mathematics

MDPI

Article

OO-MA-KP-ABE-CRF: Online/Offline Multi-Authority Key-Policy Attribute-Based Encryption with Cryptographic Reverse Firewall for Physical Ability Data

You Zhao [1], Ye Fan [2,*] and Xuefen Bian [2,*]

[1] College of Physical Education, Harbin University, Harbin 150090, China; zhaoyou860321@163.com
[2] College of Data Science and Technology, Heilongjiang University, Harbin 150080, China
* Correspondence: fy180253@163.com (Y.F.); bianxuefen@hlju.edu.cn (X.B.)

Abstract: In many universities, students' physical ability data are collected and stored in the cloud through various sensing devices to save computational and storage costs. Therefore, how to effectively access data while ensuring data security has become an urgent issue. Key-policy attribute-based encryption (KP-ABE) not only enables secure one-to-many communication and fine-grained access control but also adapts to data sharing in static scenarios, making it more suitable for the cloud sharing of physical ability data. In this paper, we construct an online/offline multi-authority key-policy attribute-based encryption with a cryptographic reverse firewall for physical ability data. This scheme uses multi-authority to avoid the single point of failure crisis of a single authority, and is combined with a cryptographic reverse firewall to resist backdoor attacks. In addition, the scheme uses outsourcing decryption to save users' computing costs, and utilizes offline/online technology to move a large amount of computing offline, reducing the online burden. Finally, the experiment shows the feasibility of the scheme.

Keywords: MA-KP-ABE; physical ability data; online/offline; non-monotonic; cryptographic reverse firewall

MSC: 94A60; 68P25

Citation: Zhao, Y.; Fan, Y.; Bian, X. OO-MA-KP-ABE-CRF: Online/Offline Multi-Authority Key-Policy Attribute-Based Encryption with Cryptographic Reverse Firewall for Physical Ability Data. *Mathematics* **2023**, *11*, 3333. https://doi.org/10.3390/math11153333

Academic Editor: Cheng-Chi Lee

Received: 25 June 2023
Revised: 23 July 2023
Accepted: 27 July 2023
Published: 29 July 2023

1. Introduction

With the widespread use of sensing devices, various sensors carried by students can collect physical ability data, such as the time spent completing a long-distance race, the number of jump rope skips within a minute, and heart rate, and upload the collected data to the cloud for storage. For security, sensitive data should be encrypted before being stored in the cloud. ABE (attribute-based encryption) can achieve fine-grained access control over ciphertext while providing encryption for data, making it suitable for protecting students' physical ability data.

ABE has two types: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In the KP-ABE scheme, attributes are used to encrypt data, and the user's decryption key corresponds to an access structure. The decryption key can correctly decrypt the ciphertext if and only if the attribute satisfies the access structure. Firstly, before encrypting the physical ability data, it is not known which users want to share, and the access structure of these users may be different. Therefore, if CP-ABE is used to encrypt physical ability data, it may involve the need to convert ciphertext under one access structure to ciphertext under another access structure [1]. Secondly, due to the sensitivity of physical ability data, the system needs to maintain an audit log. As shown in [2], when the KP-ABE encryption scheme is adopted, the system uses attributes to encrypt the physical ability data. The data can only be decrypted and accessed by the user after obtaining the corresponding key of the specified access structure, thus effectively solving the audit log problem. Finally, due to

the fact that students' physical ability data are rarely updated after collection, KP-ABE is more suitable for data sharing in static scenarios. So, compared to CP-ABE, using KP-ABE is more suitable for physical ability data encryption.

However, most KP-ABE schemes are single-authority, leading to a single point of failure crisis and making the cross-organizational sharing of confidential information challenging. The high computational overhead of KP-ABE is also a problem. The large attribute universe and flexible access structures both increase the time required for encryption and key generation. So, we need to adopt effective techniques to improve the efficiency of the KP-ABE scheme. In addition, Edward Snowden's revelations indicate that even provably secure cryptographic schemes may face the risk of privacy leakage. Adversaries can obtain users' confidential information through an undetectable backdoor, endangering their privacy and security.

To address these issues, we combined KP-ABE, multi-authority, online/offline and crypto reverse firewall (CRF) capabilities to construct an online/offline multi-authority KP-ABE with a cryptographic reverse firewall (OO-MA-KP-ABE-CRF) for students' physical ability data. The following are the specific contributions:

(1) We propose a novel OO-MA-KP-ABE-CRF scheme without a central attribute authority to coordinate key distribution between attribute authorities, while also supporting non-monotonic access structure, making the access control structure more flexible.
(2) To meet the usage demands of lightweight terminal devices, our proposed scheme utilizes online/offline technology and outsourced decryption to improve efficiency.
(3) We prove the correctness and security of the proposed OO-MA-KP-ABE-CRF scheme, which encompasses CPA security, weak security preservation, and weak demonstration resistance. These security aspects indicate that even in the face of potential backdoor attacks, the scheme can still ensure its security and functionality.

The remainder of this paper is as follows: Section 2 outlines the related work. Section 3 provides the preliminaries. Section 4 details the proposed OO-MA-KP-ABE-CRF scheme. Section 5 provides the performance analysis. Finally, the conclusion is presented in Section 6.

2. Related Work

This section provides a summary of related works on ABE, CRF, and online/offline cryptography.

