Reducing The Computational Complexity of Fuzzy Identity-Based Encryption from Lattice

Sedigheh Khajouei-Nejad iD
North Tehran Branch, Islamic
Azad University
Tehran, Iran

Hamid Haj Seyyed Javadi iD
Shahed University
Tehran, Iran

Sam Jabbehdari* iD
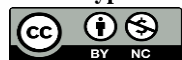North Tehran Branch, Islamic
Azad University
Tehran, Iran

Seyed Mohammad Hossein Moattar iD
Mashhad Branch, Islamic Azad University
Mashhad, Iran

Abstract—**In order to provide access control on encrypted data, Attribute-based encryption (ABE) defines each user using a set of attributes. Fuzzy identity-based encryption (FIBE) is a variant of ABE that allows for a threshold access structure for users. To address the potential threat posed by future quantum computers, this paper presents a post-quantum fuzzy IBE scheme based on lattices. However, current lattice-based ABE schemes face challenges related to computational complexity and the length of ciphertext and keys. This paper aims to improve the performance of an existing fuzzy IBE scheme by reducing key length and computational complexity during the encryption phase. While negative attributes are not utilized in our scheme, we prove its security under the learning with error (LWE) hard problem assumption in the selective security model. These improvements have significant implications for the field of ABE.**

I. INTRODUCTION

The use of information security and access control on network messages is a recurring topic in cryptography. To illustrate the importance of this subject, let us consider a scenario where a patient needs to transmit their health information to a doctor practicing at a specialized hospital. In traditional encryption methods, the patient must have knowledge of the doctor and have access to their public key. The patient would then encrypt the health information with this key and send it over. However, this method becomes problematic in large networks as users must be familiar with all other users and learn multiple keys. Fortunately, applying access control on encrypted data resolves this issue. The recommended approach is to utilize encryption with an access policy such as Attribute Based Encryption (ABE). With ABE, the message is encrypted, and the access structure is applied to the ciphertext. This provides the ability to apply access control to encrypted data, which is particularly important for sensitive data in larger networks. ABE employs an access structure that is commonly defined as a Boolean function.

There are two main groups of ABE schemes: pairing-based and lattice-based [1], [2]. However, the hard problems of number theory and bilinear pairing map can be solved in polynomial time with the advent of quantum computers [3]. Thus, it is crucial that we secure our systems before these computers are built. If quantum computers are developed, most encryption systems based on number theory will no longer provide the necessary security as their hard problems can be easily solved. Therefore, it is advisable to use problems that remain secure against these computers as they emerge. Lattice-related hard problems are one such example that remain hard even for quantum computers [3]. In light of this, it is recommended to use lattice-based techniques, such as ABE and fuzzy IBE, for social networks to ensure their security.

The utilization of lattice in ABE schemes presents three primary concerns: computational overhead, communication overhead, and key length [4], [5]. Addressing these issues is the fundamental challenge in

---

* Corresponding Author

lattice-based attribute-based encryption. The initial lattice-based ABE scheme was introduced in [6], but it suffered from the aforementioned issues. In this study, we aim to resolve these problems by proposing an improved version of the original [6] scheme. However, our solution does not support the NOT gate, unlike the previous iteration.

Our initial and primary focus will be on Agrawal's scheme [6], a post-quantum ABE scheme based on lattice, as we delve into its drawbacks. Subsequently, we will propose a scheme that addresses these limitations. In Agrawal's scheme [6], the access structure only comprises one threshold gate, and negative attributes are utilized in this structure. While this results in a more robust fine-grained access structure, it also increases computational complexity. To mitigate this complexity, we can eliminate negative attributes from the access structure. To compensate for the loss of granularity, we can adopt a tight threshold approach.

A. The paper structure and ideas

The arrangement of the paper will be as follows: Section II will contain a literature review, followed by the introduction of ABE basic requirements in section III. Our intended scheme will then be presented in section IV, while section V will provide the security proof for the scheme. Finally, a summary of all that has been discussed will be presented in section VI.

II. LITERATURE REVIEW

Earlier, we mentioned that ABE schemes fall into two main categories: number theoretic and lattice based. In this section, we first introduced related works in number theoretic ABE schemes and discussed their issues and history. Then, we repeated this process for lattice based schemes.

A. Number theoretic ABE schemes

The concept of ABE first appeared in [7] with the introduction of the Fuzzy Identity-Based Encryption (FIBE) scheme, which was initially only used for a threshold gate. Recent enhancements to this FIBE scheme have been introduced in [8]. Later, in [9], the idea of ABE was further developed with the introduction of key policy attribute-based encryption (KP-ABE), where policy-making was set on users' keys and the access structure was selected and applied by the authority. The value of threshold gates was fixed in both [7] and [9]. More recently, [10] proposed new flexible FIBE and KP-ABE schemes. Another scheme presented in [11] applies the access policy in the ciphertext, with the access structure selected and applied by the sender. These schemes are technically referred to as Ciphertext-policy attribute-based encryption (CP-ABE). Scheme [12] is an important CP-ABE scheme that solves some of the problems presented in [11]. In order to lower the complexity of the decryption process, [13] categorizes attributes into two groups: commonly used attributes and rarely used attributes, subsequently precomputing the commonly used ones.

