Fuzzy Identity Based Encryption with a flexible threshold value

Sedigheh Khajouei-Nejad
Department of Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran
se_khajouei_nejad@yahoo.com

Sam Jabbehdari
Department of Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran
Sam.Jabbehdari@iau.ac.ir

Hamid Haj Seyyed Javadi
Department of Mathematics and Computer Science, Shahed University, Tehran, Iran
h.s.javadi@shahed.ac.ir

Seyed Mohammad Hossein Moattar
Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran
moattar@mshdiau.ac.ir

***Abstract*— The issue of data and information security on the internet and social network has become more serious and pervasive in recent years. Cryptography is used to solve security problems. However, message encryption cannot merely meet the intended goals because access control over the encrypted messages is required in some applications. To achieve these requirements, attribute-based encryption (ABE) is used. This type of encryption provides both security and access structure for the network users simultaneously. Fuzzy Identity-Based Encryption (FIBE) is a special mode of ABE that provides a threshold access structure for the users. This threshold value is set by the authority for users, which is always fixed and cannot be changed. So, the sender (encryptor) will not play a role in determining the threshold value. The mentioned issue exists also in Key Policy Attribute Based Encryption (KP-ABE) schemes. In this paper, we present a FIBE scheme in addition to the authority, the sender also plays a role in determining the threshold value. Thus, the policy will be more flexible than previous FIBE schemes in that the threshold value is selected only by the authority. We can call the proposed scheme a dual-policy ABE. The proposed technique for flexibility of threshold value can be applied in most of the existing KP-ABE schemes. We use the (indistinguishable) selective security model for security proof. The hardness assumption that we use is the modified bilinear decision Diffie-Hellman problem.**

Keywords*— *Attribute-based encryption (ABE), Secret Sharing multiplication, Fuzzy Identity-Based Encryption (FIBE), fine-grained access policy, Access structure, Dual-policy ABE, Threshold value flexibility

I. Introduction

The simultaneous provision of information security, as well as the application of access control on the messages of different networks, is one of the most widely used topics in cryptography. We declare the importance of this topic by an instance. Suppose that a patient wants to send his/her health information to a doctor who works at a special hospital H. In the classic encryption methods, the patient has to be familiar with a doctor and has his public key. Then he/she should encrypt the health information with this key and send it to the doctor. This method has some problems in big networks. Because the network users have to be familiar with all of the other users. Also, the users have to learn a lot of keys from other users. So, applying access control to the encrypted data based on users' attributes can be solved this problem. In this approach, called Attribute-Based Encryption (ABE), knowing the user's ID and the related key is not required for encryption. Because the users are described with a set of attributes. Therefore, the sender only should encrypt the message by these attributes. This approach can be very effective. For instance, in the mentioned example, this is enough that the sender encrypts his message by attributes doctor and hospital H. While this approach is really useful, it has some challenges in the real world. The first and most obvious one is creating a strong fine-grained access structure. This means that we can choose any set of users to select and send messages to. In some schemes, this has not been completely solved. This issue is evident in [1] which uses a single Threshold gate as an access structure. This special type of ABE is called Fuzzy Identity Based Encryption (FIBE). We want to improve this scheme to reach a stronger fine-grained access structure than the original scheme. Computational complexity is another challenge in ABE area. We improve the [1] scheme without forcing extra computational or communication overhead. Recently, some papers like [2], [3], and [4] tried to reduce the complexity of ABE schemes. The concept of Fuzzy IBE is presented in the next for better discussion.

In Fuzzy IBE schemes like [1] users' private keys are generated related to their attributes, i.e., a user as a receiver has a set of attributes like ω. Now suppose that a sender encrypts a message with a number of attributes shown as ω' set. Now, if a receiver's attribute set ω is close enough to the set of attributes ω', the receiver is able to decrypt the message. This means that the number of attribute intersections(subscriptions) of receiver and ciphertext is greater than a threshold. To this end, a threshold value d is defined by the authority and if the condition $|\omega \cap \omega'| \geq \mathrm{d}$ holds, the user as a receiver will be able to decrypt.

In the following, we want to express the weakness of fine-grained access structure in Fuzzy IBE schemes especially in [1].