2.1. Attribute-Based Encryption

Goyal et al. [2] classified ABE into two types: KP-ABE and CP-ABE. Due to the richness of access structures, the research and application of ABE have received increasing attention, but currently, most ABE access structures are focused on monotonic access structures. In order to enrich the expression of access structures, Yamada et al. [3] modularized KP-ABE and proved that any special-type predicate encryption satisfying certain conditions can be transformed into the non-monotonic KP-ABE format. Subsequently, Attrapadung et al. [4] designed an attribute-based signature supporting non-monotonic span programs by studying predicate encryption schemes and implementing constant-size signature technology. Moreover, ABE serves as a prevalent privacy protection method, playing a crucial role in safeguarding personal privacy and ensuring the secure communication of data in various domains such as cloud computing, medical insurance, intelligent transportation, and the Internet of Things. For instance, Zhang et al. [5] surveyed various ABE-based techniques for securing cloud data, Rasori et al. [6] proposed a KP-ABE scheme against the potential threat of malicious attacks of untrustworthy cloud servers, Kumar et al. [7] researched how to combine IoT with ABE to protect user privacy, and Jaiswal et al. [8] compared and analyzed various ABE schemes in medical privacy scenarios. In addition, there has been a plethora of research related to privacy protection, such as the adoption of the secure encryption random permutation pseudo algorithm (SERPPA) to enhance network security and energy efficiency [9], investigations into ABE in the post-quantum era [10], and the development of privacy-preserving schemes in federated learning [11], among others. Considering that almost all hierarchical ABEs are designed based

on CP-ABE schemes and only support monotonic access structures, Li et al. [12] proposed a hierarchical non-monotonic KP-ABE scheme. Therefore, non-monotonic ABE schemes offer more flexible access control than monotonic ABE and can better meet the complex authorization requirements in practical applications.

2.2. Cryptographic Reverse Firewall

Edward Snowden's revelations have revealed hidden backdoor vulnerabilities in many provably secure cryptographic algorithms. To defend against malicious data streams and prevent the leakage of public parameters, Mironov and Stephens-Devidowitz [13] introduced the CRF in 2015. The CRF is deployed between user machines and external networks to intercept incoming and outgoing data and update it in real-time, preventing potential backdoor threats. Dodis, Mironov, and Stephens-Devidowitz [14] designed an efficient secure transmission protocol based on the CRF framework, focusing on whether users can securely communicate with untrusted machines and others. Ma et al. [15] used bilinear pairing to construct a COO-CP-ABE-CRF scheme, which successfully reduced the overall computational cost compared to the original scheme without CRF, and developed a libabe library which is compatible with Android devices; the prototype has been implemented on laptops and mobile phones. Hong et al. [16] designed a MA-KP-ABE system based on CRF technology that supports non-monotonic access structures. They analyzed the system's performance using the Charm library. To resist keyword guessing attacks (KGA) initiated by dishonest cloud servers, Zhou et al. [17] combined public key encryption with keyword search (PEKS) with the CRF and designed a searchable public key encryption with CRF (SPKE-CRF). Furthermore, to meet data security sharing requirements in virtual worlds like the Metaverse, Zhao et al. [18] proposed a CP-ABE-CRF scheme with outsourcing decryption, offline encryption, and black-box tracing capabilities.

2.3. Online/Offline Cryptography

The high computational overhead of KP-ABE is a problem. To address this issue, Hohenberger et al. [19] proposed an OO-ABE scheme, which separates the original cryptographic algorithm into an offline and online phase. During the offline phase, the system performs data preprocessing to enable the fast assembly of encryption ciphertexts or keys in the online phase, resulting in significant time and overhead savings. Additionally, Cui et al. [20] proposed a novel keyword search scheme with online/offline attributes in the mobile cloud, which achieved cost savings and maintained data privacy and security. Therefore, online/offline technology has significant advantages in various privacy and security scenarios with real-time requirements, such as healthcare IoT, 5G communications, industrial IoT, etc. [21–26]. In order to address the issue of low efficiency in the operation of the medical Internet of Things, Li et al. [27] proposed a flexible and efficient ciphertext-policy attribute-based encryption scheme by integrating online/offline techniques and outsourced decryption. They also effectively ensured the security of the cryptographic algorithm through CRF. Overall, online/offline cryptography technology effectively reduces computational overhead in algorithms and brings significant advantages to various application areas.

3. Preliminaries

This introduces the preliminaries of the OO-MA-KP-ABE-CRF scheme.

3.1. Bilinear Group

For the multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ with the same prime order p, we define an efficiently computable bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that satisfies the following two properties:

(1) Bilinearity: One can compute $e(P^a, Q^b) = e(P, Q)^{ab}$ for any $P, Q \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$.
(2) Non-degeneracy: Let $g \in \mathbb{G}$ and $h \in \mathbb{G}$ be the generators. The equation $e(g, h) \neq 1$ always holds.

3.2. Access Structure

For a set of participants P, we define the attribute x to represent the elements in the set P, and each attribute x is either a positive attribute x or a negative attribute x'. Assuming that the set S includes all possible attributes, $\tilde{S} = \{x'|x \in S\}$ is the set of negative attributes derived from S. For a monotonic access structure $\mathbb{A}$ defined on the attribute set S, there always exists a corresponding non-monotonic access structure $\tilde{\mathbb{A}} = NM(\mathbb{A})$, where $S \in NM(\mathbb{A})$. When $N(S) \in \mathbb{A}$, there is $N(S) = S \cup \{x'|x \in P - S\}$.

