The ISC Int'l Journal of Information Security
ISeCure

January 2025, Volume 17, Number 1 (pp. 13–23)
http://www.isecure-journal.org

Enhancing Lattice-Based Attribute-Based Encryption with Robust Fine-Grained Access Policies

Sedigheh Khajouei-Nejad[1], Sam Jabbehdari[1], Hamid Haj Seyyed Javadi[2,*], and Seyed Mohammad Hossein Moattar[3]

[1] *Department of Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran*
[2] *Department of Computer Engineering, Shahed University, Tehran, Iran*
[3] *Department of Computer engineering, Mashhad branch, Islamic Azad University, Mashhad, Iran*

ARTICLE INFO.

Article history:
Received: January 18, 2024
Revised: April 24, 2024
Accepted: August 1, 2024
Published Online: August 4, 2024

Keywords:
Attribute-Based Encryption (ABE), Learning With Errors (LWE), Access Policy, Key Policy Attribute-Based Encryption (KP-ABE), Post-Quantum Attribute-Based Encryption (PQ-ABE), Disjunctive Normal Form (DNF)

Type: Research Article

doi: 10.22042/isecure.2024.436486.1082

ABSTRACT

Protecting sensitive data is crucial in various fields, including Information Technologies, Network Security, and healthcare records. Implementing precise access policies for encrypted data is vital in large networks. Attribute-based encryption (ABE) is a solution to this challenge, enabling encryption and access control simultaneously. With the increasing significance of quantum-safe measures due to advancements in quantum computing, there is a growing need for quantum-resistant access control mechanisms for encrypted data, as addressed by Lattice-Based Attribute-based encryption. However, some existing Lattice-Based ABE schemes lack robust support for fine-grained access policies. This paper introduces an improved Key Policy Attribute-Based Encryption (KP-ABE) scheme that extends beyond threshold gates to support any boolean circuits. The proposed scheme's security is grounded in the Learning with Errors (LWE) assumption within the selective security model under the Indistinguishable CPA game. Notably, the scheme is well-suited for the Disjunctive Normal Form (DNF) representation of boolean functions, offering enhanced flexibility and security in access control mechanisms for encrypted data.

© 2024 ISC. All rights reserved.

1 Introduction

Attribute-based encryption (ABE) is a crucial cryptographic method that provides access control policies in secure data communication. By embedding access control directly into the encryption process, ABE empowers data owners with a nuanced approach to data protection. In contrast to conventional encryption systems that rely on a fixed set of cryptographic keys for access control, ABE enables the definition of access policies based on user attributes. The fundamental principle involves encrypting data with attributes, and only users possessing matching attributes are granted the authority to decrypt the information. The surge in interest surrounding ABE transcends disciplinary boundaries, capturing attention across diverse domains. In critical fields like healthcare, where precise access control and stringent data privacy are crucial, ABE emerges as a revolutionary solution. There are different types of ABE, including Key Policy ABE

[*] Corresponding author.

Email addresses: se_khajouei_nejad@yahoo.com , s_jabbehdari@iau-tnb.ac.ir, h.s.javadi@shahed.ac.ir, moattar@mshdiau.ac.ir

ISSN: 2008-2045 © 2024 ISC. All rights reserved.

(KP-ABE) and Ciphertext Policy ABE (CP-ABE). The main difference between KP-ABE and CP-ABE is how they control data access. In KP-ABE, data includes only user attributes, and decryption keys are associated with access structures, while ciphertexts are associated with sets of attributes. On the other hand, in CP-ABE, attributes are used to describe a user's credentials, and the encryptor determines a policy on who can decrypt the data. In other words, in KP-ABE, policies are built into users' keys, while in CP-ABE, the encryptor determines the policy on who can decrypt the data. KP-ABE is the dual to CP-ABE in that an access policy is applied to the user's secret key, and a ciphertext is computed concerning a set of attributes. The typical definition of an access structure involves a boolean function, where its variables represent attributes, as seen in works such as [1], [2], and [3]. Nevertheless, an access structure can also be established using an arithmetic function, where the variables correspond to attribute values, as demonstrated in [4], [5], and [6].

1.1 Related Works

The seminal work by Sahai and Waters [7] introduced the concept of Attribute-Based Encryption (ABE) and proposed the first construction of Fuzzy Identity-Based Encryption (FIBE). It laid the foundation for ABE schemes and discussed the theoretical framework behind ABE. In a recent publication, [8] introduced a novel FIBE scheme to enhance the work of [7]. Following Sahai and Waters's work, Goyal *et al.* [1] used the Key Policy Attribute Based Encryption (KP-ABE) scheme for fine-grained access control. Bethencourt *et al.* [2] presented a comprehensive framework for Ciphertext Policy Attribute Based Encryption (CP-ABE), describing the encryption and decryption algorithms, security properties, and access policy language. Although access control is typically defined using boolean functions, some schemes, such as those proposed in [5], and [6], employ arithmetic functions as access structures. There are some papers that combine ABE schemes with other technologies like blockchain [9], [10] and Internet of Things (IoT) [11], [12] and [13]. Recently, [14] unveiled Registered Attribute-Based Encryption (Registered ABE), enabling users to create their secret keys and register their public keys and attributes with a "key curator". The curator consolidates these public keys into a concise master public key. To decrypt, users occasionally need to obtain helper decryption keys from the key curator, which they combine with their secret keys. In [15], the authors proposed a Multi-Authority Attribute-Based Encryption (MA-ABE) construction from standard assumptions. This construction supports predicates beyond just polynomial-size monotone boolean formulas. In [16], the authors introduced GLUE (Generalized, Large-universe, Unbounded, and Expressive), a pioneering scheme facilitating efficient decryption implementation while accommodating negations and online/offline extensions. [17] introduced a ciphertext-policy attribute-based access control scheme that combines online/offline encryption, hidden access policy, and access policy updates. [18] and [19] also focused on fast decryption and efficient attribute revocation. [20] introduced a scheme that simultaneously supports multi-keyword search and fine-grained access control. The security of these schemes relies on number-theoretic assumptions, such as hard assumptions associated with pairings, rendering them vulnerable to quantum algorithms. A review of number-theoretic and pairing-based hard problems can be found in [21]. Next, we will delve into Post-Quantum Attribute-Based Encryption (PQ-ABE) schemes.

