1-1-2016

Efficient dynamic threshold identity-based encryption with constant-size ciphertext

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

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

Yi Mu
University of Wollongong, ymu@uow.edu.au

Efficient dynamic threshold identity-based encryption with constant-size ciphertext

Abstract

This paper revisits the notion of dynamic threshold identity-based encryption, due to the recent practical interest. In this notion, an encryptor selects n recipients and a threshold value t for the creation of the ciphertext. The plaintext can only be recovered if at least t receivers cooperate. The key issue in this notion is its dynamicity, where after the users enroll to the system, the sender can dynamically select the set of recipients as well as dynamically set the threshold t upon the creation of the ciphertext. Another essential feature of this notion is the need for a constant-size ciphertext. Interestingly, the work by Delerablée and Pointcheval in Crypto 2008 is the only work that achieves this essential feature. In this work, we propose a new scheme achieving all of these nice properties with significant improvements in terms of the computational efficiency (both the encryption and decryption). In our scheme, there is no need to conduct any encryption and decryption using additional dummy users, which are not part of the recipient group, which is in contrast to Delerablée and Pointcheval's work. This improvement has significantly reduced the amount of computations required in both encryption and decryption algorithms.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Susilo, W., Guo, F. & Mu, Y. (2016). Efficient dynamic threshold identity-based encryption with constant-size ciphertext. Theoretical Computer Science, 609 (1), 49-59.

Efficient Threshold Attribute-Based Encryption with Constant-size Ciphertexts 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 user attributes. In a threshold ABE, users who can decrypt the ciphertexts must hold at least t attributes among a certain universe of attributes, selected by the encryptor. At PKC 2010, Herranz, Laguillaumie and Ràfols presented the first threhold ABE with constant size ciphertexts. To make sure the encryptor can flexibly select the attribute set and a threshold value, they employed dummy attributes to satisfy the decryption requirement. The nice feature of this scheme is that any addition or removal of the attributes will not require any changes to any of the user's private keys. Unfortunately, the need for the dummy attributes has made the scheme become inefficient, since the encryption efficiency is linear to the size of selected attribute set and dummy attribute set. In this work, we propose a novel approach to achieve a constant-size threshold ABE *without dummy attributes*. Our scheme retains the nice feature offered earlier. Furthermore, the scheme has offered two improvements in comparison to the previous work. First, in terms of the cost for encryption and decryption is only linear to the size of the selected attribute set. Second, without any dummy attributes, majority of the computations can be conducted without the knowledge of the threshold value. 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

Attribute-based encryption (ABE) [12] has been a very active area of research recently, since it supports fine-grained access control of shared data. ABE is an extension of public key encryption that allows users to encrypt and decrypt messages based on user attributes. It is very useful in providing anonymous access control, which is a very desirable property in many applications, such as encrypted storage in distributed environments. In a ciphertext-policy attribute-based encryption (CP-ABE) scheme, the attributes of the users determine their secret keys. When an encryptor encrypts a message, he/she selects a policy indicating what kinds of subset of attributes that must be held by a receiver in order to be able to decrypt. Unfortunately, this extra functionality comes at a

cost. In a typical implementation, the size of the ciphertext is 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 with constant-size ciphertexts under AND gates access structure was proposed in [5]. Subseqently, Herranz, Laguillaumie and Ràfols [10][1] presented the first constant size ciphertexts in threshold ABE, which represents a more expressive access structure in comparison to [5]. Their construction works for the threshold case, where users who are authorized to decrypt are those who hold at least t attributes among a certain universe of attributes, for some threshold value t selected by the encryptor. The flexibility in this scheme is due to the ability of the encryptor to select any threshold value t during the encryption phase, which makes the scheme very practical. The scheme is inspired from the technique introduced by Delerablée and Pointcheval [7] in achieiving a dynamic threshold identity-based encryption. The scheme is proven secure under the standard model by reduction to the augmented multi-sequence of exponents decisional Diffie-Hellman (aMSE-DDH) problem [10].

The technique used in Delerablée and Pointcheval [7] is to incorporate some "dummy information" (and hence, the notion of *dummy users* in the context of the proposed identity-based encryption scheme in [7]) as part of the computations in order to achieve constant size property. This inherent technique is carried across to achieve the construction of threshold ABE scheme in [10] with the introduction of *dummy attributes*, which leads to significant inefficiency in both encryption and decryption algorithms, since their efficiencies are linear to the size of selected attribute set and dummy attribute set. To illustrate this, consider the following parameters used in [10]. Let s be 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. The costs for conducting encryption and decryption in [10] are mainly dominated by $m + t + 1$ exponentiations and $O(t^2 + m)$ exponentiations, resp. In a typical scenario where $m = 10,000$, $t = 3$ and $s = 10$. It means the encryptor allows the user to decrypt the ciphertext if there are 3 matching attributes among the 10 attributes specified are owned by the user. Nevertheless, the small choice of parameters in s and t will result in a large computation requirement, since m is large. It is clear that the main stumbling block for this inefficiency is due to the value of m, which is the number of dummy attributes.