3.3. Linear Secret Sharing Schemes

A linear secret sharing scheme (LSSS) involves (M, ρ) with the general attribute description U, where $M \in \mathbb{Z}_p^{l \times n}$ is a secret sharing matrix, and $\rho(M_i)$ is a corresponding attribute, where M_i is the i-th row of M . For the secret $s \in \mathbb{Z}_p$, we randomly select $y_2, \cdots, y_n \in \mathbb{Z}_p$, and then $\lambda_i = M_i(s, y_2, \cdots, y_n)^T$ is the share of secret value s corresponding to attribute $\rho(M_i)$. When reconstructing secret values s using the share λ_i, there exists c_i such that $\sum_{i \in I} c_i M_i = (1, 0, \cdots, 0)$; thus, $\sum_{i \in I} c_i \lambda_i = s$, where $I = \{i : \rho(i) \in P\}$, and P is an authorized set.

3.4. Cryptographic Reverse Firewall

The CRF of party P is a state algorithm that outputs an updated state and message based on the input of the state and the message of party P. For a scheme satisfying functionality requirement and a party P, when the CRF is applied to P polynomial times, the functionality of the scheme is maintaining, it is called CRF maintaining functionality. If a scheme is secure, and the party P in the scheme is replaced with a combination of CRF and functionality-maintaining adversarial implementations, which still satisfies the security requirement, then it is called CRF weakly preserved security. If the corrupted functionality-maintaining implementation of party P cannot leak information through the CRF, then it is called CRF weakly exfiltration resistance. Further understanding of CRF can be found in reference [27].

4. System Model and Security Model

This introduces the system model, a real-world application, and a security model of the OO-MA-KP-ABE-CRF scheme.

4.1. System Model

The scheme includes five entities accompanied by their corresponding CRF. These entities are the global-identity authority (GA), attribute authorities (AA), the data owner (DO), the data user (DU), and the cloud service provider (CSP). Each entity is equipped with a CRF, namely $\mathcal{W}_{\mathrm{GA}}$ for GA, $\mathcal{W}_{\mathrm{AA}}$ for AA, $\mathcal{W}_{\mathrm{DO}}$ for DO, and $\mathcal{W}_{\mathrm{DU}}$ for DU. The global parameters GP are generated by GA. To mitigate potential compromises in this process, GP is randomized by $\mathcal{W}_{\mathrm{GA}}$ to obtain GP', and the updated results are broadcasted throughout the system. The AA generates a public/private key pair for itself and a decryption key for the user. Additionally, the AA's keys and the users' decryption keys are randomized by $\mathcal{W}_{\mathrm{AA}}$ to mitigate potential vulnerabilities. The CSP is responsible for offering services like cloud storage and outsourced decryption. The DO encrypts the data and then uploads it to the CSP. Given the potential risk of adversaries compromising critical encryption processes, $\mathcal{W}_{\mathrm{DO}}$ applies additional randomization to the ciphertext. Subsequently, the ciphertext is downloaded from the CSP and decrypted by DU. To mitigate potential vulnerabilities in the outsourced decryption key generation process, $\mathcal{W}_{\mathrm{DU}}$ randomizes the keys used for outsourced decryption.

Let U denote the general attribute description, while $\tilde{\mathbb{A}}$ represents a non-monotonic access structure. The OO-MA-KP-ABE-CRF for $\tilde{\mathbb{A}}$ consists of 17 algorithmic steps:

***Global*.Setup$(\lambda, U) \rightarrow GP$.** For the input security parameters λ and general attribute description U , GA runs the algorithm and outputs the global public parameters GP.

$\mathcal{W}_{\mathrm{GA}}$.*Global*.**Setup**$(GP) \rightarrow GP'$. For the input GP , $\mathcal{W}_{\mathrm{GA}}$ runs the algorithm and outputs the updated global public parameters GP'.

AA.Setup$(GP') \rightarrow (PK_k, SK_k)$. For the input GP', AA_k runs the algorithm and outputs the public key $PK_k$and private key SK_k for itself.

$\mathcal{W}_{\mathrm{AA}}$.**Setup**$(PK_k, SK_k) \rightarrow (PK'_k, SK'_k)$. For the input (PK_k, SK_k), $\mathcal{W}_{\mathrm{AA}}$ runs the algorithm and outputs the updated (PK'_k, SK'_k).

KeyGen.off$(GP', PK'_k, \mathcal{A}^k_C) \rightarrow D_{k.off}$. For the input GP', PK'_k, and $\mathcal{A}^k_C$, AA_k runs the algorithm and outputs the offline decryption key $D_{k.off}$ corresponding to $\mathcal{A}^k_C$.

KeyGen.on$(GP', D_{k.off}, SK'_k, \tilde{\mathbb{A}}_k, GID) \rightarrow D_{GID,k}$. For the input GP', $D_{k.off}$, SK'_k, the non-monotonic access structure $\tilde{\mathbb{A}}_k$ of AA_k, and GID, AA_k runs the algorithm and outputs the decryption key $\{D_{GID,k}\}_{i\in\tilde{\mathbb{A}}_k}$ for the user GID in AA_k. the user's decryption key $D_{GID} = \{D_{GID,k}\}_{k\in[K]}$.