In recent years, there has been growing interest in applying lattice-based and Learning with Errors (LWE) techniques in ABE systems due to their potential for post-quantum security. Agrawal *et al.* [22] introduced a lattice-based fuzzy Identity-Based Encryption (IBE) scheme with a single threshold gate in the access structure, which can be viewed as a lattice version of the scheme presented in [7]. Recently, [23] and [24] proposed an improved scheme that enhances efficiency but sacrifices granularity compared to the original one. However, due to the utilization of a non-monotone access structure, the computational load of the scheme is increased. Zhang [25] 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 [26] proposed a KP-ABE scheme for the access structure of logic circuits based on a lattice. However, the security of Boyen's scheme was later shown to be insecure [27]. Following Boyen, Gorbunov *et al.* [28] introduced a KP-ABE scheme that can use any Boolean function as an access structure. Lattice-based ABE schemes such as [4] and [29] offer advantages in performing arithmetic circuits. Like pairing-based ABEs, lattice-based ABE schemes have been enhanced through several approaches. For example,[30], [31], [32], and [33] were devised to address key escrow, heavy computation (through outsourcing), revocation, and efficiency problems, respectively. Heavy computation is a significant issue in the area of ABE and other cryptographic fields such as key management schemes and Private Set Intersection (PSI). References [34, 35] address this problem in key management, while [36–38] focus on it in the context of PSI. [39] defines Multi-Input Attribute-Based Encryption and suggests a two-input key-policy ABE based on LWE. The mentioned post-quantum ABE schemes suffer from intensive computational requirements and large key and ciphertext sizes. These come from the fact that these schemes use LWE. To address these issues we can design ABE schemes based on Ring LWE (RLWE). For instance, [33] uses RLWE for the mentioned advantage. In recent years designing ABE based on RLWE has developed significantly by proposing efficient schemes like [40] and [41]. Let us introduce some papers that used ABE in healthcare networks. ABE schemes offer several advantages in healthcare networks, such as fine-grained access control, patient privacy protection, and secure data sharing among healthcare providers.

To achieve fine-grained access control for EHRs, [42] leveraged the ciphertext-policy attribute-based encryption (CP-ABE) technique to encrypt tables published by hospitals, including patients' EHRs. [43] presents a Cloud-based Secure Healthcare Framework (SecHS) to offer safe access to healthcare and medical data by applying the CP-ABE scheme. An efficient ABE scheme, used in healthcare networks, is proposed in [44] that outsources part of the encryption and decryption to the edge nodes and supports attribute updates, enabling flexible proper control. [45] made the proposed framework consistent with current practices and achieved favorable criteria, such as data confidentiality, data recoverability, and time-aware ciphertext. [45] used ABE to achieve these results. These papers demonstrate the application of ABE in healthcare networks, emphasizing privacy preservation, fine-grained access control, and secure data sharing in various healthcare contexts. Lattice-based Attribute-Based Encryption (ABE) schemes are a type of ABE scheme that uses lattices as the underlying mathematical structure and are considered post-quantum secure.

1.2 Our Contributions

Our contributions in this paper include the proposal of a Key Policy Attribute-Based Encryption (KP-ABE) that allows the application of any boolean function as an access function. By defining any boolean function as a Disjunctive Normal Form (DNF) in the key generation algorithm, our scheme builds upon the foundation laid by the pioneering work of [22] in Post Quantum Attribute-Based Encryption (PQ-ABE) schemes.

Moreover, our scheme goes beyond the limitations of previous works such as [23] and [24], which focused solely on efficiency, sacrificing granularity. Unlike these schemes, which only support a single threshold gate, our proposed scheme offers stronger granularity by supporting any boolean function. By utilizing Additive Secret Sharing instead of Shamir Secret Sharing, we simplify the structure of [22].

The critical contributions of our proposed scheme are as follows:

- We present a KP-ABE scheme designed for any monotone access control structure. We prove its security under the LWE assumption in the IND-CPA security model.
- Our scheme enhances the granularity of the [22] scheme, extending support to a broader range of access controls beyond the limitation of a single threshold. While [22] can accommodate a NOT gate, unlike our scheme, we can support it by doubling the number of attributes.
- Furthermore, our proposed scheme optimizes the efficiency of [22] by reducing the number of operations required during encryption and decryption, thereby shrinking the size of the secret key and ciphertext. Our scheme is also compared with those proposed in [46] and [24], demonstrating superior efficiency compared to both.