Herranz et al.'s scheme is equipped with a nice feature, namely any addition or removal of the attributes will not require any changes to any of the user's private keys. We note that there are some subsequent works that achieve threshold ABE but they are not equipped with this feature. These works will be reviewed in the related work.

Summary of Our Contributions

The contributions of this paper are twofold:

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

– We achieve an efficient threshold ABE with constant size ciphertexts without using dummy attributes. Prior to this work, the authors in [10] makes use of dummy attributes to satisfy the threshold decryption requirement. This poses great inefficiency in terms of computations in encryption and decryption phases. Let s be the number of attributes in the chosen attribute set S, t be the corresponding threshold number and m be the upper bound of attribute number in S. The major cost for encryption for the scheme in [10] in comparison to ours is $m+t+1$ exponentiations and $s+3$ exponentiations, resp. The major cost for decryption for the scheme in [10] in comparison to ours is $O(t^2+m)$ exponentiations and $O(t^s+s)$ exponentiations, resp. In our scheme, the pairing computation can be further saved using precomputation in the public parameters (refer to Sec. 3 for the detail).
– We enable an efficient threshold change for the encryptor during the encryption process, in comparison to the previous work in [10]. The impact of using dummy attributes is the threshold value t must be known in the beginning of the encryption process, as this value determines how the ciphertext is being formed. By using our approach, the impact of the value t may only be required in one or two operations during the encryption, but not the overall computation. Therefore, the encryptor can change the threshold value t without having to recompute the overall ciphertext.

Technical Contributions
In the following, we will describe the overview of our technique in comparison to the technique presented in [10]. In [10], 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.

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

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

According to the setting, all redundant group elements $e(g^\alpha,h)^{r\kappa\gamma^i}$ must be removed to extract the encryption key. Therefore, the user will successfully decrypt the ciphertext iff $F(\gamma)$ has $m-1$ degrees at most, which requires $|A_S| \geq t$. If they do not embed dummy attributes in $F(\gamma)$, the degree of $F(\gamma)$ will be always less than $m-1$ when the user has an attribute, such that the user can decrypt the ciphertext even his/her attribute number does not satisfy the threshold number.

We notice that the 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.

We take a different approach in building our scheme. We avoid the use of 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 polynimial in γ with degree $s - |A_s|$.

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

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

The user will successfully decrypt the ciphertext iff $F(\gamma)$ has an degree $s-t$. That is, $|A_S| = t$. If $|A_S| < t$, we have 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 $e(g^{\beta}, h^{\alpha\gamma^{s-t}})^{-\kappa}$.

	Structures of Private Key and Ciphertext
Private Key in [10]	$sk_A = \left\{ \left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}} \right\}_{\mathsf{at}\in A},\ \left\{ h^{r\gamma^i} \right\}_{i\in[0,m-2]},\ h^{\frac{r-1}{\gamma}} \right\}$
Ciphertext in [10]	$\left(g^{\kappa\cdot\alpha\gamma},\ h^{\kappa\cdot\alpha\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))\prod_{d\in\mathcal{D}_{m+t-1-s}}(\gamma+d)},\ e(g^{\alpha}, h)^{\kappa}\cdot M \right)$
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 the structure of Herranz et al.'s scheme [10] and our scheme. In the 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 number. κ is the chosen random number in encryption.

Using our approach, we can inherently solve the second motivation of our work, which will be illustrated later.

1.1 Related Work

The notion of attribute-based encryption (ABE) was first put forth by Sahai and Waters in [12], which was originally referred to as fuzzy identity-based encryption. Goyal et al. [9] 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 decryptable with the decryption key 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. Decryption condition is defined similarly, namely 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. [9], the first concrete construction was presented by Bethencourt, Sahai and Waters [2].

The ciphertext size in majority constructions of CP-ABE is linear in the number in the number of selected attributes. The first CP-ABE with constant-size ciphertexts under AND gates access structure was proposed in [5]. Subsequently, in [10], Herranz, Laguillaumie and Ràfols initiated the study on achieving constant size ciphertext in threshold ABE, which is more expressive than merely AND gates (c.f. [5]). They incorporated the technique from [7] to achieve this, where the original work in [7] concentrates on achieving constant size ciphertext in a dynamic threshold identity-based encryption setting. Subsequently, Ge et al. [8] and Chen et al. [4] presented other constructions of threshold ABE scheme with constant size ciphertext, which aims to achieve a stronger security model.

