)$

Table 1: Comparison between Herranz et al.'s scheme [16] and our scheme in terms of the structures of private key and ciphertext. In a private key, A is the set of attributes for a user and r is the chosen random number in private key generation. In the encryption, S is the set of attributes with s attributes where t is the corresponding threshold. κ is the random number chosen during encryption.

1.4. Related Work

The notion of attribute-based encryption (ABE) was first put forth by Sahai and Waters in [24], which was originally referred to as fuzzy identity-based encryption. Goyal et al. [15] further defined two variants of ABE, namely Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In a KP-ABE scheme, the ciphertext is associated with a set of attributes. The decryption key, which is issued by an authority, is associated with an access structure. The ciphertext will be decrypted if and only if the attribute set of ciphertext satisfies the access structure of the decryption key. In contrast, in a CP-ABE scheme, the ciphertext is equipped with an access structure, while the decryption key is associated with a set of attributes. The decryption is successful if and only if the attribute set fulfills the access structure. CP-ABE is more appropriate in access control applications, since it enables the encryptor to select the access structure to decide who is authorized to acquire the message. While the notion of CP-ABE has been proposed by Goyal et al. [15], it was first studied in [7, 3]. The work of Cheung and Newport [7] only supports AND gates. The first concrete construction with expressiveness was presented by Bethencourt, Sahai and Waters [3] by using threshold secret sharing to enforce the policy in the encryption phase. Its security was analyzed in the generic group model. Goyal et al. [14] proposed a generic construction to transform a KP-ABE scheme into a CP-ABE scheme, with the drawback of large ciphertext size (roughly $O(s^{3.4})$) which makes it impractical for expressive policies. Subsequently, a number of papers have

continued this line to achieve higher security schemes with expressive policy [18, 27, 21].

The ciphertext size in most constructions of CP-ABE, for example, [8, 26, 22, 7, 3, 17], is (at least) linear in the number of selected attributes. The first CP-ABE with constant-size ciphertexts under (n, n)-threshold access structure was proposed in [11]. While the KP-ABE scheme with constant-size ciphertexts was achieved by Attrapadung, Libert and Panafieu in [2] which supports general access structures. Herranz, Laguillaumie and Ràfols [16] initiated the study on achieving constant size ciphertext in threshold ABE, which is more expressive than merely AND gates (c.f. [7]). They incorporated the technique from [9] to achieve the goal, where the original work [9] concentrates on achieving constant-size ciphertext in a dynamic threshold identity-based encryption setting. The security in [16] is provable secure against chosen plaintext attacks (CPA) in the generic group model. Later, Yamada et al. [28] showed a generic construction for achieving chosen-ciphertext security (CCA) under the condition that the ABE scheme is of either delegatability or verifiability. Aiming to achieve CCA security in the standard model, Ge et al. [13] presented another threshold CP-ABE scheme with constant size ciphertexts by using the technique of [6]. Chen et al. [5] and Doshi and Jinwala [10] presented other constructions of threshold ABE with constant-size ciphertexts and full security.

In [13, 5], the private key generation requires a fixed universal attribute set prior to the private key generation. This means, any addition or removal of the attributes will require changes to all of the user's private keys. In contrast, Herranz et al.'s scheme [16] does not have this drawback. It is because there is no requirement to map an attribute to a group element in this scheme (cf. [13, 5]). The difference between these two approaches are usually referred to as "small universe" vs. "large universe". In a small universe constructions, at the setup time, a polynomial sized universe of attributes must be fixed. Additionally, the public parameters size is linear to the size of the attribute universe set. On the other hand, in a large universe constructions, the size of the attribute universe can be exponentially large. Furthermore, the size of the public parameters is linear to the upper bound of attribute number in the selected attribute set in the encryption phase. For further details about the differences between small universe and large universe, we refer the readers to [19, 28]. The notion of ABE was originally proposed for flexible access control. We refer the readers to such as [23, 20, 12] for some recent interesting work on access control.

2. Preliminaries

In this section, we revisit the definition and security model of threshold attribute-based encryption given in [16]. We also introduce a variant computational hard problem which is related to the security proof of our scheme.

2.1. Threshold Attribute-Based Encryption

A ciphertext-policy attribute-based encryption supporting threshold decryption policy consists of the following four algorithms.

- **Setup**$(\lambda, \mathcal{P}, m)$ The algorithm takes as input a security parameter λ, a universal set of attributes $\mathcal{P}$ and the upper bound of attribute number in encryption. It returns public parameters params and a master secret key.

- **Key Extraction**$(\mathsf{params}, A, \mathsf{msk})$ The algorithm takes as input public parameters, an attribute set $A \subseteq \mathcal{P}$ and the master secret key. It returns a private key sk_A for this attribute set.

- **Encryption**$(\mathsf{params}, S, t, M)$ The algorithm takes as input public parameters, an attribute set S, a threshold t satisfying $1 \leq t \leq |S|$ and a message M. It returns a ciphertext CT for (S, t).

- **Decryption**$(CT, (S, t), A, \mathsf{sk}_A)$ The algorithm takes as input a ciphertext for (S, t), an attribute set A and the corresponding private key sk_A. It returns a message if $|A \cap S| \geq t$, and $\perp$ otherwise.

We notice that the size of $\mathcal{P}$ in the original definition [16] is equal to m. However, we find that the size of $\mathcal{P}$ can be larger than m. The independence is much practical in use and we therefore adopt the latter definition. We show that the difference will not affect the construction and the security proof in this work.

The security of threshold ABE we consider here is *indistinguishability under selective security against chosen-plaintext attacks* (IND-sCPA), which is defined by the following game between an attacker $\mathcal{A}$ and a challenger.

1. The challenger specifies a universe of attributes $\mathcal{P}$ and upper bound number m, and gives them to the attacker $\mathcal{A}$.