The access structure, whether applied to the key or ciphertext, is typically defined as a Boolean function using gates such as AND, OR, and threshold gates. This type of function is referred to as a monotone access structure and its precise definition can be found in [9] and [11]. If the NOT gate is included in addition to the previously mentioned gates, it becomes a non-monotone access structure. However, there exist schemes such as [14], and [15] that utilize arithmetic functions as access structures, which are not covered in this paper.

In [16], Green introduced outsourced Attribute Based Encryption, which delegates the computational burden to a third party. This not only reduces the workload for users but also enables other cryptographic fields to benefit from outsourcing, as seen in [17], [18], [19] and [20]. To address issues such as key-escrow, communication overhead, revocation, and efficiency, various schemes have been proposed, including [21], [22], [23], and [24], respectively. There are some papers combine ABE schemes with other technologies like blockchain [25], [26] and Internet of Things (IoT) [27], [28]. The security of proposed schemes is based on Discrete Logarithm family of hard problems. You can see the list of these related problems at [29].

B. Lattice based ABE schemes

Previously, we discussed the significance of transitioning into the post-quantum era. In this section, we will focus on post-quantum ABE schemes. Agrawal et al [6] introduced a lattice-based fuzzy IBE scheme that is an adaptation of [7] with only one threshold gate in the access structure. It can be considered that it is a lattice version of the scheme [7]. However, due to the utilization of a non-monotone access structure, the computational load of the scheme is increased. Zhang [30] presented a lattice-based CP-ABE scheme that utilizes a non-monotone access structure with only one AND gate and can also apply a NOT gate. Boyen [31] proposed a KP-ABE scheme for the access structure of logic circuits that is based on a lattice. However, the security of Boyen's scheme was later shown to be insecure [32]. Following Boyen, Gorbunov et al [33] introduced a KP-ABE scheme that can use any Boolean function as an access structure. Lattice-based ABE schemes such as [34] and [35] offer advantages in performing arithmetic circuits.

Similar to pairing-based ABEs, lattice-based ABE schemes have been enhanced through several approaches. For example, [36], [37], [3], and [5] were devised to address key escrow, heavy computation (through outsourcing), revocation, and efficiency problems.

III. DEFINITION AND SECURITY MODEL Ease of Use

In this section, we define the algorithms of Key Policy Attribute-Based encryption. We also determine the security model as a selective security adversary model.

A. Key policy attribute-based encryption

This type of ABE like others has four algorithms: setup, key generation, encryption, and decryption algorithms. Setup and key generation algorithms are

implemented by a trusted entity (broker). The encryption algorithm is implemented by the sender (data owner) and the decryption algorithm is implemented by the receiver (data user). Now, we examine the algorithms in this scheme.

Setup (λ, l): this algorithm receives λ security parameter as well as the total number of attributes and generates master secret key (MSK) and public key (PK). The set of attributes is shown with L.

Key generation (MSK, k, B): this MSK algorithm receives the k-threshold and attribute set $B \subseteq L$ as the input and generates the SK_B (secret key).

Encryption (B', PK, M): this algorithm receives PK, the intended message (M), and the target attribute set ($B' \subseteq L$) as the input and generates $Ctx_{B'}$ ciphertext.

Decryption ($SK_B, Ctx_{B'}$): this algorithm receives SK_B and $Ctx_{B'}$. If $| B \cap B'| < k$, then the algorithm output will be $\perp$, otherwise, this algorithm recovers M (message) and generates as output.

B. Selective security model

Considering that we will prove our scheme security in the selective security model, the model will be described here.

Initialization: the adversary first identifies the attribute set of B^* challenge.
Setup: the challenger implements the setup algorithm and sends the public keys to the adversary.
Phase 1: the adversary is allowed to issue queries for private keys for a number of B_j attribute sets of its choice as long as $|B^* \cap B_j| < k$ holds true for all j.
Challenge: the adversary selects M_0 and M_1 and submits them to the challenger.
The challenger selects b random bit and encrypts M_b with B^* challenge attributes (the message is one bit in our scheme. Thus, the challenger should encrypt only a random bit).
Phase 2: phase 1 is repeated.
Guess: the adversary guesses which message is encrypted. We show the adversary guess by b'.
If the adversary identifies the intended bit with a probability more than $\frac{1}{2}$, it can decrypt the scheme.

IV. PRELIMINARIES

In this section, ABE preliminaries will be discussed. In this regard, we will provide the mathematical prerequisites to enter the main scheme.