In [8, 4], 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 [10] does not have this inherent drawback. This is because there is no requirement to map an attribute to a group element in this scheme (cf. [8, 4]). 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 polynomially 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 S, where S is the selected attribute set in the encryption phase. For further detail about the differences between these, we refer the reader to [11].

2 Preliminaries

In this section, we revisit the definition and security model of threshold attribute-based encryption given in [10]. 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 the threshold decryption policies 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 with a threshold number 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), the attribute set A and related private key sk_A. It returns a message if $|A \cap S| \geq t$.

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

The security model of threshold ABE for indistinguishability under selective security against chosen-plaintext attacks (IND-sCPA) is defined by considering 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, which are given to the attacker $\mathcal{A}$.
2. The attacker $\mathcal{A}$ selects a subset $S \subseteq \mathcal{P}$ with s attributes and a threshold number 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 given to the attacker as the challenge ciphertext.
6. Step 4 is repeated.
7. The adversary outputs a guess b' of 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 this advantage is negligible with respect to the security parameter λ for all polynomial attackers $\mathcal{A}$.

2.2 The aMSE-DDH Problem

Our scheme is also based on a bilinear pairing but its security relies on a hard problem slightly different from the problem defined in [10, 7]. Here, we still call

this problem as an augmented multi-sequence of exponents decisional Diffie-Hellman problem (aMSE-DHE) since the main difference is in the given exponents. In the subsequent section, we prove that this aMSE-DDH problem is one of generic Diffie-Hellman problems defined by Boneh, Boyen and Goh in [3].

Let $\mathbb{BG} = (\mathbb{G}, \mathbb{G}_T, p, e)$ be the pairing group, where p is the prime order of both groups 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 co-prime polynomials in the following formulas

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

and group elements

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

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. The proof will be provided in Appendix A.

3 The New Threshold ABE Scheme

3.1 Description of Scheme

Setup($\lambda, \mathcal{P}, m$). The master entity chooses a suitable encoding τ sending each of the attributes $\mathsf{at} \in \mathcal{P}$ onto a different element $\tau(\mathsf{at}) \in \mathbb{Z}_p$. He also 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 are

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

Key Extraction$(\mathsf{params}, A, \mathsf{msk})$**.** Given any subset $A \subset \mathcal{P}$, 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 $S \subset \mathcal{P}$ 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 is 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 then (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 $f_{S-A_S}(x) = \prod_{\mathsf{at}\in S-A_S}(x + \tau(\mathsf{at}))$ be the polynomial in x and b_i be the coefficient of x^i.

The user first computes the aggregation value as

$$\mathsf{Aggregate}^{2}\left(\left\{ g^{\frac{r}{\gamma+\tau(\mathsf{at})}},\ \tau(\mathsf{at}) \right\}_{\mathsf{at}\in A_S} \right) = g^{\frac{r}{\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))}}.$$

Then, the user computes

$$L = e\left(g^{\frac{r}{\prod_{\mathsf{at}\in A_S}(\gamma+\tau(\mathsf{at}))}}, C_2\right)$$

$$K^{-1}\cdot L = e\left(C_1,\ \ h^{(r-\beta)\gamma^m}\cdot\prod_{i=0}^{s-t-1}\left(h^{r\gamma^{i+m-(s-t)}}\right)^{b_i}\right)$$

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

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

3.2 Correctness

The decryption is correct since we have

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

3.3 Security Proof

Theorem 2. *Let λ be an integer. For any adversary $\mathcal{A}$ against the IND-sCPA security of our ABE scheme with advantage ϵ for a universal of q attributes P, and a challenge pair (S,t) with $s=|S|$, there exists an algorithm solving the (q,m,s,t)-aMSE-DDH problem with the same advantage ϵ.*

Proof. Suppose there exists an adversary $\mathcal{A}$ against the IND-sCPA security of our ABE scheme. We are going to construct an algorithm (simulator) $\mathcal{B}$ that uses $\mathcal{A}$ as a black-box and solves the aMSD-DDH problem. In particular, the simulator $\mathcal{B}$ is given an instance of this hard problem and his aim is to solve this problem by using the guess of encrypted message. The interaction between $\mathcal{A}$ and $\mathcal{B}$ works as follows.