2. The attacker $\mathcal{A}$ selects a subset $S \subseteq \mathcal{P}$ with s attributes and a threshold t for challenge, where s and t satisfy $1 \leq t \leq s$.
3. The challenger runs the setup algorithm of ABE algorithm and gives params to the attacker.
4. **Private Key Queries**: The attacker adaptively sends any subset of attributes $A \subseteq \mathcal{P}$ for private key queries with the restriction $|A \cap S| < t$. The challenger runs the key extraction algorithm and gives the corresponding private key sk_A to the attacker $\mathcal{A}$.
5. **Challenge**: The attacker outputs two messages M_0, M_1 for challenge. The challenger randomly chooses a bit $b \in \{0, 1\}$ and runs the encryption algorithm on the message M_b for (S, t) specified in the second step. The corresponding ciphertext CT^* is then given to the attacker as the challenge ciphertext.
6. The attacker continues to issue private key queries as in Step 4.
7. The adversary outputs a guess b' and wins the game if $b' = b$.

The advantage of the attacker in the above game is defined as $|\Pr[b' = b] - \frac{1}{2}|$. A Threshold ABE is said to be IND-sCPA secure if for all probabilistic polynomial-time attackers $\mathcal{A}$ its advantage in the game is negligible in λ.

2.2. The aMSE-DDH Problem

Our scheme is based on bilinear pairing. Its security relies on a hard problem slightly different from the problem defined in [16, 9]. Here, we still call this problem as *augmented multi-sequence of exponents decisional Diffie-Hellman problem* (aMSE-DHE) since the main difference is in the given exponents. We prove that this aMSE-DDH problem is one of the generic Diffie-Hellman problems defined by Boneh, Boyen and Goh in [4].

Let $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, p, e)$ be a bilinear pairing group, where p is the prime order of both $\mathbb{G}$ and $\mathbb{G}_T$, and e is the bilinear map. Let g_0, h_0 be two generators of $\mathbb{G}$. The input of aMSE-DDH problem consists of $q, s, t, f(x), g(x), T \in \mathbb{G}_T$ where $f(x), g(x)$ are random co-prime polynomials in the following formulas

$$f(x) = \prod_{i=1}^{q}(x + x_i), \quad g(x) = \prod_{i=1}^{s}(x + x'_i),$$

and group elements

$$
\begin{array}{llllll}
g_0, & h_0 & & & & \\
g_0^{\alpha_0}, & g_0^{\alpha_0\gamma}, & g_0^{\alpha_0\gamma^2}, \cdots, & g_0^{\alpha_0\gamma^{q+m}}, & & g_0^{\kappa\alpha_0 f(\gamma)\gamma^{s-t}} \\
g_0^{\beta_0}, & g_0^{\beta_0\gamma}, & g_0^{\beta_0\gamma^2}, \cdots, & g_0^{\beta_0\gamma^{q+t}} & & \\
g_0^{\omega}, & g_0^{\omega\gamma}, & g_0^{\omega\gamma^2}, \cdots, & g_0^{\omega\gamma^{q+t}} & & \\
h_0^{\alpha_0}, & h_0^{\alpha_0\gamma}, & h_0^{\alpha_0\gamma^2}, \cdots, & h_0^{\alpha_0\gamma^{2m}}, & & h_0^{\kappa\alpha_0 g(\gamma)\gamma^m} \\
h_0^{\beta_0}, & h_0^{\beta_0\gamma}, & h_0^{\beta_0\gamma^2}, \cdots, & h_0^{\beta_0\gamma^{m-1+(t-1)}} & & \\
h_0^{\omega}, & h_0^{\omega\gamma}, & h_0^{\omega\gamma^2}, \cdots, & h_0^{\omega\gamma^{m+t}}. & &
\end{array}
$$

All roots x_i, x_i' are given but all exponents $\alpha_0, \beta_0, \gamma, \omega$ are unknown. The aim of this problem is to decide whether the given group element T is

$$T = e(g_0, h_0)^{\kappa\alpha_0\beta_0 f(\gamma)\gamma^{m+s-1}},$$

or T is a random element from $\mathbb{G}_T$.

Theorem 1. *The aMSE-DDH assumption is a (P, Q, F)-Generic Diffie-Hellman Exponent (GDHE) assumption.*

Proof. Given $q, s, t, f(x), g(x), T \in \mathbb{G}_T$ where $f(x), g(x)$ are co-prime polynomials in the following formulas

$$
\begin{aligned}
f(x) &= \prod_{i=1}^{q}(x + x_i), \\
g(x) &= \prod_{i=1}^{s}(x + x_i'),
\end{aligned}
$$

and group elements

$$
\begin{array}{llllll}
g_0, & h_0 & & & & \\
g_0^{\alpha_0}, & g_0^{\alpha_0\gamma}, & g_0^{\alpha_0\gamma^2}, \cdots, & g_0^{\alpha_0\gamma^{q+m}}, & & g_0^{\kappa\alpha_0 f(\gamma)\gamma^{s-t}} \\
g_0^{\beta_0}, & g_0^{\beta_0\gamma}, & g_0^{\beta_0\gamma^2}, \cdots, & g_0^{\beta_0\gamma^{q+t}} & & \\
g_0^{\omega}, & g_0^{\omega\gamma}, & g_0^{\omega\gamma^2}, \cdots, & g_0^{\omega\gamma^{q+t}} & & \\
h_0^{\alpha_0}, & h_0^{\alpha_0\gamma}, & h_0^{\alpha_0\gamma^2}, \cdots, & h_0^{\alpha_0\gamma^{2m}}, & & h_0^{\kappa\alpha_0 g(\gamma)\gamma^m} \\
h_0^{\beta_0}, & h_0^{\beta_0\gamma}, & h_0^{\beta_0\gamma^2}, \cdots, & h_0^{\beta_0\gamma^{m-1+(t-1)}} & & \\
h_0^{\omega}, & h_0^{\omega\gamma}, & h_0^{\omega\gamma^2}, \cdots, & h_0^{\omega\gamma^{m+t}}, & &
\end{array}
$$

the aim of this problem is to decide whether

$$T = e(g_0, h_0)^{\kappa\alpha_0\beta_0 f(\gamma)\gamma^{m+s-1}}$$

or T is a random element from $\mathbb{G}_T$.