Fuzzy IBE scheme problems: In a fuzzy IBE scheme like [1], the access structure is not fully fine-grained. Suppose that data user u has an attribute set ω, the threshold value is d and the sender has selected attribute set ω'. The data user u receives the encrypted data. If the condition $|\omega \cap \omega'| \geq d$ holds, the user u can decrypt. Now suppose that the sender's goal is to prevent this user from decrypting. In scheme [1], the sender just can reduce the attribute set ω' which can cause the sender's target attributes not to be completely selected and other legible users may not be able to decrypt as well. For instance, suppose that there is a user his/her access policy is a threshold gate, as shown in figure 1. The sender encrypts a message by applying attribute set $\{A, B, C, E\}$. Regarding figure 1, this is clear that this user can decrypt the sender's message. Because his/her access policy is the threshold gate. The threshold value is 2 from 4 input attributes. Inputs of this gate is $\{A, B, D, F\}$ attributes. According to ciphertext attributes, this is clear that the attributes of A and B are the intersections. Therefore, this user is legal to decryption. In this example, the sender wants to ban this user's access. In previous schemes like [1], [5], [6] and [7] sender should remove some attributes in ciphertext to decrease the number of intersections. Generally, a sender cannot modify the access policy in KP-ABE schemes (e.g., [8]). In this scenario, our purpose is that sender can ban this user 's access without removing any attribute in the ciphertext. The previous schemes cannot act like this. Therefore, in these schemes, the sender cannot make a fine-grained access structure. If the sender can increase the threshold value to 3, can ban this user 's access. This is the contribution of our paper. This means that if the authority has selected the threshold as 2 and the sender chooses 1 then the total threshold value will be 3. In fact, in previous Fuzzy IBE schemes, the threshold value (for one user) is selected once and for all and remains constant. Lack of flexibility in selecting threshold will cause the above problem. Thus, we are going to solve these problems in our scheme by using the Secret sharing polynomials multiplication technique adapted from [9], and [10]. Our scheme also can be dual-policy ABE. Because authority and sender select the threshold value together. As we claimed before, the proposed technique can use in most KP-ABE schemes like [5] and [11]. In fact, if our technique is used in KP-ABE schemes, the sender can increase all threshold values at the gates in start of the circuit (leaf nodes of the access tree).

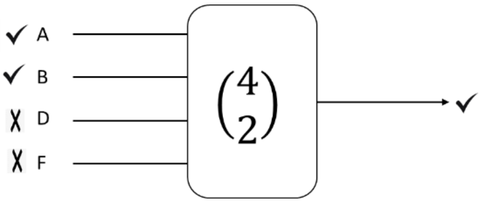

Figure 1: user's access policy (Threshold gate)

In our scheme, the threshold value is divided into two parts. One part is placed on the key by the authority and the other part is selected by the sender and placed in the ciphertext. In the end, the total threshold will be the sum of two initial thresholds. Therefore, the threshold value will no longer be fixed and it may increase during encryption. Thus, the threshold value will be flexible. For this purpose, we used a method called the multiplication of shares in Shamir's secret sharing. This technique can be used in KP-ABE designs such as [5] and [11].

The paper structure: The paper structure is as follows: In the following, the literature review and related works are presented in section II. We will introduce mathematical prerequisites and ABE basic requirements as preliminary in section III. Then we will present our intended scheme in section IV. The scheme's security proof and efficiency comparison with [1] are also included in section V. Finally, we proposed a conclusion in section VI. Note that you can find the published version of this work at [12].

II. RELATED WORKS

Sahai and Waters first introduced fuzzy IBE in [1]which led to the emergence of ABE. This scheme used only one threshold gate. As mentioned before, in this scheme sender selects a set of attributes and encrypts the message. The receivers can decrypt the message if they have enough of the sender's intended attributes, i.e., the number of the sender's desired attributes and receiver's attributes is more than a predefined threshold. That is why it is also called threshold encryption. This scheme supports only one threshold gate while by applying the access structures that combine logical gates or in general multiple threshold gates, we can achieve a stronger fine-grained access structure. Therefore, the goal is to apply the more complex access structure (like Boolean functions) to the schemes. To this end, Goyal et al. [5] proposed a scheme to apply a monotone access structure and also introduced the concept of Attribute Based Encryption (ABE). In this scheme, policy (the access structure) is applied to the users' key. This means that an access structure is selected and applied by the authority in the key generation phase. This scheme is known as key policy attribute-based encryption (KP-ABE). After that, Bethencourt et al. [13] presented a scheme in which the access policy was applied in the ciphertext. Unlike KP-ABE, in the scheme [13], the access structure is selected and applied by the sender in the encryption phase. These schemes are called Ciphertext policy attribute-based encryption (CP-ABE). Scheme [14] proposed a CP-ABE scheme that solved some of the problems and limitations in [13]. Recently, [15] proposed a CP-ABE scheme that supports the hierarchical architecture. This scheme is fully distributed which affords a high level of scalability. With increasing the number of users in a system, communication networks may encounter scalability challenges. Additionally, another type of ABE proposed in [16] is called dual-policy ABE (DP-ABE). In DP-ABE, policy-making is placed both in the users' private keys and also in the ciphertext. In fact, in this type of ABE, both the authority and the sender will be involved in policy-making.

As mentioned previously, access structure is usually defined as a Boolean function, regardless of where it is applied either in the key or the ciphertext. If AND, OR, and threshold gates are used in this function, it is called a monotone access structure. The exact definition of monotone access structure can be found in [5] and [13]. Meanwhile, if, in addition to the mentioned gates, the NOT gate is used in the access structure, it is called a non-monotone access structure. Ostrovsky et al. proposed the first ABE scheme in [17] that supports a non-monotone access structure. There are also some schemes such as [18], [19], and [20] that use mathematical functions as access structures.