A. Secret sharing

The schemes were first proposed by Shamir. We assume that we want to share a secret among several entities or individuals. Each entity is given a secret share. Each secret sharing scheme has an access structure for the set of entities; thus these entities can recover private value by this access structure. At first, Shamir et al proposed a secret sharing scheme with 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 s secret among n entities with t threshold (it is called t out of n scheme and $t \leq n$) first a random polynomial q(x) of $t-1$ degree is selected in a way that $q(0) = s$. Each i entity, that $1 \leq i \leq n$, is given $(i, q(i))$. Lagrange coefficients are used to recover the value of s secret. The Lagrangian coefficient function can be calculated as follows.

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

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

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

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

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

B. Preliminaries: Lattices

Lattice-related issues, used in ABE, are examined here. The lattice algebraic and matrix structure have led to their use in most areas of encryption specially ABE.

First, we should mention that in this paper, the vector is displayed in bold lowercase English letters. Bold uppercase letters are also used to display the matrix. Moreover, the matrix and vector elements that will be integers, are shown in light lowercase English letters. The sets will also be displayed in light uppercase English letters. Additionally, the vector norm (2-norm) is defined as the square root of the sum of the squared vector values. In general, for the i-norm and vector x, we will have the following formula:

$$\|x\|_i = \sqrt[i]{x_1^2 + \cdots + x_n^2}$$

When the norm degree is not given, it will be assumed n-2. Also, for the matrix norm x, the norm of each column vector x is calculated as the vector norm and their maximum is assumed as matrix norm x. Moreover, for a $S = \{a_1, a_2, \dots, a_m\}$ ind function is defined as $nd_S(i) = a_i$, i.e., we have ordered the elements of the set and this function selects the i'th element of the set S.

C. Lattice Definition

We will use integer lattice. For each $A \in \mathbb{Z}_q^{n \times m}$ and $u\, \mathbb{Z}_q^n$ where q is a prime number, the Integer lattice is defined as follows [6].

$$\Lambda_q^{\perp}(A) = \{e \in \mathbb{Z}_q^n \ s.t. \ Ae = 0 \ (mod \ q)\} \qquad (4)$$

$$\Lambda_q^{u}(A) = \{e \in \mathbb{Z}_q^n \ s.t. \ Ae = u \ (mod \ q)\} \qquad (5)$$

Thus, according to the above definition, all e-vectors that hold for the above relation, are considered as lattice members that can be easily calculated using this relation. However, if a condition is placed on the vector norm, it is not always easy to find the vector. Suppose that the goal is to find a vector that holds for $Ae = 0$ relation and its norm is less than β. This problem is known as Small Integer Solution Problem (SIS). If we want that it holds for $Ae = u$, it is called the Inhomogeneous Small Integer Solution Problem (ISIS). If β and the prime number q are selected to hold for the relation $q \geq \beta. \omega(\sqrt{nlogn})$, then these two problems will be considered computationally hard that even quantum computers cannot solve them. For each integer lattice $\Lambda_q^\perp(A)$, there is a full rank matrix Like $T_A \in Z_q^{m \times m}$ if the following conditions hold true:

    a) These matrix columns are the lattice members.

    b) The matrix norm, I.e., $\|T_A\|$, is small.

    c) The relation $A.T_A = 0 \bmod q$ holds.

This is called Lattice Trapdoor Matrix. It is clear that due to SIS problem hardness, having matrix A, we cannot calculate its trapdoor.

Theorem 1 (Lattice Trapdoor Generation): There is an algorithm called ***TrapGen*** that if the condition $m \geq 5n.logq$ holds for every n and m integer and prime number q, generates $A \in \mathbb{Z}_q^{n \times m}$ and $T_A \in Z_q^{m \times m}$ matrices simultaneously that $A.T_A = 0$ relation and also $T_A \leq m.\omega(\sqrt{m})$ hold. So, T_A can be considered as $\Lambda_q^\perp(A)$ lattice trapdoor.

Theorem 2 (Preimage Sampling): Suppose that we have the matrices $T_A \in Z_q^{m \times m}$ and $A \in \mathbb{Z}_q^{n \times m}$ related to matrix $\Lambda_q^\perp(A)$. The goal is to solve the ISIS problem for this lattice, i.e. we find vector e as $A.e = u$. To this aim, there is an algorithm called ***SamplePre*** that solves this problem having T_A (lattice trapdoor).

The conclusion drawn from theorem 2 is that if the goal is to generate a matrix with a small norm R and it holds under the condition $A.R = D$ where D is also a definite matrix, the trapdoor of matrix A can be used. To solve this problem, if the matrix trapdoor is not available, it will be a difficult problem.