$\mathcal{W}_{\mathrm{AA}}$.**KeyGen.off**$(GP', PK'_k, \mathcal{A}^k_C) \rightarrow D'_{k.off}$. For the input GP', PK'_k and $\mathcal{A}^k_C$, $\mathcal{W}_{\mathrm{AA}}$ runs the algorithm and outputs the the updated $D'_{k.off}$.

$\mathcal{W}_{\mathrm{AA}}$.**KeyGen.on**$(GP', D'_{k.off}, D_{GID,k}) \rightarrow D'_{GID,k}$. For the input GP', $D'_{k.off}$ and $D_{GID,k}$, $\mathcal{W}_{\mathrm{AA}}$ runs the algorithm and outputs the updated $D'_{GID,k}$. Let $D'_{GID} = \{D'_{GID,k}\}_{k\in[K]}$.

Encrypt.off$(GP', PK'_k) \rightarrow CT_{off}$. For the input GP' and PK'_k, DO runs the algorithm and outputs the CT_{off}.

Encrypt.on$(m, CT_{off}, \mathcal{A}_u) \rightarrow CT$. For the input m, CT_{off} and $\mathcal{A}_u$, DO runs the algorithm and outputs the ciphertext CT.

$\mathcal{W}_{\mathrm{DO}}$.**Encrypt.off**$(GP', PK'_k) \rightarrow IT$. For the input GP' and PK'_k, $\mathcal{W}_{\mathrm{DO}}$ runs the algorithm offline and outputs the IT.

$\mathcal{W}_{\mathrm{DO}}$.**Encrypt.on**$(CT, IT) \rightarrow CT'$. For the input CT and IT, $\mathcal{W}_{\mathrm{DO}}$ runs the algorithm online and outputs the CT'.

KeyGen.ran$(D'_{GID,k}) \rightarrow (TK, RK)$. For the input $D'_{GID,k}$, DU runs the algorithm and outputs the conversion key TK and the retrieval key RK.

$\mathcal{W}_{\mathrm{DU}}$.**TKUpdate**$(TK) \rightarrow TK'$. For the input TK , $\mathcal{W}_{\mathrm{DU}}$ runs the algorithm and outputs the TK' and a value δ.

Decrypt.out$(CT', TK') \rightarrow TCT$. For the input CT' and TK', CSP runs the algorithm and outputs the TCT.

$\mathcal{W}_{\mathrm{DU}}$.**Decrypt**$(TCT, \delta) \rightarrow TCT'$. For the input TCT and δ , $\mathcal{W}_{\mathrm{DU}}$ runs the algorithm and outputs the TCT'.

Decrypt.user$(TCT', RK) \rightarrow m$. For the input TCT' and RK, DU performs the final computation to produce the plaintext m as output.

Correctness: For $\lambda \in \mathbb{N}$, U, an access structure P and a message m, the correctness holds: for all $\mathcal{A}^k_C, \mathcal{A}_u \subseteq U, \tilde{\mathbb{A}}_k \in P$, all $GP \leftarrow Global.\mathrm{Setup}(\lambda, U)$, all $GP' \leftarrow \mathcal{W}_{\mathrm{GA}}.Global.\mathrm{Setup}(GP)$, all $(PK_k, SK_k) \leftarrow \mathrm{AA.Setup}(GP')$, all $(PK'_k, SK'_k) \leftarrow \mathcal{W}_{\mathrm{AA}}.\mathrm{Setup}(PK_k, SK_k)$, all $D_{k.off} \leftarrow \mathrm{KeyGen.off}(GP', PK'_k, \mathcal{A}^k_C)$, all $D_{GID,k} \leftarrow \mathrm{KeyGen.on}(GP', D_{k.off}, SK'_k, \tilde{\mathbb{A}}_k, GID)$, all $D'_{k.off} \leftarrow \mathcal{W}_{\mathrm{AA}}.\mathrm{KeyGen.off}(GP', PK'_k, \mathcal{A}^k_C)$, all $D'_{GID,k} \leftarrow \mathcal{W}_{\mathrm{AA}}.\mathrm{KeyGen.on}(GP', D'_{k.off}, D_{GID,k})$, all $CT_{off} \leftarrow \mathrm{Encrypt.off}(GP', PK'_k)$, all $CT \leftarrow \mathrm{Encrypt.on}(m, CT_{off}, \mathcal{A}_u)$, all $IT \leftarrow \mathcal{W}_{\mathrm{DO}}.\mathrm{Encrypt.off}(GP', PK'_k)$, all $CT' \leftarrow \mathcal{W}_{\mathrm{DO}}.\mathrm{Encrypt.on}(CT, IT)$, all $(TK, RK) \leftarrow \mathrm{KeyGen.ran}(D'_{GID,k})$, all $TK' \leftarrow \mathcal{W}_{\mathrm{DU}}.\mathrm{TKUpdate}(TK)$, all $TCT \leftarrow \mathrm{Decrypt.out}(CT', TK')$, all $TCT' \leftarrow \mathcal{W}_{\mathrm{DU}}.\mathrm{Decrypt}(TCT, \delta)$, if $\mathcal{A}_u$ satisfies $\tilde{\mathbb{A}}_k$, we have $m \leftarrow \mathrm{Decrypt.user}(TCT', RK)$.