As we mentioned before one of the most important problems in ABE schemes is computational complexity. One of the techniques to solve this problem is outsourcing. Green presented the outsourced Attribute-Based Encryption in [21] for the first time. This technique reduces the computational overhead on the part of users and the third party performs the calculations instead. Cloud is usually used as a third party. To reduce the complexity of decryption, [22] introduced a precomputation technique. Also, [23] used a trade-off between granularity and complexity. There are some other problems in ABE areas like key-escrow, communication overhead, revocation, and efficiency problems. Key-escrow problem is a common issue in networks. [24] presented a first multi–Authority ABE scheme. Recently the schemes in [25], [26] and [27] tried to solve the key escrow problem. The schemes in [28] and [29] tried to solve the communication overhead problem by presenting a scheme that the size of ciphertext is constant. In other schemes, the size of ciphertext is increased by increasing the number of used attributes or the depth of the circuit as an access structure. Revocation of user or attribute is the other problem that [30] presented a scheme to solve this problem. In this regard, [31] proposed a Revocable Storage ABE scheme. In addition, [32] proposed a Puncturable ABE scheme that can provide decryption revocation. There are some new papers like [33] and [34] that focused on solving this problem. The schemes in [35] and [36] focused on efficiency and presented an ABE scheme for practical uses.

III. Preliminary

In this section, some definitions and preliminaries, which we will use in our scheme, are proposed. This section includes the definition of Flexible Fuzzy IBE (as an ABE scheme), selective security model for KP-ABE, secret sharing schemes, bilinear pairing map and, hard problem assumption.

A. *Flexible Threshold Fuzzy Identity-Based Encryption*

Each Fuzzy IBE and ABE scheme has four algorithms: Setup, Key Generation, Encryption, and Decryption algorithms. We show these algorithms as **Setup**, **KeyGen**, **Enc** and **Dec** respectively. Setup and key generation algorithms are run by the authority. The encryption algorithm is run by the sender (data owner) and the decryption algorithm is run by the receiver (data user). Now, we define these algorithms for our schemes.

Setup ($\boldsymbol{\lambda}, \boldsymbol{U}$): This algorithm receives the security parameter λ and the set of all attributes U, then generates a master secret key (MSK) and public keys (PK). MSK has to be kept safe and PK announce for all network members. The number of all attributes is $n = |U|$.

KeyGen ($\boldsymbol{MSK}$,$\boldsymbol{d_1}$,$\boldsymbol{\omega}$): This algorithm gets the master secret key MSK, first-threshold value $\boldsymbol{d_1}$ and the attribute set $\omega \subseteq U$ as the inputs and generates the user's secret key (SK).

Enc (M, PK, $\boldsymbol{d_2}$, $\boldsymbol{\omega'}$): This algorithm gets the public key PK, the second threshold value d_2, the intended message (M), and the attribute set $\omega' \subseteq U$ as the inputs and generates the ciphertext E corresponding to ω' and the message M.

Dec ($\boldsymbol{E}, \boldsymbol{SK}$): This algorithm gets the secret key SK that is related to the attribute set ω as well as the ciphertext E that is related to the attribute set ω'. If $|\omega \cap \omega'| < \mathrm{d}_1 + d_2$ holds, the algorithm outputs ⊥, otherwise, this algorithm recovers message M and declares it as output.

B. Selective Security model

Considering that we will prove our scheme security in the selective security model, we will describe this model in this section. This model includes several phases and steps that are executed between adversary and challenger as a game. This game will be explained in the following.

Initialization: The adversary first identifies a challenging attribute set α and the value of d_2 and sends them to the challenger.

Setup: The challenger runs the setup algorithm and sends the public keys to the adversary.

Phase 1: The adversary is allowed to select attribute set γ_j and send a query for private keys of γ_j as long as $|\alpha \cap \gamma_j| < d_1 + d_2$ holds for all j.

Challenge: The adversary selects two messages $M_0$and M_1 and submits them to the challenger. Then the challenger selects a random bit b and encrypts M_b with challenge attribute set α.

Phase 2: Phase 1 is repeated.

Guess: The adversary guesses which message is encrypted. We show the adversary guess by b'. If the adversary detects the intended bit with a probability of more than $\frac{1}{2}$, it can win this game.

C. Secret sharing

Assume that we want to share a secret among several entities. Each entity is given a secret share none of them cannot compute the secret value. This is possible if a number enough entities cooperate with each other. The most important secret sharing scheme is Shamir's scheme which operates like a threshold gate. In this scheme, if a secret is shared among n entities and if there are t or more of these entities, the secret can be recovered. The scheme can be generalized to any access structure. In this scheme, we must have at least t points of a polynomial of $t - 1$ degree to recover it. To share secret s among n entities with t threshold (it is called t of n scheme and $t \leq n$) first a random polynomial $q(x)$ of $t - 1$ degree is selected which $q(0) = s$. Each entity i, that $1 \leq i \leq n$, is given $(i, q(i))$. Lagrange coefficients are used to recover the value of s secret. The Lagrange coefficient function can be calculated as follows.

$$\Delta_{i.S}(x) = \prod_{j \in S\ .j \neq i} \frac{x - j}{i - j} \qquad ,\forall\ i \in S \tag{1}$$

$$L_i = \Delta_{i.S}(0) = \prod_{j \in S\ .j \neq i} \frac{-j}{i - j} \tag{2}$$

where S is the desired set of shares of different t entities. The following formula is used to recover the share value $q(0) = s$.

$$q(0) = \sum_{i \in S} q(i) \cdot L_i \tag{3}$$

This is a threshold function. Note that AND and OR gates can be generated using this function.