1) Learning with error (LWE)

Suppose as for $A \in \mathbb{Z}_q^{n \times m}$ matrix the value is $m = poly(n)$, i.e., m value1 is greater than that of n. Also, suppose that we have a probability distribution x and an error vector whose elements are selected from this distribution, i.e., $e \in \chi^m$. Now, we have made a vector $u \in \mathbb{Z}_q^m$ as $u = A^T s + e$ where there is the vector $s \in \mathbb{Z}_q^n$. The learning with error problem is defined as follows.

Given the matrix $A \in \mathbb{Z}_q^{n \times m}$ and also vector $u \in \mathbb{Z}_q^m$, that is generated as $u = A^T s + e$, we should find the vector $s \in \mathbb{Z}_q^n$. Finding this vector is called learning with error. There is also a decision version of this problem. Thus, having the matrix $A \in \mathbb{Z}_q^{n \times m}$ and also the vector $u \in \mathbb{Z}_q^m$, it must be decided whether the vector u is linearly generated as $u = A^T s + e$ or it is a random vector. This is the decision learning with error

problem. It is proved that the decision learning with error problem is computationally the same as the learning with error problem. Therefore, from now on when we refer to learning with error, it is the decision version. It should be noted that if the matrix $A \in \mathbb{Z}_q^{n \times m}$ is replaced by the vector $w \in \mathbb{Z}_q^n$ (i.e., $v = w^T s + e$), it is still a difficult problem. In addition, if we have several examples of learning with error problems (both matrix and vector), the problem will still be difficult.

V. OUR SCHEME

In this section, a scheme is presented for implementing a threshold access structure using key-policy attribute-based encryption (KP-ABE). The threshold value is determined by the authority during key generation. However, ABE presents several challenges, such as large key sizes and ciphertexts, and high computational complexity, particularly in lattice-based schemes. This paper aims to address these challenges by proposing a scheme that avoids using a NOT gate, thereby reducing computational and communication overhead. Although this approach provides less fine-grained access policy than schemes that utilize NOT gates, more attributes can be added to create a more detailed access structure. Also, to incorporate a NOT gate into our scheme, transferring from LWE to Ring LWE (R-LWE) without removing negative attributes can be a viable option. This approach is also expected to enhance the overall efficiency of our scheme. However, we have decided to leave this idea for future work. The primary focus of this scheme is to reduce computational and communication overhead, which remains a significant challenge in this area.

We will now explain the algorithms in this scheme.

Setup (λ, l): ***TrapGen*** algorithm is run according to L number (total number of attributes) that generates $A_i \in \mathbb{Z}_q^{n \times m}$ and $i \in [1, l]$. The trapdoor $\Lambda_q^\perp(A_i)$, i.e. $T_i \in Z_q^{m \times m}$ is also generated along with these matrices. Additionally, a random vector $u \in \mathbb{Z}_q^n$ is randomly selected. The public and, master keys will be as follows.

Key generation (MSK, K, B): first, the threshold value k is specified for the intended user that has a set of B' attributes. It is quite evident that $k \leq l$. Consider the number of elements as t' in the B' set. Now for each of the elements of vector $u = (u_1, \dots, u_n)$, Shamir secret sharing between K and L is implemented. That is, a k-1 polynomial is selected for each of $u_j; j \in [n]$ so that $p_j(0) = u_j; j \in [n]$. Thus, we will have:

$$\widehat{U} = \begin{bmatrix} \widehat{u_1} \\ \widehat{u_2} \\ \vdots \\ \widehat{u_n} \end{bmatrix} = \begin{bmatrix} p_1(1) & p_2(1) & \dots & p_n(1) \\ p_1(2) & p_2(2) & \dots & p_n(2) \\ \vdots & \vdots & \ddots & \vdots \\ p_1(l) & p_2(l) & \dots & p_n(l) \end{bmatrix}$$

Accordingly, for each set $J \subseteq [l]$ that $|J| \geq k$ holds, the Lagrange interpolation coefficients, presented by L_j, can be calculated. Thus, we will have the relation $u = \sum_{j \in J} L_j \widehat{u_j} \bmod(q)$. The **SamplePre** algorithm, by the use of MSK, is implemented to find

$e_j \in \mathbb{Z}_q^n$ vectors with small norm so that $A_j.e_{ind_{B'}(j)} = \hat{u}_j ; j \in B$. Therefore, the private keys for the user are as follows.

$$Sk_{B'} = \{B, [e_1, e_2, \dots, e_{t'}]\}$$

Encryption: this algorithm first specifies the target attribute set B, having t members, to encrypt the one-bit message $b \in \{0,1\}$. A random vector is selected as $s \in \mathbb{Z}_{nq}$. The error value x from the distribution χ as well as the error vectors $i \in B; x_i \in \chi_m$ are selected. $D = (i!)^2$ value is also calculated. The ciphertext will be as follows.