1.3 Paper Structure

The subsequent sections of this paper adhere to the following structure: Section 2 provides an introduction to preliminaries, encompassing definitions and cryptographic tools. Section 3 delves into the proposed scheme and outlines its algorithms, followed by the comprehensive security proof in Section 4. The paper concludes with a summary in Section 5.

2 Preliminaries

This section provides an overview of the fundamental concepts, including key definitions and cryptographic primitives, that underpin the proposed scheme. Our exploration begins with defining the Disjunctive Normal Form (DNF) for boolean functions, adapted from [5]. This definition serves as a fundamental building block for our scheme. Note that we denote the size of set S by $|S|$, and $[n]$ represents the set of all nonzero positive integers less than $n+1$.

Definition 1 (DNF Function). Let $\mathbf{x} = [x_1, x_2, \ldots, x_n]$, $a_i \in \{0,1\}$, and $\mathbb{A}$ be a set of all subsets of the array $\mathbf{x}$. Elements of $\mathbb{A}$ are denoted by P_i. The general form of the DNF form of a Boolean function is as follows.

$$f(\mathbf{x}) = \sum_{i\in[|\mathbb{A}|]} (a_i \prod_{j\in P_i} x_j) \tag{1}$$

We define the set $\mathbb{S} = \{P_i | a_i \neq 0\}$. For simplicity, we can rewrite (1) as follows:

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{|\mathbb{S}|} (\prod_{i\in P_j} x_i) \tag{2}$$

The DNF form of the function is also called a Sum of Products.

For a set B, $f(B)$ denotes the substitution $x_i = 1$ for all $x_i \in B$ and $x_j = 0$ for all $x_j \notin B$ in (2).

Definition 2 (Key Policy Attribute-Based Encryption – KP-ABE). Key Policy Attribute-Based Encryption (KP-ABE) involves four key algorithms: setup, key generation, encryption, and decryption, denoted by `Setup`, `KeyGen`, `Enc`, and `Dec` respectively. The `Setup` and `KeyGen` algorithms are executed by a trusted entity. In contrast, the `Enc` algorithm is executed by the sender (data owner), and the `Dec` algorithm is executed by the receiver (data user). The algorithms are formally defined as follows:

- `Setup`(λ, ℓ): The setup algorithm receives the security parameter λ and the total number of attributes and generates the master secret key (MSK) and public key (PK). The set of attributes is shown with $\mathbb{U}$.
- `KeyGen`(MSK, f): The key generation algorithm receives a boolean function in DNF form f and master secret key MSK as input and generates the secret key (SK_f).
- `Enc`(PK, B, m): The encryption algorithm receives the public key (PK), the intended message (M), and the target attribute set $(B \subset L)$ as input and generates the ciphertext Ctx_B.
- `Dec`(Ctx_B, SK_f): this algorithm receives SK_f and Ctx_B. If $f(B) \neq 1$, then the algorithm output will be $\perp$; otherwise, this algorithm recovers M (message) and generates as output.

2.1 Selective Security Model

This section defines the selective security model by running Ind-CPA game between a challenger and an attacker. The following delineates the specific details encompassed within the selective security model.

- **Initialization:** The adversary first identifies the challenge attribute set B^*.
- **Setup:** The challenger runs the setup algorithm and sends the public keys to the adversary.
- **Phase 1:** The adversary is allowed to issue queries for private keys for several f_j functions as long as $f(B^*) \neq 1$ holds 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. Note that 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. The adversary's guess is shown by b'.

If the adversary can distinguish the intended bit with a probability of $1/2 + \epsilon$, where ϵ is non-negligible, we call the adversary win the proposed Indistinguishable CPA (Ind-CPA) game. Otherwise, the scheme is deemed secure.

2.2 Secret Sharing

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 proposed a secret sharing scheme with a threshold gate. In this scheme, a secret is shared among n entities, and if t or more of these entities collaborate, they can recover the secret. 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.

$$\Delta_{i,S}(x) = \prod_{j \in S, i \neq j} \frac{x-j}{i-j} \quad , \quad i \in S \tag{3}$$

$$L_i = \Delta_{i,S}(0) = \prod_{j \in S, j \neq i} \frac{-j}{i-j} \tag{4}$$

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

$$q(0) = \sum_{i \in S} q(i) \cdot L_i \tag{5}$$

The above-mentioned formula is used for a threshold function and AND and OR gates can be generated using this function.

2.2.1 Additive Secret Sharing

With an access threshold of $t = n$, every share is required to recover the original secret, simulating an AND gate in an access structure. While this setup is more restrictive than allowing an arbitrary threshold where $t \leq n$, it is a widely used approach. This constraint on t permits highly efficient schemes.

Suppose we want to divide a secret into n shares such that the total sum of all shares equals the original secret, s. To achieve this, select random values for the shares, x_i, for $1 \leq i < n$. Finally, set the last share as $x_n = s - \sum_{i=1}^{n-1} x_i$. This way, the condition $\sum_{i=1}^{n} x_i =$

s is met, ensuring that all shares are needed to recover the secret, reflecting the behavior of an AND gate in an access structure.