1) Secret sharing polynomials multiplication

In this subsection, we will discuss the relations of the multiplication of the shares related to two Shamir secret sharing schemes adapted from [9], and [10] i.e., we have two different polynomials for two different secrets. We conclude that multiplying these shares is equivalent to multiplying these two polynomials. In the following, we will examine this method. Suppose we have n entities $P_1, \dots, P_n$. We have the polynomial $q(x)$ of degree $d_1 - 1$ that

$d_1 < n$ and the secret of this polynomial is $q(0) = s_1$. Some of the secret shares are allocated to the above entities as $P_i \leftarrow (i, q(i))$; $1 \le i \le n$. This relation indicates that the entity P_i receives $(i, q(i))$. Thus, with d_1 participants from n available entities, the secret s_1 can be recovered. Now suppose we have a polynomial $p(x)$ of the degree d_2 that its secret is $p(0) = s_2$. Some secret shares are allocated to the above entities as $P_i \leftarrow (i, p(i))$; $1 \le i \le n$. Now if we multiply the previous shares (i.e., $P_i \leftarrow (i, q(i).p(i))$; $1 \le i \le n$) then interpolate, it equals to the polynomial product of $h(x) = q(x).p(x)$ with the secret $h(0) = q(0)p(0) = s_1 s_2$. The degree of the obtained polynomial is $d_1 + d_2 - 1$. If the condition $d_1 + d_2 < n$ holds, it can be considered that the secret sharing is performed for $h(x)$. So, the secret of the polynomial product will be recovered with at least $d_1 + d_2$ participants.

It should be noted that the degree of the first polynomial is $d_1 - 1$, the second one is d_2 and the threshold value for their product is $d_1 + d_2$.

D. *Bilinear pairing map*

A symmetric bilinear pairing map is a mapping from two elements of one group to an element from a second group. So bilinear pairing map, which is shown by e, can be defined as $e: G_1 \times G_1 \rightarrow G_T$. Discreet logarithm problems must be hard in each group, to ensure security in the encryption applications. The main feature of this mapping is its bilinear form. So, if g is the generator of the group $G_1$and the size of group q is a large prime number and also $a, b \in \mathbb{Z}_q$ then we have:

$$e(g^a, g^b) = e(g, g)^{ab}$$

By this definition, the element $e(g, g)$ will be the generator of group G_T. Therefore, the relation $e(g, g) \neq 1$ must hold for the function to work properly. Note that the complexity of a pairing operation is heavier than the exponentiation [37].

E. *Modified decisional bilinear Diffie-Hellman problem*

Suppose that there exists the bilinear pairing map $e: G_1 \times G_1 \rightarrow G_2$. If the vector $(g^a, g^b, g^c, e(g, g)^z)$ is given, distinguishing whether z is equal to ab/c or not, is known as the Modified decisional bilinear Diffie-Hellman (MDBDH) problem. We assume that this problem is hard and the adversary normally with $\frac{1}{2} + negl$ probability is able to solve this problem. Here, $negl$ means negligible. The list of some hard problems related to pairing can be found in [38].

IV. OUR SCHEME

As aforementioned, we will provide a scheme in this section that is used for the threshold access structure. This threshold value is jointly selected by the authority in the key generation algorithm and the sender in the encryption algorithm. The threshold defined by the authority is called the first threshold d_1 and the threshold defined by the sender is called the second threshold d_2. The first threshold is fixed and will not change but the second threshold will be selected for each encryption. This allows the threshold to be flexible. Regarding ABE, it is interpreted that each user is defined by a set of attributes ω and has the private keys corresponding to these attributes. The sender encrypts the message using a number of attributes represented as ω'. Now if the message receiver is close enough to the attribute set of the ciphertext, it is able to decrypt. The criterion for being close to the ciphertext attributes is the threshold value. In other words, if the condition $|\omega \cap \omega'| \ge \mathrm{d}_1 + d_2$ holds, the recipient user will be able to decrypt. Our proposed technique to increase the threshold value can execute in many KP-ABE schemes like [5] and [11] as well. We explain the algorithms of this scheme in the following.

Setup ($\boldsymbol{\lambda}$, U): The group G_1 that is of p order is selected where g is the group generator. Also, a bilinear pairing map e is selected as $G_1 \times G_1 \rightarrow G_T$. The set $\{G_1, G_T, g, e\}$ is known as pp public parameters. It is assumed that these parameters are available in the public key PK. The security parameter λ is the input of this algorithm. This algorithm randomly selects the values $t_1, \ldots, t_{|U|}$from the set $\mathbb{Z}_p$. Then it randomly selects the value y from the set $\mathbb{Z}_p^*$. The master secret key is as follows.

$$MSK: t_1, \ldots, t_{|U|}, y$$

Moreover, the public keys are published as follows.

$$\mathrm{PK}: \mathrm{T}_1 = \mathrm{g}^{\mathrm{t}_1}, \dots, \mathrm{T}_{|\mathrm{U}|} = \mathrm{g}^{\mathrm{t}_{|\mathrm{U}|}}, \mathrm{Y} = \mathrm{e}(\mathrm{g}, \mathrm{g})^{\mathrm{y}}$$