In the following theorem, we prove that this hard problem captures the independence as required in the (P, Q, F)-GDHE problem.

Theorem 2. *The aMSE-DDH assumption is a (P, Q, F)-GDHE assumption.*

Proof. Let $h_0 = g_0^{\eta}$ for some integer η. The aMSE-DDH problem can be reformulated as a (P, Q, F)-GDHE structure where

$$\begin{aligned}
P &= \begin{pmatrix}
1 & \eta & \kappa\alpha_0 f(\gamma)\gamma^{s-t} & \eta\kappa\alpha_0 g(\gamma)\gamma^{m} & \\
\alpha_0 & \alpha_0\gamma & \alpha_0\gamma^2 & \cdots & \alpha_0\gamma^{q+m} \\
\beta_0 & \beta_0\gamma & \beta_0\gamma^2 & \cdots & \beta_0\gamma^{q+t} \\
\omega & \omega\gamma & \omega\gamma^2 & \cdots & \omega\gamma^{q+t} \\
\eta\alpha_0 & \eta\alpha_0\gamma & \eta\alpha_0\gamma^2 & \cdots & \eta\alpha_0\gamma^{2m} \\
\eta\beta_0 & \eta\beta_0\gamma & \eta\beta_0\gamma^2 & \cdots & \eta\beta_0\gamma^{m+t-2} \\
\eta\omega & \eta\omega\gamma & \eta\omega\gamma^2 & \cdots & \eta\omega\gamma^{m+t}
\end{pmatrix}, \\
Q &= 1, \\
F &= \eta\kappa\alpha_0\beta_0 f(\gamma)\gamma^{m+s-1}.
\end{aligned}$$

To prove aMSE-DDH problem is a (P, Q, F)-GDHE problem, we need to prove that no coefficients $\{a_{i,j}\}$ and b_1 exist such that

$$F = \sum_{i,j=1}^{|P|} a_{i,j} p_i p_j + b_1 q_1,$$

where p_i, p_j are from P and q_1 is from Q. By making all possible products of two polynomials from P that contains common parameter $\eta\kappa\alpha_0\beta_0$, we prove that there is no linear combination from the set R below which can generate F.

$$R = \begin{pmatrix}
\eta\kappa\alpha_0\beta_0 \cdot g(\gamma)\gamma^{m} & \eta\kappa\alpha_0\beta_0 \cdot g(\gamma)\gamma^{m+1} & \cdots & \eta\kappa\alpha_0\beta_0 \cdot g(\gamma)\gamma^{q+m+t} \\
\eta\kappa\alpha_0\beta_0 \cdot f(\gamma)\gamma^{s-t} & \eta\kappa\alpha_0\beta_0 \cdot f(\gamma)\gamma^{s-t+1} & \cdots & \eta\kappa\alpha_0\beta_0 \cdot f(\gamma)\gamma^{m+s-2}
\end{pmatrix}.$$

If there exists such a combination, it can be written as

$$\eta\kappa\alpha_0\beta_0 f(\gamma)\gamma^{m+s-1} = \eta\kappa\alpha_0\beta_0 g(\gamma)\gamma^m \cdot A(\gamma) + \eta\kappa\alpha_0\beta_0 f(\gamma)\gamma^{s-t} \cdot B(\gamma),$$

where $A(\gamma)$ is a polynomial in γ of degree at most $(q+t)$ and $B(\gamma)$ is a polynomial of degree at most $(m+t-2)$. Let the degree of $A(x)$ be d_A in the above formula. We firstly simplify the formula as

$$f(\gamma)\gamma^{m+s-1} = g(\gamma)\gamma^m \cdot A(\gamma) + f(\gamma)\gamma^{s-t} \cdot B(\gamma).$$

Then, we have that

$$f(\gamma)\Big(\gamma^{m+t-1} - B(\gamma)\Big) = g(\gamma)\gamma^{m+t-s}A(\gamma).$$

The degree of $B(\gamma)$ is at most $m+s-2$ so that the left polynomial cannot be equivalent to zero. Therefore, the above equation implies that the two non-zero polynomials must have the same degree. The degree of the left polynomial is $q+m+t-1$ while the degree of the right polynomial is $s+m+t-s+d_A$. Hence, we have that $d_A = q-1$.

Since $f(\gamma)$ and $g(\gamma)\gamma^{m+t-s}$ are co-prime, we therefore have $f(\gamma)|A(\gamma)$ or $A(\gamma) \equiv 0$. The degree $d_A = q-1$ implies that $A(\gamma) \equiv 0$ and then $f(\gamma)\Big(\gamma^{m+t-1} - B(\gamma)\Big) \equiv 0$, which is contrary to non-zero $f(\gamma)\Big(\gamma^{m+t-1} - B(\gamma)\Big)$. This indicates no $A(\alpha), B(\alpha)$ exist and then no $\{a_{i,j}, b_1\}$ exist. This yields the theorem. □

3. Our New Threshold ABE Scheme

In this part we describe our threshold ABE scheme in details, which does not use any dummy attributes during encryption and decryption.

3.1. Description of Scheme

Setup$(\lambda, \mathcal{P}, m)$. The master entity chooses a suitable encoding τ[3] which maps each of the attributes $\mathsf{at} \in \mathcal{P}$ to a different element $\tau(\mathsf{at}) \in \mathbb{Z}_p$. It also

[3]We adopt the encoding τ used in the original paper [16] for scheme construction and security proof.

chooses a bilinear group $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, p, e)$ and generators g, h of $\mathbb{G}_1$. Next, the master entity picks at random $\alpha, \beta, \gamma \in \mathbb{Z}_p$ and sets

$$g_i = g^{\frac{\alpha}{\gamma^i}}, \quad h_i = h^{\alpha\gamma^i}, \quad u = g^{\beta}, \quad i \in [0, m].$$

The master secret key is $\mathsf{msk} = (g, h, \beta, \gamma)$ and the public parameters for $\mathcal{P}$ are

$$\mathsf{params} = \left\{ \mathbb{BG},\ m,\ g_0,\ g_1,\ g_2,\ \cdots,\ g_m,\ h_0,\ h_1,\ h_2, \cdots,\ h_m,\ u,\ \tau \right\}.$$