2.3 Lattice

During 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 the square root of the sum of the squared vector values. In general, for the p-norm and vector $\mathbf{x}$, we will have the following formula:

$$\parallel \mathbf{x} \parallel_p = \sqrt[p]{x_1^p + \cdots + x_n^p} \tag{6}$$

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

We will use an integer lattice. For each $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{u} \in \mathbb{Z}_q^n$ where q is a prime number, the Integer lattice is defined as follows [22].

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{d} \in \mathbb{Z}_q^n \ s.t. \ \mathbf{Ad} = \mathbf{0} \mod q\} \tag{7}$$

$$\Lambda_q^{u}(\mathbf{A}) = \{\mathbf{d} \in \mathbb{Z}_q^n \ s.t. \ \mathbf{Ad} = \mathbf{u} \mod q\} \tag{8}$$

Based on the provided definition, all e-vectors that satisfy the given relation are regarded as lattice members. These lattice members can be readily computed using the relation. However, if an additional constraint is imposed on the vector norm, finding a vector that meets both the relation and the norm condition may not always be straightforward. Suppose the goal is to find a vector that holds for $\mathbf{Ae} = 0$ relation and its norm is less than β. This problem is known as the Small Integer Solution Problem (SIS). For the case of $\mathbf{Ae} = \mathbf{u}$, it is called the Inhomogeneous Small Integer Solution Problem (ISIS). If β and the prime number q are selected to hold for the relation $q \geq \beta.\omega(\sqrt{nlogn})$, these two problems will be considered computationally hard that even quantum computers cannot solve them. For each integer lattice $\Lambda_q^{\perp}(\mathbf{A})$,there is a full rank matrix Like $\mathbf{T_A} \in \mathbb{Z}_q^{m\times m}$ if the following conditions hold true:

- These matrix columns are the lattice members;
- The norm of matrix, i.e., $\parallel T_A \parallel$, is small;
- The relation $\mathbf{A}.\mathbf{T_A} = 0 \mod q$ holds.

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

Definition 3 (Lattice Trapdoor Generation). There is an algorithm called ***TrapGen*** that if the condition $m \geq 5n \cdot \log q$ holds for every n and m integer and prime number q, generates $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{T_A} \in \mathbb{Z}_q^{m\times m}$ matrices simultaneously that $A \cdot \mathbf{T_A} = 0$ relation and also $\mathbf{T_A} \geq m \cdot \omega(\sqrt{m})$ hold. So, $\mathbf{T_A}$ can be considered as $\Lambda_q^{\perp}(\mathbf{A})$ lattice trapdoor.

Definition 4 (Preimage Sampling). Suppose that we have the matrices $\mathbf{T_A} \in \mathbb{Z}_q^{m\times m}$ and $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ related to matrix $\Lambda_q^{\perp}(\mathbf{A})$. The goal is to solve the ISIS problem for this lattice, i.e., we find vector $\mathbf{e}$ as $\mathbf{A}.\mathbf{d} = \mathbf{u}$. To this aim, there is an algorithm called ***SamplePre*** that solves this problem by having $\mathbf{T_A}$ (lattice trapdoor).

The conclusion drawn from Definition 4 is that if the goal is to generate a matrix with a small norm R and it holds under the condition $\mathbf{A} \cdot \mathbf{R} = \mathbf{D}$ where $\mathbf{D}$ is also a definite matrix, the trapdoor of matrix $\mathbf{A}$ can be used. This problem is considered computationally hard without access to the matrix trapdoor.

2.4 Learning with Errors (LWE)

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

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

3 The Proposed Scheme

In this section, we introduce an enhanced version of the [22] scheme, transforming it from a Fuzzy Identity-Based Encryption (FIBE) to a Key Policy Attribute-Based Encryption (KP-ABE) variant capable of accommodating any boolean function in Disjunctive Normal Form (DNF). Similar to the approach in [22], our scheme can support negative attributes by doubling the number of attributes. However, for the sake of simplicity, we opt to overlook this straightforward technique. The scheme involves four fundamental algorithms: setup, key generation, encryption, and decryption. Detailed explanations of these algorithms are presented below.

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

$$PP = [\{\mathbf{A}_i\}_{i\in[\ell]}, \mathbf{u}] \quad , \quad MK = \{\mathbf{T}_i\}_{i\in[\ell]} \tag{9}$$

- `KeyGen`$(MSK, K, f(\mathbf{x}))$: First, the access function is specified for the intended user as DNF form $f(\mathbf{x}) = \vee_{i=1}^{l}(\wedge_{j\in B_i} x_j)$. Note that B_i is the set of attributes, where some of them can be negative. Now, for each of the clauses of the function, additive secret sharing for vector $\mathbf{u}$ is implemented. Therefore, for each B_i where $1 \le i \le l$, a set of random vectors $\mathbf{u}_{ij}$ are chosen as follows:

$$\sum_{j\in B_i} \mathbf{u}_{ij} = \mathbf{u} \mod q \ , \ 1 \le i \le l \tag{10}$$

The ***SamplePre*** algorithm, by the use of MSK, is implemented to find $\mathbf{d}_{ij} \in \mathbb{Z}_q^n$ vectors with small norm so that $\mathbf{A}_j.\mathbf{d}_{ij} = \mathbf{u}_{ij}; j \in B_i$. Therefore, the private keys for the user are as follows.

$$Sk_f = \{f(\mathbf{x}), [\mathbf{D}_1, \mathbf{D}_2, \ldots, \mathbf{D}_l]\} \tag{11}$$

Where each $\mathbf{D}_i$ is a matrix that its columns are $\mathbf{d}_{ij}$ defined according to B_i.