4.2. Real-World Application

We describe the practical workflow of OO-MA-KP-ABE-CRF for physical ability data, as shown in Figure 1.

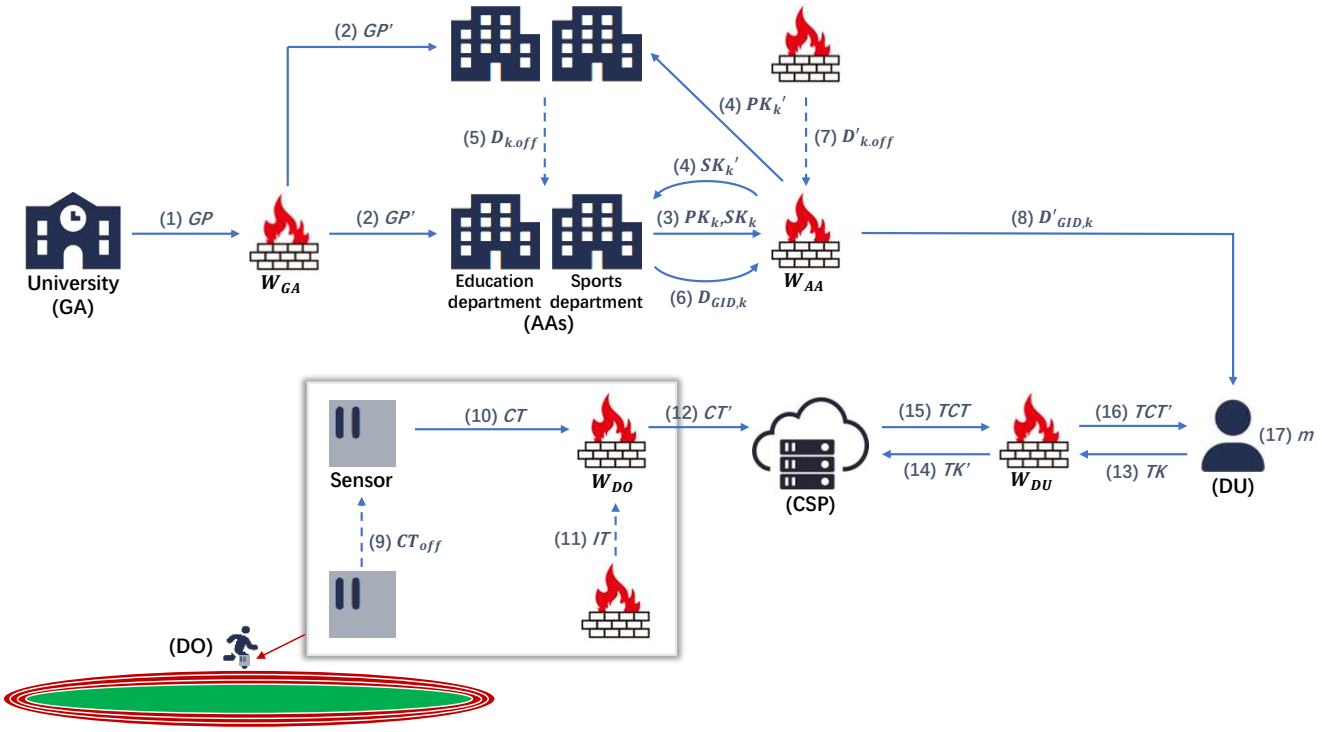


Figure 1. Practical workflow of OO-MA-KP-ABE-CRF.

Setup phase: (1) Students participating in physical ability tests register their identities on the school platform based on their attributes, such as college, grade, age, and so on. (2) The university calculates global parameters based on these attributes and the CRF of the university randomly updates these parameters. (3) Each department (attribute authority) within the university, such as the education department and the sports department as an attribute authority, independently generates public/private key pairs in the system. (4) To prevent information leakage, the CRF of each department randomizes the update of public/private key pairs.

Key generation phase: (5) and (6) The offline phase is responsible for generating offline keys, while the online phase is responsible for assembling offline keys and generating keys. (7) and (8) Finally, the corresponding CRF of each department updates and outputs the decryption key for the user.

Encryption phase: (9) In physical ability testing, the sensors worn by students collect their current physical ability data in real time. After obtaining the ciphertext by encrypting the data using the attributes, it is then uploaded to the CSP. (10) The offline/online technology is used in the encryption for saving computational costs. (11) and (12) The ciphertext generated by the sensors is not immediately sent to the CSP but is first transmitted to the CRF, which updates and transforms the ciphertext.

Decryption phase: (13) Authorized teachers with specific access structures plan to access the physical ability data of students stored in the CSP through mobile devices. They first generate a conversion key and retrieval key based on the obtained decryption key. The conversion key is sent to the CSP for outsourced decryption, while the retrieval key is retained by the teacher. (14) Before sending to CSP, the conversion key is updated by the CRF of the mobile device. (15)(16) After receiving the updated conversion key, CSP runs decryption and sends the result to CRF of the mobile device. (17) Ultimately, the teacher successfully recovers the physical ability data of the students using the retrieval key.