$$c_0 = u^T s + Dx + b.\left\lfloor\frac{q}{2}\right\rfloor$$
$$c_i = A_i^T s + Dx_i \in \mathbb{Z}_q^m; \quad i \in B$$
$$Ctx_B = \{B, c_0, \{c_i\}_{i \in B}\} \tag{6}$$

Decryption: suppose a user with an attribute set B intends to decrypt ciphertext Ctx_B. First, the set J that contains the intersections between B and B', is generated here. If $|J| < k$, then the algorithm output will be $\bot$, otherwise, the Lagrange interpolation coefficients L_j can be calculated. We know that the relation $\sum_{j \in J} L_j A_j e_{ind_{B'}(j)} = \sum_{j \in J} L_j \hat{u}_j = u$ holds. Now, the value r is calculated as follows:

$$r = c_0 - \sum_{j \in J} L_j.e_{ind_{B'}(j)}^T c_j \quad mod(q) \tag{7}$$

For this value, we have $r \in \left[-\left\lfloor\frac{q}{2}\right\rfloor, \left\lfloor\frac{q}{2}\right\rfloor\right] \subset \mathbb{Z}$. After this value is calculated, the decision for the value of the transmitted bit will be the following.

$$b = \begin{cases} 0, & |r| < \frac{q}{4} \\ 1, & else \end{cases} \tag{8}$$

The correctness of the relation 8 can be checked as follows.

$$r = c_0 - \sum_{j \in J} L_j.e_j^T c_j \quad mod(q)$$
$$= u^T s + Dx + b.\left\lfloor\frac{q}{2}\right\rfloor$$
$$- \sum_{j \in J} L_j.e_j^T \left(A_{j,id_j}^T s + Dx_i\right)$$
$$= b.\left\lfloor\frac{q}{2}\right\rfloor$$
$$+ \underbrace{\left\{u^T s - \sum_{j \in J}\left(L_j.e_j^T A_{j,id_j}^T\right)s\right\}}_{=0 \quad mod(q)}$$
$$+ \underbrace{\left\{Dx - \sum_{j \in J} DL_j.e_j^T x_i\right\}}_{\approx 0} \approx b.\left\lfloor\frac{q}{2}\right\rfloor$$

The above relation will be valid when the following condition is met.

$$Dx - \sum_{j \in J} DL_j.e_j^T x_i < \frac{q}{4} \tag{9}$$

In [6], it has been proved that relation 9 holds. Thus, we will not go into details. So if the value of r is closer to zero, the value of b will be that 0-bit to which some error has been added or subtracted. But if it is close to the value $\frac{q}{2}$, the value of b will be one-bit to which some error has been added or subtracted. As you can see, if the condition $|B \cap B'| \geq k$ does not hold, we cannot define the set J. As a result, it is not possible to recover the message by relations 7 and 8. The collusion of two or more users is not possible as well since the polynomials used in each user's private key are different. Therefore, since in the Lagrange interpolation relation, part of the shares is selected from a polynomial and another part from another polynomial, the Lagrange interpolation encounters an error and the message is not received.

B. Security proof

In this section, we will prove our scheme security by using the selective security model and assuming the hardness of the decision learning with error (LWE) problem. Suppose that the challenger has the following samples of the decision LWE problem and wants to solve it.

$$(w,v) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$$
$$(A_i,v_i) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m \quad ; i \in [1,t]$$

We also assume that there is an adversary A that breaks our scheme with $\frac{1}{2} + \varepsilon$ probability where ε is non-negligible. The challenger must use the adversary response to solve the decision LWE problem. If this happens, considering that it is a difficult problem and cannot be solved, we will conclude that there should be an adversary like A to break our scheme. To this end, we implement the phases of selective security model.

Initialization: the adversary first identifies the attribute set of B^* challenge.

Setup: the challenger simulates the setup algorithm for the adversary. It sets the public keys as A_i for $i \in [1,t]$, from the samples of decision LWE problem. The TrapGen algorithm is also implemented for $j \in [t+1,l]$. So, A_js and T_js will be placed in the public and private keys respectively. Additionally, another sample of the LWE problem is chosen as u=w and is placed in the public keys. Thus, the parameters and public keys are identified and transmitted to the adversary.

Phase 1: the adversary issues the queries associated with receiving the private key, for each set of B attributes that $|B \cap B*| = k'$ in a way that the condition k'<k holds.

- Assume Γ and Γ' as follows. $\Gamma = B \cap B^*$ and $\Gamma \subseteq \Gamma' \subseteq B$ where $|\Gamma'| = k - 1$.
- Also, consider that the samples associated with u will be as $\hat{u}_i = u + a_1 i + a_2 i^2 + \cdots + a_{k-1} i^{k-1}$ where $a_1, \dots, a_{k-1}$ are the vectors of length n.
- Thus, private keys e_i are generated for all $i \in B$ as follows.
  - If $\in \Gamma$: the random vector $e_1 \in \mathbb{Z}_p^n$ with a small norm is selected and the ith sample from u is placed as $\hat{u}_i = A_i.e_i$.
  - If $i \in \Gamma' - \Gamma$: the random vectors $\hat{u}_{t+1}, \dots, \hat{u}_{k-1}$ are selected. Therefore, the

variables $a_1, \ldots, a_{k-1}$ and all samples $\hat{u}_1, \ldots, \hat{u}_l$ can be easily calculated.