- `Enc`(m, B, PP): 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 $\mathbf{s} \in \mathbb{Z}_n^q$. The error value x from the distribution χ and the error vectors $i \in B; e_i \in \chi_m$ are selected. The ciphertext will be as follows.

$$c_0 = \mathbf{u}^T\mathbf{s} + e + b \cdot [q/2] \tag{12}$$

$$\mathbf{c}_i = \mathbf{A}_i^T\mathbf{s} + \mathbf{e}_i \in \mathbb{Z}_q^m \quad , \quad i \in B \tag{13}$$

$$Ctx_B = \{B, c_0, \mathbf{c}_i\}_{i\in B} \quad , \quad |B| = t \tag{14}$$

- `Dec`(Ctx_B, Sk_f): suppose a user with a secret key Sk_f intends to decrypt ciphertext Ctx_B. If $f(x) \neq 1$, then the output of the algorithm will be $\perp$, otherwise, one of the clauses satisfied by B, is selected. For efficiency purposes, we select the $B_i \subseteq B$ with the fewest elements among all possible clauses that satisfy the function. We know that the relation $\sum_{j\in B_i} \mathbf{A}_j.\mathbf{d}_{ij} = \sum_{j\in B_i} \mathbf{u}_{ij} = \mathbf{u}$ holds. Now, the value r is calculated as follows:

$$r = c_0 - \sum_{j\in B_i} \mathbf{d}_{ij}^T\mathbf{c}_j \mod (q) \tag{15}$$

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

$$b = \begin{cases} 0 & |r| \le q/4 \\ 1 & else \end{cases} \tag{16}$$

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. However, if it is close to the value $q/2$, the value of b will be one bit to which some error has been added or subtracted.

The correctness of the relation (15) can be checked as follows.

$$\begin{aligned} r &= c_0 - \sum_{j\in B_i} \mathbf{d}_{ij}^T\mathbf{c}_j \\ &= \mathbf{u}^T\mathbf{s} + e + b.[q/2] - \sum_{j\in B_i} \mathbf{d}_{ij}^T(\mathbf{A}_j^T\mathbf{s} + \mathbf{e}_i) \\ &= b \cdot [q/2] + \underbrace{(\mathbf{u}^T\mathbf{s} - \sum_{j\in B_i} \mathbf{d}_{ij}^T\mathbf{A}_j^T\mathbf{s})}_{=0} + \underbrace{(e - \sum_{j\in B_i} \mathbf{d}_{ij}^T\mathbf{e}_i)}_{\approx 0} \\ &\approx b \cdot [q/2] \end{aligned}$$

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

$$e - \sum_{j\in J} \mathbf{d}_{ij}^T\mathbf{e}_i \le q/4$$

If the condition is not met, the message cannot be recovered using relations (15) and (16). Therefore, the secret key vectors $\mathbf{d}_{ij}$ must have a low norm to satisfy the condition. This is crucial for choosing the correct parameters, as discussed in [22]. The collision of two or more users is also not possible 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.

4 Security and Performance Analysis

This section demonstrates the security of the proposed scheme in the selective security model, assuming the hardness of the LWE problem. This section also compares the proposed scheme with [22] and [23] regarding efficiency and granularity.

4.1 Security Proof

If there exists an adversary $\mathcal{A}$ who can win the Ind-CPA game for the proposed scheme in the selective security model, then a challenger can construct an algorithm to solve the LWE problem. Suppose that the challenger has the following samples of the decision LWE problem and wants to solve it.

$$(\mathbf{w}, v) \in \mathbb{Z}_q^n \times \mathbb{Z}_q \tag{17}$$

$$(\mathbf{A}_i, \mathbf{v}_i) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m \ , \quad i \in [1, t] \tag{18}$$

We also assume that there is an adversary $\mathcal{A}$ that breaks our scheme in the selective security model with probability $1/2 + \epsilon$ where ϵ is non-negligible. The challenger must use the adversary's response to solve the decision LWE problem. If this happens, considering that it is a hard problem and cannot be solved, we will conclude that there should not be an adversary like $\mathcal{A}$ to break our scheme. To start the proof, the challenger runs IND-CPA game with the attacker in selective security model.