KeyGen (*MSK*,$\boldsymbol{d_1}$,$\boldsymbol{\omega}$): This algorithm selects a polynomial function $q(x)$ with one degree less than the threshold value d_1. So, this polynomial is of $d_1 - 1$ degree and this polynomial is selected randomly so that $q(0) = y$. The user's secret key will be as follows.

$$SK: D_i = g^{\frac{q(i)}{t_i}} ; i \in \omega$$

Enc (M, PK, $\boldsymbol{d_2}$, $\boldsymbol{\omega'}$): This algorithm chooses a random value s from the set $\mathbb{Z}_p^*$. Then a polynomial $p(x)$ of d_2 degree is selected so that the relation $p(0)$=s holds. The ciphertext will be as follows.

$$E = \left\{d_2, \omega', E' = M.Y^s, \left\{E_i = T_i^{p(i)}\right\}_{i \in \omega'}\right\} \qquad (4)$$

Dec (*E*, *SK*): Suppose that the receiver user has the secret key SK associated with the set of attributes ω. This receiver can decrypt E if the condition $|\omega \cap \omega'| \geq d_1 + d_2$ holds. If it does not hold, the algorithm output $\perp$. For decrypting, the receiver selects the set S including $d_1 + d_2$ members from $|\omega \cap \omega'|$. The decryption will be as follows.

$$M = \frac{E'}{\prod_{i \in S}\left(e(D_i, E_i)\right)^{\Delta_{i,S}(0)}} \qquad (5)$$

In equation 5, $\Delta_{i,S}(0)$ is the Lagrange coefficient. The correctness of relation 5 to recover the message M can be proved as follows.

$$\frac{E'}{\prod_{i \in S}\left(e(D_i, E_i)\right)^{\Delta_{i,S}(0)}} = \frac{M.e(g,g)^{ys}}{\prod_{i \in S}\left(e\left(g^{\frac{q(i)}{t_i}}, g^{p(i).t_i}\right)\right)^{\Delta_{i,S}(0)}}$$

$$= \frac{M.e(g,g)^{ys}}{\prod_{i \in S}\left(e(g,g)^{q(i).p(i)}\right)^{\Delta_{i,S}(0)}} = \frac{M.e(g,g)^{ys}}{e(g,g)^{\sum_{i \in S} q(i).p(i)\Delta_{i,S}(0)}}$$

$$= \frac{M.e(g,g)^{ys}}{e(g,g)^{ys}} = M$$

As you can see, if the condition $|\omega \cap \omega'| \leq \mathrm{d}_1 + d_2$ does not hold, the set S cannot be defined. Therefore, it is not possible to recover the message using relation 5.

V. Security and efficiency evalution

In this section, we will prove our scheme security by using the selective security model and assuming the hardness of the modified bilinear decision Diffie-Hellman problem. Also, we will compare our scheme with the [1] scheme and conclude that our scheme's computational complexity and communication overhead are almost the same as [1].

A. *Security proof*

We assume that the challenger wants to answer the modified bilinear decision Diffie-Hellman problem by having the parameters of $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^z)$. We also assume that there is an adversary $\mathcal{A}$ that can break our scheme with $\frac{1}{2} + \varepsilon$ probability where ε is non-negligible. The challenger must use the adversary response to solve the modified bilinear decision Diffie-Hellman problem. If this is possible, considering that it is a difficult problem and cannot be solved, we will conclude that there is not an adversary like $\mathcal{A}$ to break our scheme. To this end, we run the phases of the selective security model.

Initialization: Adversary $\mathcal{A}$ first identifies the attribute set of challenge α and the value of d_2.

Setup: the challenger simulates the setup algorithm for the adversary and sets $Y = e(g, A) = e(g,g)^a$. Additionally, it selects the random value $\beta_i \in \mathbb{Z}_p$ for each $i \in \alpha$ and sets $T_i = C^{\beta_i} = g^{c\beta_i}$. It selects the random value $\omega_i \in \mathbb{Z}_p$ for each $i \in U - \alpha$ and sets $T_i = g^{\omega_i}$. So, the public parameters are selected and given to the adversary.

Phase 1: The adversary selects attribute set γ that $|\alpha \cap \gamma| < d_1 + d_2$ and sends it to the challenger. The challenger should generate secret keys related to γ. We will first define the sets Γ, Γ' and S for each attribute set γ that $|\alpha \cap \gamma| < d_1 + d_2$ as follows:

$$S = \Gamma' \cup \{0\} \text{ and } \Gamma \subseteq \Gamma' \subseteq \gamma; \ |\Gamma'| = d_1 - 1 \text{ and } \Gamma = \gamma \cap \alpha$$

Challenger generates private keys D_i for all $i \in \Gamma'$ as follows:

- If $i \in \Gamma$: the random value $s_i \in \mathbb{Z}_p$ is selected and $D_i = g^{s_i}$ is set.
- If $i \in \Gamma' - \Gamma$: the random value $\lambda_i \in \mathbb{Z}_p$ is selected and $D_i = g^{\frac{\lambda_i}{\omega_i}}$ is set.