4.3. Security Model

We present the security model for the OO-MA-KP-ABE-CRF scheme based on [16,27].

Adversarial Model: We assume the full trustworthiness of GA, AA, DO, and DC, and the semi-trust of CSP. Given that Global.Setup, AA.Setup, KeyGen.off, KeyGen.on, Encrypt.off, Encrypt.on, and KeyGen.ran in the scheme remain functional despite the presence of malicious backdoors, it is important to consider that they may be compromised without the knowledge of the executing parties. Owing to the curiosity of $\mathcal{W}_{\mathrm{DO}}$ and $\mathcal{W}_{\mathrm{DU}}$ regarding user data, we assume that $\mathcal{W}_{\mathrm{DO}}$ and $\mathcal{W}_{\mathrm{DU}}$ are semi-trusted. Since $\mathcal{W}_{\mathrm{AA}}$ has access to users' decryption keys, we assume that $\mathcal{W}_{\mathrm{AA}}$ is fully trusted. Furthermore, all CRFs are regarded as trusted domains and are immune to external tampering.

The selective-set CPA security game for the scheme is played by a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Init: The $\mathcal{A}$ publicizes the set of AA_k, along with the corresponding attribute set $\mathcal{A}_u = \mathcal{A}_u^1, \cdots, \mathcal{A}_u^K$. The $\mathcal{A}$ sends algorithms $Global$.Setup*, AA.Setup*, KeyGen.off*, KeyGen.on*, KeyGen.ran*, Encrypt.off*, and Encrypt.on* to the $\mathcal{C}$.

Setup: The $\mathcal{C}$ obtains $GP \leftarrow Global.\mathrm{Setup}^*(\lambda, U)$, $GP' \leftarrow \mathcal{W}_{\mathrm{GA}}.Global.\mathrm{Setup}(GP)$, $(PK_k, SK_k) \leftarrow \mathrm{AA.Setup}^*(GP')$, and $(PK_k', SK_k') \leftarrow \mathcal{W}_{\mathrm{AA}}.\mathrm{Setup}^*(PK_k, SK_k)$, and then sends GP', the PK_k' of the honest authority, and the (PK_k', SK_k') of the corrupted authority to the $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can adaptively issue queries to the AA_k. When the access structure $\mathbb{A}_k$ satisfies the attribute $\mathcal{A}_u$, the honest AA_k refuse to answer, and otherwise answer the corresponding private key. For each query, the $\mathcal{C}$ runs $D_{k.off} \leftarrow \mathrm{KeyGen.off}^*(GP', PK_k', \mathcal{A}_C^k)$, $D_{GID,k} \leftarrow \mathrm{KeyGen.on}^*(GP', D_{k.off}, SK_k', \tilde{\mathbb{A}}_k, GID)$, $D_{k.off}' \leftarrow \mathcal{W}_{\mathrm{AA}}.\mathrm{KeyGen.off}(GP', PK_k', \mathcal{A}_C^k)$, $D_{GID,k}' \leftarrow \mathcal{W}_{\mathrm{AA}}.\mathrm{KeyGen.on}(GP', D_{k.off}', D_{GID,k})$, $(TK, RK) \leftarrow \mathrm{KeyGen.ran}^*(D_{GID,k}')$, $TK' \leftarrow \mathcal{W}_{\mathrm{DU}}.\mathrm{TKUpdate}(TK)$, and sends $\left(D_{GID,k}', TK'\right)$ as a response to the adversary $\mathcal{A}$.

Challenge: The $\mathcal{A}$ sends two plaintexts, m_0 and m_1, of equal length to the challenger $\mathcal{C}$. Then, $\mathcal{C}$ randomly selects $b \in \{0,1\}$ and runs $CT_{off} \leftarrow \mathrm{Encrypt.off}^*(GP', PK_k')$, $CT_b \leftarrow \mathrm{Encrypt.on}^*(m_b, CT_{off}, \mathcal{A}_u)$, $IT \leftarrow \mathcal{W}_{\mathrm{DO}}.\mathrm{Encrypt.off}(GP', PK_k')$, $CT_b' \leftarrow \mathcal{W}_{\mathrm{DO}}.\mathrm{Encrypt.on}(CT_b, IT)$. Finally, $\mathcal{C}$ sends CT_b' to the $\mathcal{A}$.

Phase 2: Same as Phase 1.

Guess: The $\mathcal{A}$ outputs a guess b' for b.

Definition 1. *If all PPT adversaries have at most negligible advantages in the above game, then the OO-MA-KP-ABE-CRF scheme is selective-set CPA-secure.*

5. OO-MA-KP-ABE-CRF

Firstly, a basic OO-MA-KP-ABE scheme is proposed. Then, we construct the OO-MA-KP-ABE-CRF scheme, and finally show the security.

5.1. Basic Construction of OO-MA-KP-ABE Scheme

Based on the KP-ABE scheme [28], this section introduces the OO- KP-ABE scheme using a decentralized approach similar to [29] incorporating the user's identity GID. Compared with [30], our scheme not only resists collusion attacks, but also eliminates the need for a central attribute authority to coordinate the key distribution among attribute authorities.