- If $i \in B - \Gamma'$: the challenger, considering that it knows the trapdoor associated with A_i ; $i \notin B^*$, can implement SamplePre algorithm to calculate e_i key.

So, in the private keys $e_i; i \in B$ we modify the subscripts as $e_1, e_2, \ldots, e_{t'}$ where t' is the number of B elements.

These keys are transmitted to the adversary.

Challenge: the challenger selects a random bit $b^* \in \{0,1\}$ and encrypts it with B^* challenge attributes as follows:

$$c_0 = Dv + b^* \cdot \left\lfloor \frac{q}{2} \right\rfloor$$
$$c_i = DA_i \; ; i \in B^*$$

If the samples of the hard LWE problem are generated as a linear matrix, c_0 and ci will be the same as the ciphertext for b^* bit. Thus, the challenger has been able to simulate the ciphertext for b^* one-bit message.

Phase 2: phase 1 is repeated.

Guess: in this phase, the adversary presents b' bit as its guess. If the samples of hard LWE problem is generated as a linear matrix, the adversary's success probability (i.e. $b' = b^*$) 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 for our scheme. Now if the samples of hard LWE problem are randomly generated, the adversary's success probability (i.e. $b' = b^*$) will be $\frac{1}{2}$. Since the challenger receives the value b' , if $b' = b^*$, it is assumed that the samples related to the hard LWE problem are generated as a linear matrix, and if $b' \neq b^*$, it is assumed that the samples associated with the hard LWE problem are generated as a linear matrix thus, the challenger can solve the decision LWE problem. Now, we calculate the challenger's success probability ($P(Ch)$).

$$P(Ch) = \frac{1}{2} P(b' = b^* | linear)$$
$$+ \frac{1}{2} \Pr(b' = b^* | random)$$
$$= \frac{1}{2}\left(\frac{1}{2} + \epsilon\right) + \frac{1}{2}\left(\frac{1}{2}\right)$$
$$= \frac{1}{2} + \frac{\epsilon}{2}$$

Since we assume that ϵ is non-negligible, $\frac{\epsilon}{2}$ will be non-negligible as well. Then the challenger can solve the decision LWE problem. But this contradicts our assumption because 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.

VI. RESULTS

The efficiency of ABE schemes usually is discussed from two aspects, computational complexity and the length of keys and ciphertext. The length of the

ciphertext has a direct relation with communication overhead. Therefore, we will compare our scheme with scheme [6] by supposing these two aspects.

We have compared the length of keys and ciphertext (communication overhead) in table 1. The length of secret (private) keys and ciphertext are more important than others.

TABLE I. THE COMPARISON OF THE LENGTH OF PARAMETERS

Parameter	Scheme [6]	Our scheme
The public key length	$(\mathbb{Z}_q^{n \times m})^{2l} + \mathbb{Z}_q^n$	$(\mathbb{Z}_q^{n \times m})^l + \mathbb{Z}_q^n$
The master key length	$(\mathbb{Z}_q^{m \times m})^{2l}$	$(\mathbb{Z}_q^{m \times m})^l$
The private key length	$(\mathbb{Z}_q^n)^l$	$(\mathbb{Z}_q^n)^{t'}$
The ciphertext length	$(\mathbb{Z}_q^m)^l + \mathbb{Z}_q$	$(\mathbb{Z}_q^m)^t + \mathbb{Z}_q$

According to table 1, we realize that the length of public and master keys has almost halved. Regarding the private key length, it should be noted that $t' \leq l$ and considering that in [6] the identity mode is used and in a random identity there is an equal number of 0-bit and one-bit. So, we can say that $t' \approx \frac{1}{2} l$ and the length of the private key has halved. Additionally, for the ciphertext length that is directly related to the communication overhead, $t \leq l$ holds and it has halved as well. These results mean that our scheme is more efficient than [6] in key length and communication overhead aspects. In the rest of the paper, we compare our scheme and [6] in other aspects.

Table 2 indicates a comparison of the computational overhead. The encryption and decryption phases are more important than others.

TABLE II. THE COMPARISON OF THE COMPUTATIONAL OVERHEAD

Operation	Scheme [6]	Our scheme
Setup	$2l(TG)$	$l(TG)$
Key generation	$l(SP)$	$t'(SP)$
Encryption	$l(MV) + 1(VV)$	$t(MV) + 1(VV)$
Decryption	$2k(VV)$	$2k(VV)$

In table 2, TG stands for the ***TrapGen*** algorithm, SP stands for the ***SamplePre*** algorithm, MV stands for matrix-vector and VV stands for vector-vector multiplication.