Key Extraction$(\mathsf{params}, A, \mathsf{msk})$**.** Given any subset $A \subseteq \mathcal{P}$, the master entity picks $r \in \mathbb{Z}_p$ at random and computes sk_A as

$$\mathsf{sk}_A = \left\{ \left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}} \right\}_{\mathsf{at}\in A},\ \ h^{r\gamma^1},\ \ h^{r\gamma^2}, \cdots,\ h^{r\gamma^{m-1}},\ h^{(r-\beta)\gamma^m} \right\}.$$

Encryption$(\mathsf{params}, S, t, M)$**.** Given a subset $S \subseteq \mathcal{P}$ with $s = |S|$ attributes, a threshold t satisfying $1 \le t \le s$, and a message $M \in \mathbb{G}_T$, the sender picks at random $\kappa \in \mathbb{Z}_p$ and computes

$$\begin{cases} C_1 = \left(g_{m-(s-t)}\right)^{\kappa} \\ C_2 = h^{\kappa\cdot\alpha\cdot\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))} \\ K = e(h_{s-t}, u)^{\kappa}. \end{cases}$$

The group element C_2 could be computed from $h^{\alpha\gamma^i}$ given in the public parameters params. Let $f_S(x) = \prod_{\mathsf{at}\in S}(x + \tau(\mathsf{at}))$ be the polynomial in x and a_i be the coefficient of x^i. We have $C_2 = \prod_{i=0}^{s}(h^{\alpha\gamma^i})^{a_i\kappa}$. The ciphertext is (C_1, C_2, C_3), where $C_3 = K \cdot M$.

Decryption$((C_1, C_2, C_3), (S, t), A, \mathsf{sk}_A)$**.** Any user with a set of attributes A satisfying $|A \cap S| \ge t$ can decrypt the ciphertext by using the private key sk_A. The decryption works as follows. Let A_S be any subset of $A \cap S$ with $|A_S| = t$, and $f_{S\setminus A_S}(x) = \prod_{\mathsf{at}\in S\setminus A_S}(x + \tau(\mathsf{at}))$ be the polynomial in x and b_i be the coefficient of x^i.

The user first computes the aggregation value as

$$\mathsf{Aggregate}^{4}\left(\left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}},\ \tau(\mathsf{at}) \right\}_{\mathsf{at}\in A_S} \right) = g^{\frac{r}{\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))}}.$$

[4]The detail aggregation algroithm can be found in [9], which requires $O(t^2)$ exponentiations.

Then, it computes

$$\begin{aligned} L &= e\Big(g^{\overline{\prod_{\mathsf{at}\in A_S}^{r}(\gamma+\tau(\mathsf{at}))}}, C_2\Big) \\ K^{-1}\cdot L &= e\left(C_1,\quad h^{(r-\beta)\gamma^m}\cdot\prod_{i=0}^{s-t-1}\left(h^{r\gamma^{i+m-(s-t)}}\right)^{b_i}\right) \end{aligned}$$

Finally, the user recovers the message by computing $M = C_3 \cdot K^{-1}L/L$.

3.2. Correctness

The decryption is correct since we have

$$\begin{aligned} L &= e\Big(g^{\overline{\prod_{\mathsf{at}\in A_S}^{r}(\gamma+\tau(\mathsf{at}))}}, C_2\Big) \\ &= e\Big(g^{\overline{\prod_{\mathsf{at}\in A_S}^{r}(\gamma+\tau(\mathsf{at}))}}, h^{\kappa\cdot\alpha\cdot\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))}\Big) \\ &= e(g,h)^{r\kappa\alpha\prod_{\mathsf{at}\in(S-A_S)}\left(\gamma+\tau(\mathsf{at})\right)}, \\ K^{-1}L &= e\left(C_1,\quad h^{(r-\beta)\gamma^m}\cdot\prod_{i=0}^{s-t-1}\left(h^{r\gamma^{i+m-(s-t)}}\right)^{b_i}\right) \\ &= e\left(g^{\frac{\kappa\alpha}{\gamma^{m-(s-t)}}},\quad h^{(r-\beta)\gamma^m}\cdot\prod_{i=0}^{s-t-1}\left(h^{r\gamma^{i+m-(s-t)}}\right)^{b_i}\right) \\ &= e\left(g^{\kappa\alpha},\quad h^{(r-\beta)\gamma^{s-t}}\cdot\prod_{i=0}^{s-t-1}\left(h^{r\gamma^{i}}\right)^{b_i}\right) \\ &= e\left(g^{\kappa\alpha},\quad h^{-\beta\gamma^{s-t}}\cdot\prod_{i=0}^{s-t}\left(h^{r\gamma^{i}}\right)^{b_i}\right) \\ &= e(g,h)^{-\kappa\alpha\beta\gamma^{s-t}}\cdot\prod_{i=0}^{s-t}e(g,h)^{\kappa\alpha r\cdot b_i\gamma^i} \\ &= e(g,h)^{-\kappa\alpha\beta\gamma^{s-t}}\cdot e(g,h)^{r\kappa\alpha\prod_{\mathsf{at}\in(S-A_S)}\left(\gamma+\tau(\mathsf{at})\right)}. \end{aligned}$$

3.3. Security Proof

Theorem 3. *For any adversary $\mathcal{A}$ against the IND-sCPA security of our ABE scheme with advantage ϵ for a universe P of q attributes, and a challenge pair (S,t) with $s = |S|$, there exists an algorithm for solving the (q,m,s,t)-aMSE-DDH problem with at least the same advantage ϵ.*

Proof. Let $\mathcal{A}$ be an adversary against the IND-sCPA security of our ABE scheme. We construct an algorithm (simulator) $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine to solve the aMSD-DDH problem. In particular, the simulator $\mathcal{B}$ is given an instance of this hard problem and its aim is to solve this problem by using $\mathcal{A}$'s guess of the encrypted message. The interaction between $\mathcal{A}$ and $\mathcal{B}$ works as follows.