(1) $\boldsymbol{Global.\mathrm{Setup}(\lambda, U) \rightarrow \mathrm{GP}}$. The system selects $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, with prime order p, and randomly selects generators g and h of the group $\mathbb{G}$ and hash functions $H, F : \{0,1\}^* \rightarrow \mathbb{G}$. Finally, the system outputs $GP = \{g, h, H(\cdot), F(\cdot)\}$.

(2) $\boldsymbol{\mathrm{AA.Setup}(GP) \rightarrow (PK_k, SK_k)}$. For $k \in [K]$, attribute authority AA_k randomly selects $\alpha_{k1}, \alpha_{k2}, b_k \leftarrow \mathbb{Z}_p$ and computes $\alpha_k = \alpha_{k1} \cdot \alpha_{k2}$. Finally, we compute and output the public key $PK_k = \{g_{k1} = g^{\alpha_{k1}}, g_{k2} = g^{\alpha_{k2}}, g^{b_k}, g^{b_k^2}, h^{b_k}, e(g,g)^{\alpha_k}\}$, while retaining the secret key $SK_k = \{\alpha_{k1}, \alpha_{k2}, b_k\}$.

(3) **KeyGen.off**$(GP, PK_k, \mathcal{A}_C^k) \rightarrow D_{k.off}$. For $x_i \in \mathcal{A}_C^k$, AA_k randomly selects $r_{k,i} \leftarrow \mathbb{Z}_p$, calculates $D_{k,i}^{(1)} = H(x_i)^{r_{k,i}}$, $D_{k,i}^{(2)} = g^{r_{k,i}}$, $D_{k,i}^{(3)} = g^{b_k^2 r_{k,i}}$, $D_{k,i}^{(4)} = g^{r_{k,i} b_k x_i} h^{r_{k,i}}$, $D_{k,i}^{(5)} = g^{-r_{k,i}}$, and finally outputs $D_{k.off} = \{D_{k,i}^{(1)}, D_{k,i}^{(2)}, D_{k,i}^{(3)}, D_{k,i}^{(4)}, D_{k,i}^{(5)}\}_{i \in \mathcal{A}_C^k}$.

(4) **KeyGen.on**$(GP, D_{k.off}, SK_k, \tilde{\mathbb{A}}_k, GID) \rightarrow D_{GID.k}$. AA_k selects the non-monotonic access structure $\tilde{\mathbb{A}}_k$, which associates with an LSS matrix (M, ρ). By utilizing the LSSS mechanism Π, we can acquire the share $\{\lambda_{k,i}\}$ of α_{k1} and the share $\{\omega_{k,i}\}$ of 0, where $\lambda_{k,i} = M_i \lambda$, λ is a random vector with the first term being α_{k1}. $\omega_{k,i} = M_i \omega$, where ω is a random vector with the first term being 0. M_i is row i of M, $i \in [l], l \leq P$, and P is the maximum number of row of M.
If $\rho(i) = x_i$ is non-negative, calculating

$$D_{k,i}^{(1)\prime} = g_{k2}^{\lambda_{k,i}} \cdot D_{k,i}^{(1)} \cdot F(GID)^{\omega_{k,i}} = g_{k2}^{\lambda_{k,i}} H(x_i)^{r_{k,i}} F(GID)^{\omega_{k,i}}, D_{k,i}^{(2)\prime} = D_{k,i}^{(2)} = g^{r_{k,i}},$$

then we let $D_{k,i} = (D_{k,i}^{(1)\prime}, D_{k,i}^{(2)\prime})$.
If $\rho(i) = x_i{}'$ is negative, calculating

$$D_{k,i}^{(3)\prime} = g_{k2}^{\lambda_{k,i}} \cdot D_{k,i}^{(3)} \cdot F(GID)^{\omega_{k,i}} = g_{k2}^{\lambda_{k,i}} g^{b_k^2 r_{k,i}} F(GID)^{\omega_{k,i}},$$

$$D_{k,i}^{(4)\prime} = D_{k,i}^{(4)} = g^{r_{k,i} b_k x_i} h^{r_{k,i}}, D_{k,i}^{(5)\prime} = D_{k,i}^{(5)} = g^{-r_{k,i}},$$

then we let $D_{k,i} = (D_{k,i}^{(3)\prime}, D_{k,i}^{(4)\prime}, D_{k,i}^{(5)\prime})$. Finally, we output the decryption key $D_{GID.k} = \{D_{k.i}\}_{i \in [l]}$ of the user GID in AA_k. The user's decryption key $D_{GID} = \{D_{GID,k}\}_{k \in [K]}$.