In order to select a polynomial q(x) of degree $d_1 - 1$, we can randomly select $d_1 - 1$ points and $q(0) = a$ is set as well. According to our scheme and the above, we have $q(i) = c\beta_i s_i$ for $i \in \Gamma$ and $q(i) = \lambda_i$ for $i \in \Gamma - \Gamma'$.

The challenger, regarding that it knows the discreet logarithm associated with $T_i\,; i \notin \alpha$ $(\text{i.e.}, \omega_\text{i})$, can do the following to calculate the key $D_i; i \notin \Gamma'$.

$$i \notin \Gamma': D_i = \left(\prod_{j\in\Gamma} C^{\frac{\beta_i s_i \Delta_{j,S}(i)}{\omega_i}}\right)\left(\prod_{j\in\Gamma'-\Gamma} g^{\frac{\lambda_i . \Delta_{j,S}(i)}{\omega_i}}\right) A^{\frac{\Delta_{0,S}(i)}{\omega_i}}$$

The challenger by using interpolation was able to calculate $D_i = g^{\frac{q(i)}{t_i}} : i \notin \Gamma'_i$ where $q(x)$ was created using $d_1 - 1$ value of $D_i; i \notin \Gamma'$ and one value of $A = g^a$. So, the private keys corresponding to γ were generated.

Challenge: The adversary selects the two messages M_0 and M_1 and sends them to the challenger. The challenger selects the random bit v and encrypts the message M_v with the challenge attributes α as follows.

To encrypt, it first selects the polynomial $p'(x)$ of degree d_2 that $p'(0) = 1$ holds. The ciphertext is generated as follows.

$$E = \left\{d_2, \omega', E' = M_v . Z, \left\{E_i = B^{p'(i)\beta_i}\right\}_{i\in\omega'}\right\}$$

If $z = \frac{ab}{c}$ we assume that $r' = \frac{b}{c}$ and we have $E' = M_v . e(g,g)^{\frac{ab}{c}} = M_v . e(g,g)^{ar'} = M_v . Y^{r'}$ and $E_i = B^{p'(i)\beta_i} = g^{p'(i)b\beta_i} = g^{p'(i)\frac{b}{c}c\beta_i} = g^{p(i)c\beta_i} = T_i^{p(i)}$.

In the above relation, $p(x) = \frac{b}{c}p'(x) = r'p'(x)$ holds where $p(x)$ is a polynomial of d_2 degree and $p(0) = r'$. So, the challenger has been able to simulate the ciphertext for M_v.

Now if z is a random value, E' will be completely random.

Phase 2: Phase 1 is repeated.

Guess: in this phase, the adversary guesses bit v'. If $z = \frac{ab}{c}$, the adversary's success probability (i.e., $v' = v$) will be $\frac{1}{2} + \epsilon$ because we assumed that the adversary with $\frac{1}{2} + \epsilon$ probability and non-negligible ϵ can identify the encrypted bit v for our scheme. If z is random, the adversary's success probability (i.e.,$v' = v$)) will be $\frac{1}{2}$.

Considering that the challenger receives the value v', if $v' = v$, it is assumed that $z = \frac{ab}{c}$ holds and if $v' \neq v$, it is assumed that z is random. Thus, the challenger can solve the BDMDH problem. Now we calculate the success probability of the challenger ($P(Ch)$).

$$\text{P}(Ch) = \frac{1}{2}\text{P}\left(v' = v \middle| z = \frac{ab}{c}\right) + \frac{1}{2}\text{Pr}\left(v' = v \middle| z \in_r \mathbb{Z}_p\right)$$
$$= \frac{1}{2}\left(\frac{1}{2} + \epsilon\right) + \frac{1}{2}\left(\frac{1}{2}\right) = \frac{1}{2} + \frac{\epsilon}{2}$$

Since we assume that ϵ is non-negligible, $\frac{\epsilon}{2}$ will be non-negligible as well. Then the challenger can solve the BDMDH problem. But this contradicts our assumption since we assume that no algorithm can break this problem. So, there is also no adversary like $\mathcal{A}$ to be able to break our scheme.

B. *Comparison with previous scheme*

In the proposed scheme, the sender can interfere with the threshold value or access policy unlike previous ones (e.g., [1], [5], and [11]). The proposed scheme captures this feature without applying more complexity compared to previous schemes. In this subsection, we show that using of secret sharing polynomials multiplication technique does not force any extra computation and communication overhead compared to the original version.

We compare our scheme with [1] (and also [5] and [11] by supposing that our technique is applied to them) in four algorithms, i.e., setup, key generation, encryption, and decryption. We consider the computational complexity and the ciphertext size, which is directly related to communication overhead, in our comparison.

Setup: The algorithm of setup in our scheme is exactly the same as the algorithm of setup in [1] and [5] (and very similar to [11]). So, the computation complexity and the size of the public key are the same. The public key in [11] also includes extra two Hash functions H_1 and H_2.

KeyGen: The algorithm of key generation in our scheme is exactly the same as the algorithm of setup in [1] (and [5], and [11] with some minor differences). So, the computation complexity and the size of the secret key are the same.