- **Initialization**: The adversary identifies the challenge attribute set B^*, which contains t number of attributes.
- **Setup**: The challenger simulates the setup algorithm for the adversary. It sets the public keys as $\mathbf{A}_i$ for $i \in [1, t]$, from the samples of decision LWE problem. The ***TrapGen*** algorithm is also implemented for $j \in [t+1, \ell]$. So, $\mathbf{A}_j$'s and $\mathbf{T}_j$'s will be placed in the public and master secret keys, respectively. Additionally, another sample of the LWE problem is set as $\mathbf{u} = \mathbf{w}$ and published as a part of the public keys. Thus, the parameters and public keys are identified and transmitted to the adversary.
- **Phase 1**: The adversary submits queries to obtain secret keys for each DNF-formed boolean function f where $f(B^*) \neq 1$. The challenger responds as follows.
  - Since $f(B^*) \neq 1$ is met, so $B_i \not\subseteq B^*$ is true for every set B_i of this function. Assume Λ and Λ' as follows. $\Lambda = B_i \bigcap B^*$. Also, consider that the samples associated with $\mathbf{u}$ will be as $\mathbf{u} = \sum \mathbf{u}_i$ where $\mathbf{u}_i = \mathbf{A}_i \cdot \mathbf{d}_i$ are the vectors of length n. Thus, private keys $\mathbf{d}_i$ are generated for all $i \in B_i$.
  - If $k \in \Lambda$: the random vector $\mathbf{d}_1 \in \mathbb{Z}_p^n$ with a small norm is selected and the ith sample from u is placed as $\mathbf{u}_k = \mathbf{A}_k \cdot \mathbf{d}_k$. Suppose $\hat{\mathbf{u}} = \sum_{k\in\Lambda} \mathbf{u}_k$.
  - If $k \in B \setminus \Lambda$: Considering the equation $\sum_{k\in B\setminus\Lambda} = \mathbf{u} - \hat{\mathbf{u}}$, where $\mathbf{u}_k = \mathbf{A}_k \cdot \mathbf{d}_k$, the challenger has the ability to select a random vector $\mathbf{d}_k \in \mathbb{Z}_p^n$ with a small norm for all $k \in B \setminus \Lambda$ except one. For the last secret key, given the knowledge of the trapdoor associated with $\mathbf{A}_k; k \notin B^*$, the challenger can execute the ***SamplePre*** algorithm to calculate the secret key.

  These keys are sent to the adversary $\mathcal{A}$.
- **Challenge**: The challenger selects a random bit $b^* \in \{0, 1\}$ and encrypts it with B^* challenge attributes as follows:

  $$c_0 = v + b^* \cdot [q/2]$$
  $$\mathbf{c}_i = \mathbf{v}_i \ , \ i \in B^*$$

  If the samples of the LWE problem are generated as a linear matrix, both c_0 and $\mathbf{c}_i$ will be identical for the ciphertext corresponding to bit b^*. Consequently, the challenger can successfully simulate the ciphertext for a one-bit message of b^*. Conversely, when the LWE problem is generated randomly, c_0 and $\mathbf{c}_i$ become random elements.
- **Phase 2**: Phase 1 is repeated.
- **Guess**: In this phase, the adversary posits its guess as b' bit. In the scenario where the samples of the LWE problem are generated as a linear matrix, the adversary's success probability (i.e., $b' = b^*$) is $1/2 + \epsilon$. This assumption is based on our consideration that an adversary with a probability of $1/2 + \epsilon$, where ϵ is non-negligible, can identify the encrypted bit in our scheme. Conversely, if the samples of the LWE problem are randomly generated, the adversary's success probability (i.e., $b' = b^*$) becomes $1/2$. Upon receiving the value b', the challenger makes an assumption: if $b' = b^*$, the LWE problem samples are generated as a linear matrix; if $b' \neq b^*$, the LWE problem samples are generated randomly. Accordingly, the challenger can then solve the decision LWE problem.

The challenger's success probability under above mentioned security game ($P(Ch)$) is as follows.

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

Since we assume that ϵ is non-negligible, $\epsilon/2$ will also be non-negligible.

4.2 Comparison

This section compares our proposed scheme with previous schemes, such as [22], [23], and their eprint versions [46] and [24]. The comparison is presented in Table 1, which includes various items such as access structure type, ciphertext size, encryption complexity, and decryption complexity, denoted as Granularity, Ctx size, Enc, and Dec, respectively.

The table uses MV to represent the multiplication of

Table 1. Comparison

	Granularity	Ctx size	Enc	Dec
Our scheme	Monotone	$\mathbb{Z}_q^{tm+1}$	t(MV)+ VV	k'(VV)
[22]	Threshold	$\mathbb{Z}_q^{\ell m+1}$	ℓ(MV)+ VV	$2k$(VV)
[23]	Threshold	$\mathbb{Z}_q^{tm+1}$	t(MV)+ VV	$2k$(VV)

a matrix by a vector and VV to represent vector by vector. For instance, "t(MV)+ VV" indicates that t matrix-vector multiplications and one vector-vector multiplication are required. Our proposed scheme outperforms the other schemes in all items. Since our scheme supports any boolean function as an access structure, it is superior to the other schemes. Additionally, as $t \leq \ell$, our scheme performs better in the Ctx size and Enc items. In the Dec item, k' denotes the size of the B_i of the secret key selected in the decryption algorithm, and $k' \leq k$. In [22] and [23], k Lagrangian vectors must be multiplied, but this is not necessary in our scheme due to additive secret sharing. Therefore, our scheme is more efficient and has better granularity than the others.

5 Conclusion

In summary, our research has developed a new Key Policy Attribute-Based Encryption (KP-ABE) scheme that enables access structures with any Disjunctive Normal Form (DNF) functions, going beyond the constraints of the Fuzzy Identity-Based Encryption (FIBE) scheme in [22]. Unlike the previous scheme, which was limited to threshold access control, our proposed scheme broadens its applicability to any boolean function. We have proven the security of our scheme in the selective security model, relying on the hardness of the learning with errors problem, thereby confirming its quantum-safe status. Additionally, our contributions include optimizing the efficiency of the encryption and decryption processes, reducing the required operations, and minimizing the ciphertext size. Compared to existing schemes, such as those presented in [46] and [24], the proposed scheme demonstrates superior efficiency.