Initialize: The simulator $\mathcal{B}$ specifies a universe of attributes $\mathcal{P} = \{\mathsf{at}_1, \cdots, \mathsf{at}_q\}$. Next, the adversary selectively chooses (S, t) to attack, where S is a set with s attributes and t is a threshold t satisfying $1 \leq t \leq s$. Without loss of generality, let $S = \{\mathsf{at}_1, \mathsf{at}_2, \cdots, \mathsf{at}_s\}$ be the challenge set.

Setup: Let group elements in the instance that $\mathcal{B}$ receives be

$$g_0^{\alpha_0},\ g_0^{\alpha_0\gamma},\ g_0^{\alpha_0\gamma^2}, \cdots,\ g_0^{\alpha_0\gamma^{q+m}},\qquad g_0^{\kappa\alpha_0 f(\gamma)\gamma^{s-t}}, \quad (1)$$

$$g_0^{\beta_0},\ g_0^{\beta_0\gamma},\ g_0^{\beta_0\gamma^2}, \cdots,\ g_0^{\beta_0\gamma^{q+t}}, \quad (2)$$

$$g_0^{\omega},\ g_0^{\omega\gamma},\ g_0^{\omega\gamma^2}, \cdots,\ g_0^{\omega\gamma^{q+t}}, \quad (3)$$

$$h_0^{\alpha_0},\ h_0^{\alpha_0\gamma},\ h_0^{\alpha_0\gamma^2}, \cdots,\ h_0^{\alpha_0\gamma^{2m}},\qquad h_0^{\kappa\alpha_0 g(\gamma)\gamma^m}, \quad (4)$$

$$h_0^{\beta_0},\ h_0^{\beta_0\gamma},\ h_0^{\beta_0\gamma^2}, \cdots,\ h_0^{\beta_0\gamma^{m-1+(t-1)}}, \quad (5)$$

$$h_0^{\omega},\ h_0^{\omega\gamma},\ h_0^{\omega\gamma^2}, \cdots,\ h_0^{\omega\gamma^{m+t}}, \quad (6)$$

where $f(x), g(x)$ are co-prime polynomials with degrees q and s, respectively, defined as

$$f(x) = \prod_{i=1}^{q}(x + x_i), \qquad g(x) = \prod_{i=1}^{s}(x + x_i^*).$$

The simulator $\mathcal{B}$ defines the encoding of each attribute into a unique root as below:

$$\tau(\mathsf{at}) = \begin{cases} x \text{ is a root of } f(x) & \text{if } \mathsf{at} \notin S, \\ x \text{ is a root of } g(x) & \text{if } \mathsf{at} \in S. \end{cases}$$

Then it sets $g, h, \alpha, \beta, \gamma$ using the group elements and unknown exponents in the instance as

$$g = g_0^{f(\gamma)},\quad h = h_0,\quad \alpha = \alpha_0\gamma^m,\quad \beta = \beta_0\gamma^{t-1},\quad \gamma = \gamma.$$

Then we have

$$\begin{aligned} g_i &= g^{\frac{\alpha}{\gamma^i}} = g_0^{\frac{f(\gamma)\alpha_0\gamma^m}{\gamma^i}} = g_0^{\alpha_0\gamma^{m-i}f(\gamma)} : \quad i \in [0, m], \\ h_i &= h_0^{\alpha_0\gamma^m\gamma^i} = h_0^{\alpha_0\gamma^{m+i}} : \quad i \in [0, m], \\ u &= g^{\beta} = g_0^{\beta_0 f(\gamma)\gamma^{t-1}}. \end{aligned}$$

The degree of polynomial $\gamma^{m-i}f(\gamma)$ in γ is at most $q+m$. And we have that all g_i can be computed from the line (1) of the instance, all h_i are available from the line (4) of the instance, and u can be computed from the line (2) of the instance because $f(\gamma)\gamma^{t-1}$ in u has degree $q+t-1$ only.

The algorithm $\mathcal{B}$ then simulates the rest of the game as below.

KeyGen: For a key extraction query on the attribute set $A \subseteq \mathcal{P}$, let $A_S = A \cap S$ where S is the challenge attribute set. We should have that $|A_S| \leq t-1$. The corresponding private key for this attribute set is

$$\mathsf{sk}_A = \left\{ \left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}} \right\}_{\mathsf{at}\in A}, \quad h^{r\gamma^1}, \quad h^{r\gamma^2}, \cdots, \ h^{r\gamma^{m-1}}, \ h^{(r-\beta)\gamma^m} \right\},$$

which requires the simulator to compute without knowing α and β.

The simulator first randomly chooses $r' \in \mathbb{Z}_p$ and sets the random number r in the above private key as

$$r = (r'\omega\gamma + \beta_0)\gamma^{t-1-|A_S|} \prod_{\mathsf{at}\in A_S} (\gamma + \tau(\mathsf{at})),$$

where β_0, γ, ω are from the instance. We have that r is uniformly random due to r'.

Since each attribute at in A is either in the set $A \backslash A_S$ or A_S, we have

$$x + \tau(\mathsf{at}_i) \ \Big| f(x) \prod_{\mathsf{at}\in A_S} (x + \tau(\mathsf{at})).$$

Let $f_{\mathsf{at}_i}(x)$ be

$$f_{\mathsf{at}_i}(x) = \frac{x^{t-1-|A_S|} f(x) \prod_{\mathsf{at}\in A_S}(x+\tau(\mathsf{at}))}{x + \tau(\mathsf{at}_i)},$$

which therefore is a polynomial in x of degree at most $q+t-1$. Define the following polynomials $f_1^i(x)$ and $f_2(x)$:

$$\begin{aligned} f_1^i(x) &= x^{i+t-1-|A_S|} \prod_{\mathsf{at}\in A_S} (x + \tau(\mathsf{at})), \quad \forall i \in [1, m-1], \\ f_2(x) &= x^{m+t-1-|A_S|} \prod_{\mathsf{at}\in A_S} (x + \tau(\mathsf{at})) - x^{m+t-1}. \end{aligned}$$