Enc: The differences between encryption algorithm in our scheme and the schemes of [1], [5], and [11] are that there is extra d_2 in equation (4) and also is computed $\left\{\mathrm{E_i} = \mathrm{T_i^{p(i)}}\right\}_{\mathrm{i}\in\omega'}$ instead of $\{\mathrm{E_i} = \mathrm{T_i}^{s}\}_{\mathrm{i}\in\omega'}$. This means that the communication overhead (size of ciphertext) of our scheme has an extra element named d_2. This can be managed by adding at most 8 bits in the ciphertext. Because this element represents the second threshold value which is a small number. So, we can ignore it. Also, the computational complexity of the encryption algorithm in our scheme is the same as mentioned schemes. Note that in our scheme **Enc** algorithm should select a polynomial $p(x)$ and also computes $\{\mathrm{p(i)}\}_{\mathrm{i}\in\omega'}$ which these computations are negligible. So, we can claim that the computational complexity and communication overhead are almost the same as mentioned schemes. While in [11] the sender computes $E' = H_2(Y^{s.H_1(m)})$ instead of $E' = M.Y^s$, but the computation complexity and the size of ciphertext are the same as the proposed scheme.

Dec: The decryption algorithm of our scheme is exactly the same as the decryption algorithm of [1] and the decryption node algorithm in [5], and [11] supposing that $d = d_1 + d_2$. This affects choosing of the intersection set S. However, the decryption operations are the same.

Therefore, we can conclude that using the secret sharing polynomials multiplication technique does not force extra computation complexity, size of keys, and ciphertext.

VI. Conclusion

In this paper, we have proposed the idea of multiplication of the shares associated with Shamir's secret sharing scheme to make the threshold value flexible in FIBE and KP-ABE schemes. In this regard, we presented a new FIBE scheme with a flexible threshold. Considering that in our scheme the access structure (Threshold gate) is applied to both the key and the ciphertext. In fact, one threshold value is applied in keys and another one is applied in the ciphertext. In the other words, part of the threshold value is determined by the authority in the key generation algorithm and the other part is determined by the sender in the encryption algorithm. The threshold selected by the authority is always fixed but the threshold associated with the sender is changeable for each encryption. Therefore, our scheme is more flexible than Sahai and Waters's scheme [1]. The total threshold value is the sum of them. To this end, we have used the idea of multiplication of the shares associated with Shamir's secret sharing scheme. This flexibility does not lead to any additional computational and communication overhead (other than the value d_2 in the ciphertext) compared to the scheme [1]. In other words, our scheme, while providing a flexible scheme, has the same computational and communication overhead as the previous one [1]. We also look at the drawbacks of the scheme [1] that may occur in a network. Our scheme solved these problems. These flexibility techniques and dual-policy can also be applied to improve the existing KP-ABE scheme e.g., [5], [11], or others. Furthermore, we compared the computation complexity, size of keys, and the size of ciphertext of our scheme with [1] and also with [5] and [11] by this assumption that the idea of multiplication of the shares is applied to them.

References

[1] Amit Sahai and Brent Waters, "Fuzzy Identity-Based Encryption," *EUROCRYPT,* Vols. Fuzzy Identity-Based Encryption, no. EUROCRYPT, 2005.

[2] Sana Belguith, Nesrine kaaniche, Giovanni Russello, "PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT," *International Conference on Cloud Computing,* 2018.

[3] Syh-Yuan Tan , Kin-Woon Yeow, and Seong Oun Hwang, "Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things," *IEEE INTERNET OF THINGS JOURNAL,* 2019.

[4] Hang Li , Keping Yu , Bin Liu , Chaosheng Feng , Zhiguang Qin , and Gautam Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS,* vol. 26, 2022.

[5] Vipul Goyal , Omkant Pandey, Amit Sahai, Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *ACM conference on Computer and communications security,* 2006.

[6] Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, "Fuzzy Identity Based Encryption from Lattices," *IACR Cryptol. ePrint Arch.,* 2011.

[7] Sergey Gorbunov, Vinod Vaikuntanathan, Hoeteck Wee, "Attribute-Based Encryption for Circuits," *Journal of the ACM (Association for Computing Machinery),* May 2013.

[8] Y. Sreenivasa Rao, Ratna Dutta, "Computational friendly attribute-based encryptions with short ciphertext," *Theoretical Computer Science,* vol. 668, 2017.

[9] M. M. Oliaee, M. Delavar, M. H. Ameri, J. Mohajeri and M. R. Aref, "On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets," in *2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC),* 2017.

[10] Mehdi Mahdavi Oliaee, Mahshid Delavar, Mohammad Hassan Ameri, Javad Mohajeri, and Mohammad Reza Aref, "On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets," *The ISC International Journal of Information Security (ISeCure),* vol. 10, no. 2, pp. 117-127, 2018.

[11] Yong Yu , Junbin Shi, Huilin Li, Yannan Li, Xiaojiang Du, and Mohsen Guizani, "Key-Policy Attribute-Based Encryption With Keyword Search in Virtualized Environments," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,* vol. 38, 2020.