The table 2 shows that the number of ***TrapGen*** algorithms has halved in the setup phase. We can say that in the key generation phase, based on our discussion about t' and l, the number of ***SamplePre*** algorithms has also halved. The number of MV in the encryption phase has nearly halved as well. The computational complexity of MV operations is higher than others. So, reducing these operations decreases the computational complexity. According to table 2, you can see that we have reduced the number of MV operations from l to t . The number of decryption operations has not changed. As the computational complexity of lattice operations is high, reducing these

operations has really good effects on the efficiency of the scheme. These results mean that our scheme also is more efficient than [6] in the computational complexity aspect.

VII. Conclusion

In this paper, a Fuzzy Identity-Based Encryption (IBE) scheme is presented that leverages lattice problems - a specific type of Attribute-Based Encryption (ABE). Ensuring security against quantum attacks is a vital security concern in these discussions. By utilizing lattice-based hard problems, encryption schemes can resist quantum computers, making them a suitable solution for this purpose. The first lattice-based ABE scheme was presented in [6], and our current scheme builds upon it with various improvements. These enhancements include reducing the size of the public key, master key, private keys, and ciphertexts, as well as reducing the number of operations required for set up, key generation, and encryption. In order to demonstrate the efficiency of our scheme in comparison to [6], we have compared the relevant items in tables 1 and 2. In ABE, minimizing computational and communicational overhead is critical. We examine these improvements in terms of two general types of overhead, but it should be noted that unlike [6], our scheme cannot use the NOT gate, which is not a significant issue in many applications.

VIII. References

[1] J. Zhao, H. Gao and B. Hu, "Ciphertext-policy attribute-based encryption for circuits from lattices under weak security model," in Chinese Conference on Trusted Computing and Information Security, Springer, 2018, pp. 1-15.

[2] R. Tsabary, "Fully secure attribute-based encryption for t-CNF from LWE," Annual International Cryptology Conference, 2019.

[3] X. Dong, Y. Zhang, B. Wang and J. Chen, "Server-aided revocable attribute-based encryption from lattices," Security and Communication Networks, vol. 2020, 2020.

[4] X. Liu, J. Ma, J. Xiong, Q. Li, T. Zhang and H. Zhu, "Threshold attribute-based encryption with attribute hierarchy for lattices in the standard model," IET Information Security, 2014.

[5] W. Zhu, J. Yu, T. Wang, P. Zhang and W. Xie, "Efficient attribute-based encryption from R-LWE," Chinese Journal of Electronics, vol. 23, 2014.

[6] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris and H. Wee, "Functional encryption for threshold functions (or fuzzy IBE) from lattices," in Public Key Cryptography--PKC 2012: 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings 15, Springer, 2012, pp. 280-297.

[7] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Annual international conference on the theory and applications of cryptographic techniques, Vols. Fuzzy Identity-Based Encryption, Springer, 2005, pp. 457-473.

[8] 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.

[9] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in Proceedings of the 13th ACM conference on Computer and communications security, 2006, pp. 89-98.

[10] S. Khajouei-Nejad, S. Jabbehdari, H. Haj Seyyed Javadi and S. M. H. Moattar, "Fuzzy Identity Based Encryption with a flexible threshold value," Journal of Communication Engineering, 2023.

[11] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in 2007 IEEE symposium on security and privacy (SP'07), IEEE, 2007, pp. 321-334.

[12] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," in Public Key Cryptography--PKC 2011: 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings 14, Springer, 2011, pp. 53-70.

[13] 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.

[14] 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, pp. 1-14, 2022.

[15] M. MahdaviOliaee and Z. Ahmadian, "Ciphertext Policy Attribute Based Encryption for Arithmetic Circuits," eprint, 2021.

[16] M. Green, S. Hohenberger and B. Waters, "Outsourcing the decryption of abe ciphertexts," in USENIX security symposium, vol. 2011, 2011.

[17] M. Mahdavi 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," The ISC International Journal of Information Security (ISeCure), vol. 10, no. 2, pp. 117-127, 2018.

[18] M. Mahdavi 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), IEEE, 2017, pp. 2047-2051.

[19] 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.

[20] H. E. D. Kang, D. Kim, S. Kim, D. D. Kim, J. H. Cheon and B. W. Anthony, "Homomorphic Encryption as a secure PHM outsourcing solution for small and medium manufacturing enterprise," Journal of Manufacturing Systems, vol. 61, pp. 856-865, 2021.

[21] M. Chase, "Multi-authority Attribute Based Encryption," in Theory of Cryptography: 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007. Proceedings 4, Berlin, Heidelberg, Springer, 2007, pp. 515-534.