Their degrees are both at most $m+t-2$. Then we have

$$\begin{aligned}
g^{\frac{r}{\gamma+\tau(\mathsf{at})}} &= g_0^{\frac{(r'\omega\gamma+\beta_0)\gamma^{t-1-|A_S|}\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))\cdot f(\gamma)}{\gamma+\tau(\mathsf{at})}} \\
&= g_0^{r'\omega\gamma f_{\mathsf{at}_i}(\gamma)+\beta_0 f_{\mathsf{at}_i}(\gamma)}, \\
h^{r\gamma^i} &= h_0^{(r'\omega\gamma+\beta_0)\gamma^{t-1-|A_S|}\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))\cdot\gamma^i} \\
&= h_0^{(r'\omega\gamma+\beta_0)\gamma^{i+t-1-|A_S|}\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))} \\
&= h_0^{r'\omega\gamma f_1^i(\gamma)+\beta_0 f_1^i(\gamma)}, \\
h^{(r-\beta)\gamma^m} &= h_0^{\left((r'\omega\gamma+\beta_0)\gamma^{t-1-|A_S|}\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))-\beta\right)\gamma^m} \\
&= h_0^{(r'\omega\gamma+\beta_0)\gamma^{m+t-1-|A_S|}\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))-\beta\gamma^m} \\
&= h_0^{(r'\omega\gamma+\beta_0)\gamma^{m+t-1-|A_S|}\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))-\beta_0\gamma^{m+t-1}} \\
&= h_0^{r'\omega\gamma f_1^m(\gamma)+\beta_0 f_2(\gamma)},
\end{aligned}$$

and

- $\omega\gamma f_{\mathsf{at}_i}(\gamma)$ is a polynomial in γ with $q+t$ degree at most;
- $\beta_0 f_{\mathsf{at}_i}(\gamma)$ is a polynomial in γ with $q+t-1$ degree at most;
- $\omega\gamma f_1^i(\gamma)$ is a polynomial in γ with $m+t-1$ degree at most;
- $\beta_0 f_1^i(\gamma)$ is a polynomial in γ with $m+t-2$ degree at most;
- $\omega\gamma f_1^m(\gamma)$ is a polynomial in γ with $m+t-1$ degree at most;
- $\beta_0 f_2(\gamma)$ is a polynomial in γ with $m+t-2$ degree at most.

Finally, the simulator $\mathcal{B}$ computes $g^{\frac{r}{\gamma+\tau(\mathsf{at}_i)}}$ for all at_i from the lines (2) and (3) of the instance, $h^{r\gamma^i}$ for all $i\in[1,m-1]$ and $h^{(r-\beta)\gamma^m}$ from the lines (5) and (6) of the instance.

Challenge: Once the adversary $\mathcal{A}$ sends two messages $M_0, M_1 \in \mathbb{G}_T$ for challenge, the simulator $\mathcal{B}$ flips a random coin $b\in\{0,1\}$ and sets the challenge ciphertext on message M_b for (S,t) as

$$\begin{cases} C_1^* = g_0^{\kappa\alpha_0 f(\gamma)\gamma^{s-t}}, \\ C_2^* = h_0^{\kappa\alpha_0\alpha_0 g(\gamma)\gamma^m}, \\ C_3^* = T\cdot M_b, \end{cases}$$

where $g_0^{\kappa\alpha_0 f(\gamma)\gamma^{s-t}}$ is from the last element of the line (1), $h_0^{\kappa\alpha_0\alpha_0 g(\gamma)\gamma^m}$ is from the last element of the line (2) and T is the unknown element to be decided.

Let κ in the instance be the random number for encryption. If $T = e(g_0, h_0)^{\alpha_0\beta_0 f(\gamma)\gamma^{m+s-1}}$, we have

$$\begin{cases} C_1^* = \left(g_{m-(s-t)}\right)^{\kappa} = g^{\kappa\alpha\gamma^{s-t-m}} = g_0^{\kappa\alpha_0 f(\gamma)\gamma^{s-t}}, \\ C_2^* = h^{\kappa\cdot\alpha\cdot\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))} = h_0^{\kappa\alpha_0 g(\gamma)\gamma^m}, \\ C_3^* = e(h_{s-t}, u)^{\kappa}\cdot M_b = e(h_0^{\alpha_0\gamma^{m+s-t}}, g_0^{f(\gamma)\beta_0\gamma^{t-1}})\cdot M_b = T\cdot M_b. \end{cases}$$

Therefore, CT^* is a valid challenge ciphertext for (S, t) on the message M_b. On the other hand, if T is random, C_3 is random and independent of the choice of the bit b.

Guess: The adversary returns a guess b' of b, and the simulator returns true if $b' = b$ which means $T = e(g_0, h_0)^{\alpha_0\beta_0 f(\gamma)\gamma^{m+s-1}}$. Otherwise, the simulator returns a random T.

There is no abortion during the simulation as all private keys and the challenge ciphertext are computable from the instance of the hard problem. It is easy to see that g, h are random group elements because of g_0, h_0 and α, β, γ are uniformly random and independent due to $\alpha_0, \beta_0, \gamma$ in the instance. Notice that each random number r in the private key generation is computed by $(r'\omega\gamma + \beta_0)\gamma^{t-1-|A_S|}\prod_{\mathsf{at}\in A_S}(\gamma + \tau(\mathsf{at}))$ where r' is chosen randomly and independently. Therefore, the simulation is indistinguishable from the real scheme when T is true. The adversary cannot distinguish the simulation from the real scheme and will break the scheme with advantage ϵ according to the definition of security. When T is false, it is uniformly random and independent from the view of C_1^*, C_2^* so that it is a one-time pad and hence the adversary has no advantage in guessing the chosen bit b. Therefore we have that

$$\begin{aligned} \epsilon_{reduction} &= \left|\Pr[\mathcal{B} \text{ guess T=True}|\text{T=True}] - \Pr[\mathcal{B} \text{ guess T=True}|\text{T=False}]\right| \\ &= \left|\Pr[b' = b|\text{T=True}] - \Pr[b' = b|\text{T=False}]\right| \\ &= \frac{1}{2} + \epsilon - \frac{1}{2} \\ &= \epsilon. \end{aligned}$$