Initialize: The simulator $\mathcal{B}$ specifies a universe of attributes $\mathcal{P}=\{\mathsf{at}_1,\mathsf{at}_2,\cdots,\mathsf{at}_q\}$. Next, the adversary selectively chooses (S,t) to attack, where S is a set with s attributes and t is a threshold number t satisfying $1\le t\le s$. 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

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

$$g_0^{\beta_0},\ g_0^{\beta_0\gamma},\ g_0^{\beta_0\gamma^2},\cdots,\ g_0^{\beta_0\gamma^{q+t}} \tag{2}$$

$$g_0^{\omega},\ g_0^{\omega\gamma},\ g_0^{\omega\gamma^2},\cdots,\ g_0^{\omega\gamma^{q+t}} \tag{3}$$

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

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

$$h_0^{\omega},\ h_0^{\omega\gamma},\ h_0^{\omega\gamma^2},\cdots,\ h_0^{\omega\gamma^{m+t}} \tag{6}$$

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

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

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

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

where 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 $\gamma^{m-i}f(\gamma)$ in γ is $q+m$ at most, we have all g_i can be computed from the line (1) of the instance. It is easy to find that are 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.

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

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

which requires the simulator to compute it 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 r is uniformly random due to r'.

In terms of the simulation on the private key, we have the holding of the following equations. Since each attribute at in A is either in the set $A - A_S$ 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 with degree $q + t - 1$ at most.

Let $f_1^i(x), f_2^i(x), f_3(x)$ be polynomials defined as

$$\begin{aligned}
f_1^i(x) &= x \cdot x^{i+t-1-|A_S|} \prod_{\mathsf{at} \in A_S} (x + \tau(\mathsf{at})) \\
f_2^i(x) &= x^{i+t-1-|A_S|} \prod_{\mathsf{at} \in A_S} (x + \tau(\mathsf{at})) \\
f_3(x) &= x^{m+t-1-|A_S|} \prod_{\mathsf{at} \in A_S} (x + \tau(\mathsf{at})) - \gamma^{m+t-1}
\end{aligned}$$

whose degrees are $m + t - 1, m + t - 2, m + t - 2$ at most. We have

$$\begin{aligned}
g^{\frac{r}{\gamma + \tau(\mathsf{at})}} &= g_0^{\frac{(r'\omega\gamma + \beta_0)\gamma^{t-1-|A_S|} \cdot f(\gamma) \prod_{\mathsf{at} \in A_S} (\gamma + \tau(\mathsf{at}))}{\gamma + \tau(\mathsf{at})}} \\
&= g_0^{r'\omega\gamma f_{\mathsf{at}_i}(\gamma) + \beta_0 f_{\mathsf{at}_i}(\gamma)} \\
h^{r\gamma^i} &= h_0^{(r'\omega\gamma + \beta_0)\gamma^{t-1-|A_S|} \prod_{\mathsf{at} \in A_S} (\gamma + \tau(\mathsf{at}))\gamma^i} \\
&= h_0^{r'\omega f_1^i(\gamma) + \beta_0 f_2^i(\gamma)} \\
h^{(r-\beta)\gamma^m} &= h_0^{\left((r'\omega\gamma + \beta_0)\gamma^{t-1-|A_S|} \prod_{\mathsf{at} \in A_S} (\gamma + \tau(\mathsf{at})) - \beta\right)\gamma^m} \\
&= h_0^{(r'\omega\gamma + \beta_0)\gamma^{m+t-1-|A_S|} \prod_{\mathsf{at} \in A_S} (\gamma + \tau(\mathsf{at})) - \beta\gamma^m} \\
&= h_0^{r'\omega f_1^m(\gamma) + \beta_0 f_3(\gamma)}
\end{aligned}$$

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 $m+t$ degree at most.
$\beta_0 f_2^i(\gamma)$ is a polynomial in γ with $m+t-2$ degree at most.
$\omega\gamma f_1^m(\gamma)$ is a polynomial in γ with $m+t$ degree at most.
$\beta_0 f_3(\gamma)$ 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.

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 false.

The simulation is completed. The correctness of simulation is analyzed as follows.

There is no abortion during the simulation for the simulator 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 for 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, we have the simulation is indistinguishable from the real scheme when T is true.

When T is true, we have 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 unformly random and independent from the view of C_1^*, C_2^* such that it is a one-time pad and hence the adversary has no advantage in guessing the chosen bit b. We therefore duduce

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

This completes the proof for theorem. □

4 Discussion

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 $\kappa, h^{\alpha\gamma^i} : \quad i \in [0, m]$ 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 $h^{\kappa\alpha f(\gamma)(\gamma+d)}$, note that 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 linear number of exponentiations in the degree of $f(\gamma)(\gamma+d)$.