References

[1] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98, 2006.

[2] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE symposium on security and privacy (SP'07)*, pages 321–334. IEEE, 2007.

[3] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 195–203, 2007.

[4] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit abe and compact garbled circuits. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 533–556. Springer, 2014.

[5] Mahdi MahdaviOliaee and Zahra Ahmadian. Fine-grained flexible access control: ciphertext policy attribute based encryption for arithmetic circuits. *Journal of Computer Virology and Hacking Techniques*, pages 1–14, 2022.

[6] Mahdi Mahdavi Oliaee and Zahra Ahmadian. Ciphertext policy attribute based encryption for arithmetic circuits. *Cryptology ePrint Archive*, 2021.

[7] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 457–473. Springer, 2005.

[8] Sedigheh Khajouei-Nejad, Sam Jabbehdari, Hamid Haj Seyyed Javadi, and Seyed Mohammad Hossein Moattar. Fuzzy identity based encryption with a flexible threshold value. *Journal of Communication Engineering*, 2023.

[9] Zhitao Guan, Xin Lu, Wenti Yang, Longfei Wu, Naiyu Wang, and Zijian Zhang. Achieving efficient and privacy-preserving energy trading based on blockchain and abe in smart grid. *Journal of Parallel and Distributed Computing*, 147:34–45, 2021.

[10] Zhijun Zhang and Xiaojun Ren. Data security sharing method based on cp-abe and blockchain. *Journal of Intelligent & Fuzzy Systems*, 40(2):2193–2203, 2021.

[11] Jiguo Yu, Suhui Liu, Minghui Xu, Hechuan Guo, Fangtian Zhong, and Wei Cheng. An efficient revocable and searchable ma-abe scheme with blockchain assistance for c-iot. *IEEE Internet of Things Journal*, 10(3):2754–2766, 2022.

[12] Mahdi Mahdavi, Mohammad Hesam Tadayon, Mohammad Sayad Haghighi, and Zahra Ahmadian. Iot-friendly, pre-computed and outsourced attribute based encryption. *Future Generation Computer Systems*, 150:115–126, 2024.

[13] Sangjukta Das and Suyel Namasudra. Multiauthority cp-abe-based access control model for iot-enabled healthcare infrastructure. *IEEE Transactions on Industrial Informatics*, 19(1):821–829,

2022.

[14] Susan Hohenberger, George Lu, Brent Waters, and David J Wu. Registered attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 511–542. Springer, 2023.

[15] Rachit Garg, Rishab Goyal, and George Lu. Dynamic collusion functional encryption and multi-authority attribute-based encryption. In *IACR International Conference on Public-Key Cryptography*, pages 69–104. Springer, 2024.

[16] Marloes Venema and Greg Alpár. Glue: Generalizing unbounded attribute-based encryption for flexible efficiency trade-offs. In *IACR International Conference on Public-Key Cryptography*, pages 652–682. Springer, 2023.

[17] Mostafa Chegenizadeh, Mohammad Ali, Javad Mohajeri, and Mohammad Reza Aref. Huap: Practical attribute-based access control supporting hidden updatable access policies for resource-constrained devices. *The ISC International Journal of Information Security*, 16(1):93–114, 2024.

[18] Sajjad Palanki and Alireza Shafieinejad. Attribute-based encryption with efficient attribute revocation, decryption outsourcing, and multi-keyword searching in cloud storage. *The ISC International Journal of Information Security*, 14(3):135–149, 2022.

[19] Sina Abdollahi, Javad Mohajeri, and Mahmoud Salmasizadeh. Highly efficient and revocable cp-abe with outsourcing decryption for iot. In *2021 18th International ISC Conference on Information Security and Cryptology (ISCISC)*, pages 81–88. IEEE, 2021.

[20] Aniseh Najafi, Majid Bayat, and Hamid Haj Seyyed Javadi. Privacy preserving attribute-based encryption with conjunctive keyword search for e-health records in cloud. *The ISC International Journal of Information Security*, 13(2):87–100, 2021.

[21] Mahdi Mahdavi Oliaee, Sahar Khaleghifard, and Zahra Ahmadian. New variations of discrete logarithm problem. *The ISC International Journal of Information Security*, 15(3):91–100, 2023.

[22] Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, and Hoeteck 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*, pages 280–297. Springer, 2012.

[23] Sedigheh Khajouei-Nejad, Hamid Haj Seyyed Javadi, Sam Jabbehdari, and Seyed Mohammad Hossein and Moattar. Reducing the computational complexity of fuzzy identity-based encryption from lattice. *International Journal of Information and Communication Technology Research*, 16(1), 2024.

[24] Sedigheh Khajouei-Nejad, Hamid Haj Seyyed Javadi, Sam Jabbehdari, and Seyed Mohammad Hossein Moattar. Reducing the computational complexity of fuzzy identity-based encryption from lattice. *Cryptology ePrint Archive*, 2024.

[25] Jiang Zhang and Zhenfeng Zhang. A ciphertext policy attribute-based encryption scheme without pairings. In *International Conference on Information Security and Cryptology*, pages 324–340. Springer, 2011.