This completes the proof for theorem. □

4. Discussion and Comparison

4.1. Benefits of Encryption without Dummy Attributes

Let $f(\gamma)$ be the polynomial in γ whose degree is $m-1$. We have the computation on $h^{\kappa\alpha f(\gamma)}$ from $\kappa, h^{\alpha\gamma^i}: \ i \in [0, m-1]$ requires m exponentiations. In particular, let f_i be the coefficient of γ^i in $f(\gamma)$. We have $h^{\kappa\alpha f(\gamma)}$ is computed by

$$h^{\kappa\alpha f(\gamma)} = \prod_{i=0}^{m} (h^{\alpha\gamma^i})^{f_i}.$$

If we want to compute $h^{\kappa\alpha f(\gamma)(\gamma+d)}$, we cannot save the overload computation with the additional input $h^{\kappa\alpha f(\gamma)}$ as $h^{\kappa\alpha f(\gamma)(\gamma+d)}$ must be computed by

$$h^{\kappa\alpha f(\gamma)(\gamma+d)} = \prod_{i=0}^{m} (h^{\alpha\gamma^{i+1}})^{f_i} \cdot \left(h^{\kappa\alpha f(\gamma)}\right)^d,$$

which still requires a linear number of exponentiations in the degree of $f(\gamma)(\gamma+d)$.

The main computation in encryption of [16] is dominated by

$$C_2 = h^{\kappa\cdot\alpha \prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))\prod_{d\in\mathcal{D}_{m+t-1-s}}(\gamma+d)},$$

while in our scheme it is dominated by $C_2 = h^{\kappa\cdot\alpha\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))}$. Based on the above analysis, our encryption time is liner in the number of s while the scheme in [16] is linear in the number of m, where m is the upper bound of s. The corresponding decryption is also different and ours will be much faster. The detailed efficiency comparison is provided in Table 2.

4.2. Efficient Threshold Change

Another benefit of our encryption is the dynamic choice of the threshold t after the selection of attribute set S. Notice that an encryption is to compute C_1, C_2 and K, which costs one exponentiation, $|S|$ exponentiations and one exponentiation, respectively. In our scheme, upon receiving the set S, the encryptor can compute C_2 without the need of the threshold t, which dominates most of exponentiations in encryption. Once the threshold t is given, only two exponentiations are required to compute C_1 and K. While in [16], both S and t must be provided before the encryption, otherwise the encryptor cannot perform the computation of C_2. This property allows

Schemes	Key Size	Ciphertext Size	Encryption Cost	Decryption Cost
CN[7]	$(2n+1)\|\mathbb{G}\|$	$(n+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(n+2)\mathbf{e}$	$(n+1)\mathbf{p}$
DJ[10]	$(\|A\|+2)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$3\mathbf{e}$	$2\mathbf{p}$
EMN+[11]	$2\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$3\mathbf{e}$	$2\mathbf{p}+3\mathbf{e}$
BSW[3]	$(2\|A\|+1)\|\mathbb{G}\|$	$(\ell+1)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(2\ell+2)\mathbf{e}$	$\|I\|\mathbf{p}$
W[27]	$(\|A\|+2)\|\mathbb{G}\|$	$(\ell+2)\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(2\ell+2)\mathbf{e}$	$\|I\|\mathbf{p}$
GZC+[13]	$2n(n+\|A\|)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$3\mathbf{e}$	$2\mathbf{p}+2n\mathbf{e}$
HLR[16]	$(m+\|A\|)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$(m+t+1)\mathbf{e}$	$3\mathbf{p}+O(t^2+m)\mathbf{e}$
Ours	$(m+\|A\|)\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$1\mathbf{p}+(s+3)\mathbf{e}$	$2\mathbf{p}+O(t^2+s)\mathbf{e}$

Table 2: Efficiency Comparison of related CP-ABE schemes. $\mathbf{p}$ and $\mathbf{e}$ are paring computation and exponentiation computation, respectively. n is the number of universal attributes. ℓ is the size of an access formula. s is the number of attributes in the chosen attribute set S. t is the corresponding threshold number and m is the upper bound of attribute number in S. $|A|$ and $|I|$ are the numbers of attributes in a user's key and the number of attributes satisfied the function, respectively. We notice that the pairing computation in the encryption can be saved if all $e(h^{\alpha\gamma^i}, u)$ have been precomputed in the public parameters.

the encryptor to flexibly change the threshold during the application before publishing the ciphertext. More precisely, suppose the encryptor has already created a ciphertext for (S, t) using the random number κ and the ciphertext is not yet published. If the threshold t needs to be revised with t' for any t', the encryptor can use the old C_2 and re-compute C_1, K for the updated threshold t', which allows the encryptor to quickly change (S, t) into (S, t') with two exponentiations. There is no security issue in this variant encryption because only the ciphertext for (S, t') is published and it is equivalent to a ciphertext generation from the encryption algorithm directly. The detailed performance comparison is provided in Table 3.

5. Conclusion

Attribute-based encryption (ABE) has proven to be a very promising cryptographic primitive that offers fine-grain access control. Herranz et al. proposed the first constant-size threshold ABE. However, their scheme makes use of dummy attributes, which leads to inefficiency. In this work, we improved Herranz et al.'s work and proposed a new threshold ABE scheme which *does not require any dummy attributes*. We made two specific improvements in comparison to the previous work. First, the cost for encryption and decryption is only linear to the size of the selected attribute set. Second, the threshold can be decided after the selection of the attribute set in the

Schemes	Universe	Threshold Change	Security	Expressiveness
CN[7]	Small	×	Selective	AND-gate
DJ[10]	Small	×	Full	AND-gate
EMN+[11]	Small	×	Selective	(n,n)-Threshold
BSW[3]	Large	×	Selective	Access Tree
W [27]	Small	×	Selective	LSSS
GZC+[13]	Small	$\approx 1\mathbf{e}$	Selective	Threshold
HLR[16]	Large	$(m+t-1)\mathbf{e}$	Selective	Threshold
Ours	Large	$2\mathbf{e}$	Selective	Threshold

Table 3: Comparison of related CP-ABE schemes. The symbol "×" means that it does not support the corresponding functionality.

encryption phase. These two properties make our scheme more attractive in practical use.