The main computation in encryption is dominated by $C_2 = h^{\kappa\cdot\alpha \prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))\prod_{d\in\mathcal{D}_{m+t-1-s}}(\gamma+d)}$ in the scheme [10] compared to $C_2 = h^{\kappa\cdot\alpha\prod_{\mathsf{at}\in S}(\gamma+\tau(\mathsf{at}))}$ in our scheme. Based on the above analysis, our encryption time is liner in the number of s while the scheme in [10] is linear in the number of m, where m is the upper bound of all choice s. The corresponding decryption is also different and ours will be much faster. The detailed efficiency is provided in the following table.

4.2 Efficient Threshold Change

Another benefit of our encryption is the dynamic choice of threshold number t after the selection of attribute set S. In our scheme, upon receiving the set S, the encryptor can complete most of exponentiations. Once the threshold number t is given, only two exponentiations are required. While in [10], both S and

Schemes	Herranz et al. [10]	Ours
Encryption	$m + t + 1$ exponentiations	1 pairing and $s + 3$ exponentiations
Decryption	3 pairings and $O(t^2 + m)$ exponentiations	2 pairings and $O(t^2 + s)$ exponentiations

Table 2. Comparison of two Threshold ABE with Constant-Size Ciphertexts. 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. 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.

t must be provided, otherwise, the encryptor cannot perform C_2 computation. This property allows the encryptor to flexibly change the threshold during the application. More precisely, given a ciphertext for (S, t) and the random number κ, the encryption can quickly change it into (S, t') for any t' with two exponentiations.

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. The scheme has nice feature, namely there is no necessity to change any of the user's private keys due to any addition or removal of the attributes. Additionally, the public key size is linear in the upperbound of the selected attribute set in the encryption phase. Unfortunately, this work makes use of dummy attributes in their construction, which leads to inefficiency. In this work, we proposed a novel approach to achieve a constant-size threshold ABE *without dummy attributes*. We also retain the nice features offered by the previous scheme. We make 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, threshold number can be decided after the selection of the attribute set in the encryption phase.

References

1. N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols. Attribute-based encryption schemes with constant-size ciphertexts. *Theor. Comput. Sci.*, 422:15–38, 2012.
2. J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*, pages 321–334. IEEE Computer Society, 2007.
3. D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based encryption with constant size ciphertext. In Cramer [6], pages 440–456.
4. C. Chen, J. Chen, H. W. Lim, Z. Zhang, D. Feng, S. Ling, and H. Wang. Fully secure attribute-based systems with short ciphertexts/signatures and threshold

access structures. In E. Dawson, editor, *Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, San Francisco,CA, USA, February 25-March 1, 2013. Proceedings*, volume 7779 of *Lecture Notes in Computer Science*, pages 50–67. Springer, 2013.

5. L. Cheung and C. C. Newport. Provably secure ciphertext policy ABE. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*, pages 456–465. ACM, 2007.
6. R. Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.
7. C. Delerablée and D. Pointcheval. Dynamic threshold public-key encryption. In D. Wagner, editor, *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 317–334. Springer, 2008.
8. A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts. In W. Susilo, Y. Mu, and J. Seberry, editors, *Information Security and Privacy - 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9-11, 2012. Proceedings*, volume 7372 of *Lecture Notes in Computer Science*, pages 336–349. Springer, 2012.
9. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, *Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006*, pages 89–98. ACM, 2006.
10. J. Herranz, F. Laguillaumie, and C. Ràfols. Constant size ciphertexts in threshold attribute-based encryption. In P. Q. Nguyen and D. Pointcheval, editors, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, volume 6056 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2010.
11. A. B. Lewko and B. Waters. Unbounded HIBE and attribute-based encryption. In K. G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 547–567. Springer, 2011.
12. A. Sahai and B. Waters. Fuzzy identity-based encryption. In Cramer [6], pages 457–473.

Appendix

A Analysis of Hard Problem

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

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

and group elements

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

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

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

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

To prove our assumption is a (P, Q, F)-GDHE assumption, 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 below set R which can generate F.

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

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 $(q+t)$-degree at most polynomial in γ and $B(\gamma)$ is an $(m+t-2)$-degree at most polynomial in γ. 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 deduce

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

The degree of $B(\gamma)$ is $m+s-2$ at most, such that the left polynomial cannot be equivalent to zero. Therefore, the above equation implies 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 $d_A = q - 1$.

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. We therefore yield the theorem. □