[22] J. Ge, M. Wen, L. Wang and R. Xie, "Attribute-Based Collaborative Access Control Scheme with Constant Ciphertext Length for Smart Grid," in ICC 2022-IEEE International Conference on Communications, IEEE, 2022, pp. 540-546.

[23] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, 2010.

[24] Z. Liu and D. S. Wong, "Practical attribute-based encryption: traitor tracing, revocation and large universe," The Computer Journal, vol. 59, no. 7, pp. 983-1004, 2016.

[25] Z. a. L. X. Guan, W. Yang, L. Wu, N. Wang and Z. Zhang, "Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid," Journal of Parallel and Distributed Computing, vol. 147, pp. 34-45, 2021.

[26] Z. Zhang and X. Ren, "Data security sharing method based on CP-ABE and blockchain," Journal of Intelligent \& Fuzzy Systems, vol. 40, no. 2, pp. 2193-2203, 2021.

[27] J. Yu, S. Liu, M. Xu, H. Guo, F. Zhong and W. Cheng, "An Efficient Revocable and Searchable MA-ABE Scheme with Blockchain assistance for C-IoT," IEEE Internet of Things Journal, 2022.

[28] S. Das and S. Namasudra, "Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure," IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 821-829, 2022.

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

[30] J. Zhang and Z. Zhang, "A Ciphertext Policy Attribute-Based Encryption Scheme without Pairings," in Information Security and Cryptology: 7th International Conference, Inscrypt 2011, Beijing, China, November 30--December 3, 2011. Revised Selected Papers 7, Berlin, Heidelberg, Springer, 2012, pp. 324-340.

[31] X. Boyen, "Attribute-Based Functional Encryption on Lattices," in Theory of Cryptography: 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3-6, 2013. Proceedings, Springer, 2013, pp. 122-142.

[32] S. Agrawal, R. Biswas, R. Nishimaki, K. Xagawa, X. Xie and S. Yamada, "Cryptanalysis of Boyen's attribute-based encryption scheme in TCC 2013," Designs, Codes and Cryptography, vol. 90, no. 10, pp. 2301-2318, 2022.

[33] S. Gorbunov, V. Vaikuntanathan and H. Wee, "Attribute-Based Encryption for Circuits," Journal of the ACM (Association for Computing Machinery), vol. 62, no. 6, pp. 1-33, May 2013.

[34] D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan and D. Vinayagamurthy, "Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits," in Advances in Cryptology--EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings 33, Springer, 2014, pp. 533-556.

[35] W. Susilo, D. H. Duong, H. Q. Le and J. Pieprzyk, "Puncturable encryption: a generic construction from delegatable fully key-homomorphic encryption," in Computer Security--ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14--18, 2020, Proceedings, Part II 25, Springer, 2020, pp. 107-127.

[36] S. Kim, "Multi-authority attribute-based encryption from LWE in the OT model," Cryptology ePrint Archive, 2019.

[37] U. S. Varri, S. K. Pasupuleti and K. Kadambari, "CP-ABSEL: Ciphertext-policy attribute-based searchable encryption from lattice in cloud storage," Peer-to-Peer Networking and Applications, vol. 14, no. 3, pp. 1290-1302, 2021.

Sedigheh Khajouei-Nejad is a Ph.D. student of Communication Systems at the Department of Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran. She received her M.Sc. degree in Computer Engineering from Islamic Azad University, Mashhad, Iran. Her research interests are Machine Learning and Public-Key Cryptosystems such as Attribute-based Encryption, Blockchain, and Post-Quantum Cryptography.

Hamid Haj Seyyed Javadi is currently a Professor of Mathematics and Computer Science in the Department of Computer Engineering at Shahed University. He received his Ph.D. from Amirkabir University of Technology, Tehran, Iran. He also received his B.Sc. and M.Sc. degrees from Amirkabir University of Technology, Tehran, Iran.

Sam Jabbehdari currently working as an Associated Professor at the Department of Computer Engineering in IAU (Islamic Azad University), North Tehran Branch, in Tehran, since 1993. He received his both B.Sc. and M.Sc. degrees in Electrical Engineering Telecommunication from Khajeh Nasir Toosi University of Technology and IAU, South Tehran branch in Tehran, Iran, respectively. He was honored Ph.D. degree in Computer Engineering from IAU, Science and Research Branch, Tehran, Iran in 2005. His current research interests are Scheduling, QoS, MANETs, Wireless Sensor Networks, and Cloud Computing.

Mohammad Hossein Moattar received his Ph.D. in 2010 from Amirkabir University of Technology, Tehran, Iran. Currently, he is working as an Associate Professor at the Department of Computer Engineering, Islamic Azad University, Mashhad branch, Mashhad, Iran. His research areas include Artificial Intelligence, Machine Learning, and Pattern Recognition.