[12] S. Khajouei-Nejad, S. Jabbehdari, H. S. J. Hamid and S. M. H. Moattar, "Fuzzy Identity Based Encryption with a flexible threshold value," *Journal of Communication Engineering,* vol. 10, no. 2, 2023.

[13] John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption," *IEEE symposium on security and privacy (SP'07),* 2007.

[14] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," *International Workshop on Public Key Cryptography,* 2011.

[15] Ali Mohammad, Javad Mohajeri, Mohammad-RezaSadeghi, Ximeng Liu, "A fully distributed hierarchical attribute-based encryption scheme," *Theoretical Computer Science,* vol. 815, pp. 25-46, 2020.

[16] Nuttapong Attrapadung, Hideki Imai, "Dual-Policy Attribute Based Encryption," *International Conference on Applied Cryptography and Network Security,* 2009.

[17] Ostrovsky, Sahai, Waters, "Attribute-based encryption with non-monotonic access structures," *Proceedings of the 14th ACM conference on Computer and communications security,* 2007.

[18] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, Dhinakaran Vinayagamurthy, "Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits," *Annual International Conference on the Theory and Applications of Cryptographic Techniques,* 2014.

[19] M. MahdaviOliaee and Z. Ahmadian, "Fine-grained flexible access control: ciphertext policy attribute based encryption for arithmetic circuits," *Journal of Computer Virology and Hacking Techniques,* vol. 19, no. 4, pp. 515-528, 2023.

[20] Mahdi Mahdavi Oliaeea, and Zahra Ahmadian, "Ciphertext Policy Attribute Based Encryption for Arithmetic Circuits," *eprint,* 2021.

[21] Green,Matthew , Susan Hohenberger, Brent Waters, "Outsourcing the decryption of abe ciphertexts," *USENIX security symposium* , vol. 2011, 2011.

[22] M. Mahdavi, M. H. Tadayon, M. S. Haghighi and Z. Ahmadian, "IoT-friendly, pre-computed and outsourced attribute based encryption," *Future Generation Computer Systems,* vol. 150, pp. 115-126, 2024.

[23] S. Khajouei-Nejad, H. H. S. Javadi, S. Jabbehdari and S. M. H. Moattar, "Reducing the computational complexity of fuzzy identity-based encryption from lattice," *Cryptology ePrint Archive,* 2024.

[24] M. Chase, "Multi-authority Attribute Based Encryption," *Theory of cryptography conference,* 2007.

[25] Ruyuan Zhanga, Jiguo Li, Yang Lu, Jinguang Han, and Yichen Zhang, "Key escrow-free attribute based encryption with user revocation," *Information Sciences,* vol. 600, 2022.

[26] Er-Shuo Zhuang; Chun-I Fan; and I-Hua Kuo, "Multi-Authority Attribute-Based Encryption with Dynamic Membership from Lattices," *IEEE Access,* 2022.

[27] Xiao Zhang, Faguo Wu, Wang Yao, Zhao Wang, and Wenhua Wang, "Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation," *Concurrency and Computation: Practice and Experience,* vol. 31, 2019.

[28] Nuttapong Attrapadung, Benoˆıt Libert,, and Elie de Panafieu, Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts, 2011.

[29] Attrapadung, Nuttapong, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie De Panafieu, and Carla Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theoretical computer science,* 2012.

[30] Junbeom Hur; and Dong Kun Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems,* vol. 22, 2010.

[31] Lee, Kwangsu and Choi, Seung Geol and Lee, Dong Hoon and Park, Jong Hwan and Yung, Moti, "Self-updatable encryption: Time constrained access control with hidden attributes and better efficiency," *Theoretical Computer Science,* vol. 667, pp. 51-92, 2017.

[32] Priyanka Dutta, Willy Susilo, Dung Hoang Duong, Partha Sarathi Roy, "Puncturable identity-based and attribute-based encryption from lattices," *Theoretical Computer Science,* vol. 929, pp. 18-38, 2022.

[33] Chunpeng Ge , Willy Susilo , Joonsang Baek, Zhe Liu, Jinyue Xia, and Liming Fang, "Revocable attribute-based encryption with data integrity in clouds," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, 2021.

[34] Shijie Deng, Gaobo Yang, Wen Dong, and Ming Xia, "Flexible revocation in ciphertext-policy attribute-based encryption with verifiable ciphertext delegation," *Multimedia Tools and Applications,* 2022.

[35] Zhen Liu, and Duncan S. Wong, "Practical attribute-based encryption: traitor tracing, revocation and large universe," *The Computer Journal*, vol. 59, 2016.

[36] Marloes Venema, Greg Alpár, and Jaap-Henk Hoepman, "Systematizing core properties of pairing-based attribute-based encryption to uncover remaining challenges in enforcing access control in practice," *Designs, Codes and Cryptography*, 2022.

[37] M. M. Oliaiy, M. H. Ameri, J. Mohajeri and M. R. Aref, "A verifiable delegated set intersection without pairing," in *2017 Iranian Conference on Electrical Engineering (ICEE)*, 2017.

[38] M. Mahdavi, S. Khaleghifard and Z. Ahmadian, "New Variations of Discrete Logarithm Problem.," *ISeCure*, vol. 15, no. 3, 2023.