[26] Xavier Boyen. Attribute-based functional encryption on lattices. In *Theory of Cryptography Conference*, pages 122–142. Springer, 2013.

[27] Shweta Agrawal, Rajarshi Biswas, Ryo Nishimaki, Keita Xagawa, Xiang Xie, and Shota Yamada. Cryptanalysis of boyen's attribute-based encryption scheme in tcc 2013. *Designs, Codes and Cryptography*, 90(10):2301–2318, 2022.

[28] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. *Journal of the ACM (JACM)*, 62(6):1–33, 2015.

[29] Willy Susilo, Dung Hoang Duong, Huy Quoc Le, and Josef 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*, pages 107–127. Springer, 2020.

[30] Sam Kim. Multi-authority attribute-based encryption from lwe in the ot model. *Cryptology ePrint Archive*, 2019.

[31] Uma Sankararao Varri, Syam Kumar Pasupuleti, and KV Kadambari. Cp-absel: Ciphertext-policy attribute-based searchable encryption from lattice in cloud storage. *Peer-to-Peer Networking and Applications*, 14:1290–1302, 2021.

[32] Xingting Dong, Yanhua Zhang, Baocang Wang, and Jiangshan Chen. Server-aided revocable attribute-based encryption from lattices. *Security and Communication Networks*, 2020:1–13, 2020.

[33] Weiling Zhu, Jianping Yu, Ting Wang, Peng Zhang, and Weixin Xie. Efficient attribute-based encryption from r-lwe. *Chin. J. Electron*, 23(4):778–782, 2014.

[34] Akbar Morshed Aski, Hamid Haj Seyyed Javadi, and Gholam Hassan Shirdel. A full connectable and high scalable key pre-distribution scheme based on combinatorial designs for resource-

constrained devices in iot network. *Wireless Personal Communications*, 114(3):2079–2103, 2020.

[35] Nafiseh Masaeli, Hamid Haj Seyyed Javadi, and Seyed Hossein Erfani. Key pre-distribution scheme based on transversal design in large mobile fog networks with multi-clouds. *Journal of Information Security and Applications*, 54:102519, 2020.

[36] 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 (extended version). *The ISC International Journal of Information Security*, 10(2):117–127, 2018.

[37] Mehdi Oliaee Mahdavi, 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. In *2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, pages 77–81. IEEE, 2017.

[38] Mahdi MahdaviOliaiy, Mohammad Hassan Ameri, Javad Mohajeri, and Mohammad Reza Aref. A verifiable delegated set intersection without pairing. In *2017 Iranian Conference on Electrical Engineering (ICEE)*, pages 2047–2051. IEEE, 2017.

[39] Shweta Agrawal, Anshu Yadav, and Shota Yamada. Multi-input attribute based encryption and predicate encryption. In *Annual International Cryptology Conference*, pages 590–621. Springer, 2022.

[40] Yang Yang, Jianguo Sun, Zechao Liu, and YuQing Qiao. Practical revocable and multi-authority cp-abe scheme from rlwe for cloud computing. *Journal of Information Security and Applications*, 65:103108, 2022.

[41] Hui Liu and Rui Jiang. Efficient revocable attribute-based encryption from r-lwe in cloud storage. In *Advances in Intelligent Automation and Soft Computing*, pages 1051–1058. Springer, 2022.

[42] Cheng Guo, Ruhan Zhuang, Yingmo Jie, Yizhi Ren, Ting Wu, and Kim-Kwang Raymond Choo. Fine-grained database field search using attribute-based encryption for e-healthcare clouds. *Journal of medical systems*, 40:1–8, 2016.

[43] Siti Dhalila Mohd Satar, Masnida Hussin, Zurina Mohd Hanapi, and Mohamad Afendee Mohamed. Cloud-based secure healthcare framework by using enhanced ciphertext policy attribute-based encryption scheme. *Int. J. Adv. Comput. Sci. Appl*, 12:393–399, 2021.

[44] Hong Zhong, Yiyuan Zhou, Qingyang Zhang, Yan Xu, and Jie Cui. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. *Future Generation Computer Systems*, 115:486–496, 2021.

[45] Liang Zhang, Haibin Kan, and Honglan Huang. Patient-centered cross-enterprise document sharing and dynamic consent framework using consortium blockchain and ciphertext-policy attribute-based encryption. In *Proceedings of the 19th ACM International Conference on Computing Frontiers*, pages 58–66, 2022.

[46] Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, and Hoeteck Wee. Fuzzy identity based encryption from lattices. *IACR Cryptol. ePrint Arch.*, 2011:414, 2011.

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 a master's degree in Computer Engineering from Mashhad Branch, Islamic Azad University, Mashhad, Iran. Her research interests are Machin Learning and Public-Key Cryptosystems such as Attribute-Based Encryption, Blockchain and Post-Quantum Cryptography.

Sam Jabbehdari currently working as an Associated Professor at the Department of Computer Engineering in North Tehran Branch, Islamic Azad University (IAU), 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 South Tehran branch, IAU in Tehran, Iran, respectively. He was honored Ph.D. degree in Computer Engineering from Science and Research Branch, IAU, Tehran, Iran in 2005. His current research interests are Scheduling, QoS, MANETs, Wireless Sensor Networks and Cloud Computing.

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, Tehran, Iran. He also received his bachelor's and master's degrees from Amirkabir University, Tehran, Iran.

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