Acknowledgement

Qiong Huang is supported by Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2014A030306021), Guangdong Program for Special Support of Top-notch Young Professionals (No. 2015TQ01X796), Pearl River Nova Program of Guangzhou (No. 201610010037), the National Natural Science Foundation of China (No. 61472146), and the CICAEET fund and the PAPD fund (No. KJR1615).

References

[1] Attrapadung, N., Herranz, J., Laguillaumie, F., Libert, B., de Panafieu, E., Ràfols, C.. Attribute-based encryption schemes with constant-size ciphertexts. Theoretical Computer Science 2012;422:15–38.

[2] Attrapadung, N., Libert, B., de Panafieu, E.. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A., editors. PKC 2011. Springer; volume 6571 of *LNCS*; 2011. p. 90–108.

[3] Bethencourt, J., Sahai, A., Waters, B.. Ciphertext-policy attribute-based encryption. In: S&P 2007. IEEE Computer Society; 2007. p. 321–334.

[4] Boneh, D., Boyen, X., Goh, E.. Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R., editor. EUROCRYPT 2005. Springer; volume 3494 of *LNCS*; 2005. p. 440–456.

[5] Chen, C., Chen, J., Lim, H.W., Zhang, Z., Feng, D., Ling, S., Wang, H.. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In: Dawson, E., editor. CT-RSA 2013. Springer; volume 7779 of *LNCS*; 2013. p. 50–67.

[6] Chen, C., Zhang, Z., Feng, D.. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In: Boyen, X., Chen, X., editors. ProvSec 2011. Springer; volume 6980 of *LNCS*; 2011. p. 84–101.

[7] Cheung, L., Newport, C.C.. Provably secure ciphertext policy ABE. In: Ning, P., di Vimercati, S.D.C., Syverson, P.F., editors. ACM CCS 2007. ACM; 2007. p. 456–465.

[8] Daza, V., Herranz, J., Morillo, P., Ràfols, C.. Extended access structures and their cryptographic applications. IACR Cryptology ePrint Archive 2008;2008:502.

[9] Delerablée, C., Pointcheval, D.. Dynamic threshold public-key encryption. In: Wagner, D., editor. CRYPTO 2008. Springer; volume 5157 of *LNCS*; 2008. p. 317–334.

[10] Doshi, N., Jinwala, D.C.. Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption. Security and Communication Networks 2014;7(11):1988–2002.

[11] Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M.. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: Bao, F., Li, H., Wang, G., editors. ISPEC 2009. Springer; volume 5451 of *LNCS*; 2009. p. 13–23.

[12] Gai, K., Qiu, M., Ming, Z., Zhao, H., Qiu, L.. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. IEEE Transactions on Smart Grid 2017;PP(99).

[13] Ge, A., Zhang, R., Chen, C., Ma, C., Zhang, Z.. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts. In: Susilo, W., Mu, Y., Seberry, J., editors. ACISP 2012. Springer; volume 7372 of *Lecture Notes in Computer Science*; 2012. p. 336–349.

[14] 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., editors. ICALP 2008. Springer; volume 5126 of *LNCS*; 2008. p. 579–591.

[15] 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., editors. ACM CCS 2006. ACM; 2006. p. 89–98.

[16] Herranz, J., Laguillaumie, F., Ràfols, C.. Constant size ciphertexts in threshold attribute-based encryption. In: Nguyen, P.Q., Pointcheval, D., editors. PKC 2010. Springer; volume 6056 of *LNCS*; 2010. p. 19–34.

[17] Karati, A., Amin, R., Biswas, G.P.. Provably secure threshold-based abe scheme without bilinear map. Arabian Journal for Science and Engineering 2016;41(8):3201–3213.

[18] Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K., Waters, B.. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H., editor. EUROCRYPT 2010. Springer; volume 6110 of *LNCS*; 2010. p. 62–91.

[19] Lewko, A.B., Waters, B.. Unbounded HIBE and attribute-based encryption. In: Paterson, K.G., editor. EUROCRYPT 2011. Springer; volume 6632 of *LNCS*; 2011. p. 547–567.

[20] Li, Y., Gai, K., Ming, Z., Zhao, H., Qiu, M.. Intercrossed access controls for secure financial services on multimedia big data in cloud systems. TOMCCAP 2016;12(4s):67:1–67:18.

[21] Okamoto, T., Takashima, K.. Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T., editor. CRYPTO 2010. Springer; volume 6223 of *LNCS*; 2010. p. 191–208.

[22] Phuong, T.V.X., Yang, G., Susilo, W.. Hidden ciphertext policy attribute-based encryption under standard assumptions. IEEE Trans Information Forensics and Security 2016;11(1):35–45.

[23] Qiu, M., Gai, K., Thuraisingham, B., Tao, L., Zhao, H.. Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future Generation Computer Systems 2016;.

[24] Sahai, A., Waters, B.. Fuzzy identity-based encryption. In: Cramer, R., editor. EUROCRYPT 2005. Springer; volume 3494 of *LNCS*; 2005. p. 457–473.

[25] Susilo, W., Guo, F., Mu, Y.. Efficient dynamic threshold identity-based encryption with constant-size ciphertext. Theoretical Computer Science 2016;609:49–59.

[26] Waters, B.. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. IACR Cryptology ePrint Archive 2008;2008:290.

[27] Waters, B.. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A., editors. PKC 2011. Springer; volume 6571 of *LNCS*; 2011. p. 53–70.

[28] Yamada, S., Attrapadung, N., Hanaoka, G., Kunihiro, N.. Generic constructions for chosen-ciphertext secure attribute based encryption. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A., editors. PKC 2011. Springer; volume 6571 of *LNCS*; 2011. p. 71–89.