(5) **KeyGen.ran**$(D_{GID,k}) \rightarrow (TK, RK)$. With input D_{GID}, the user GID randomly selects $\tau \leftarrow \mathbb{Z}_p$.
If $\rho(i) = x_i$ is non-negative, let

$$\hat{D}_{k,i} = (\hat{D}_{k,i}^{(1)}, \hat{D}_{k,i}^{(2)}) = (D_{k,i}^{(1)\prime \frac{1}{\tau}}, D_{k,i}^{(2)\prime \frac{1}{\tau}}) = (g_{k2}^{\frac{\lambda_{k,i}}{\tau}} F(GID)^{\frac{\omega_{k,i}}{\tau}} H(x_i)^{\frac{r_{k,i}}{\tau}}, g^{\frac{r_{k,i}}{\tau}}).$$

If $\rho(i) = x_i{}'$ is negative, let

$$\hat{D}_{k,i} = (\hat{D}_{k,i}^{(3)}, \hat{D}_{k,i}^{(4)}, \hat{D}_{k,i}^{(5)}) = (D_{k,i}^{(3)\prime \frac{1}{\tau}}, D_{k,i}^{(4)\prime \frac{1}{\tau}}, D_{k,i}^{(5)\prime \frac{1}{\tau}}) = (g_{k2}^{\frac{\lambda_{k,i}}{\tau}} F(GID)^{\frac{\omega_{k,i}}{\tau}} g^{\frac{b_k^2 r_{k,i}}{\tau}}, g^{\frac{r_{k,i} b_k x_i}{\tau}} h^{\frac{r_{k,i}}{\tau}}, g^{-\frac{r_{k,i}}{\tau}}).$$

Finally, the conversion key $TK = \{\hat{D}_{k,i}\}_{k \in [K], i \in [l]}$ and the retrieval key $RK = \tau$ are generated and outputted.

(6) **Encrypt.off**$(GP, PK_k) \rightarrow CT_{off}$. For $\forall x_i \in \mathcal{A}_u$, the DO computes $C_k^{(1)} = \prod_{k=1}^{K} e(g,g)^{\alpha_k}$, $C_{k,i}^{(5)} = g^{b_k^2 x_i} h^{b_k}$ and outputs $CT_{off} = \{C_k^{(1)}, C_{k,i}^{(5)}\}_{x_i \in \mathcal{A}_u}$.

(7) **Encrypt.on**$(m, CT_{off}, \mathcal{A}_u) \rightarrow CT$. For $\forall x_i \in \mathcal{A}_u$, the DO randomly selects $s_i \leftarrow \mathbb{Z}_p$.
Let $s = \sum_{x_i \in \mathcal{A}_u} s_i$. The DO calculates $C^{(1)\prime} = m \cdot (C_k^{(1)})^s = m \cdot e(g,g)^{s(\sum_{k=1}^{K} \alpha_k)}$, $C^{(2)\prime} = g^s$, $C_i^{(3)\prime} = H(x_i)^s$, $C_k^{(4)\prime} = \{g^{b_k s}\}_{k \in [K]}$, $C_{k,i}^{(5)\prime} = (C_{k,i}^{(5)})^s = g^{b_k^2 s x_i} h^{b_k s}$ and outputs $CT = \{C^{(1)\prime}, C^{(2)\prime}, C_i^{(3)\prime}, C_k^{(4)\prime}, C_{k,i}^{(5)\prime}\}$.

(8) **Decrypt.out**$(TK, CT) \rightarrow TCT$. Let the attribute set $\mathcal{A}_u = \mathcal{A}_u^1, \cdots, \mathcal{A}_u^K$. If $\mathcal{A}_u^k \notin \tilde{\mathbb{A}}_k$, we terminate the process and output $\perp$. If $\mathcal{A}_u^k \in \tilde{\mathbb{A}}_k$, then $\mathcal{A}_u^{k\prime} = N(\mathcal{A}_u^k) \in \mathbb{A}_k$, where $\tilde{\mathbb{A}}_k$ is the corresponding non-monotonic access structure of $\mathbb{A}_k$. Let $I = \{i : \rho(i) \in \mathcal{A}_u^{k\prime}\}$.
If $\rho(i) = x$, we have $Z_{k,i} = \frac{e(\hat{D}_{k,i}^{(1)}, C^{(2)\prime})}{e(\hat{D}_{k,i}^{(2)}, C_{k,i}^{(3)\prime})} = e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}}$.
If $\rho(i) = x'$, we obtain

$$
\begin{aligned}
Z_{k,i} &= \frac{e(\hat{D}_{k,i}^{(3)}, C^{(2)\prime})}{e(\hat{D}_{k,i}^{(4)}, \prod_{x_j \in \mathcal{A}_u^k} C_k^{(4)\prime \frac{1}{x_i - x_j}}) \cdot e(\hat{D}_{k,i}^{(5)}, \prod_{x_j \in \mathcal{A}_u^k} C_{k,j}^{(5)\prime \frac{1}{x_i - x_j}})} \\
&= \frac{e(g_{k2}^{\frac{\lambda_{k,i}}{\tau}} F(GID)^{\frac{\omega_{k,i}}{\tau}} g^{\frac{b_k^2 r_{k,i}}{\tau}}, g^s)}{e(g^{\frac{r_{k,i} b_k x_i}{\tau}} h^{\frac{r_{k,i}}{\tau}}, \prod_{x_j \in \mathcal{A}_u^k} (g^{b_k s})^{\frac{1}{x_i - x_j}}) \cdot e(g^{-\frac{r_{k,i}}{\tau}}, \prod_{x_j \in \mathcal{A}_u^k} (g^{b_k^2 s x_j} h^{b_k s})^{\frac{1}{x_i - x_j}})} \\
&= \frac{e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}} e(g, g)^{\frac{b_k^2 r_{k,i} s}{\tau}}}{e(g^{\frac{r_{k,i} b_k x_i}{\tau}} h^{\frac{r_{k,i}}{\tau}}, \prod_{x_j \in \mathcal{A}_u^k} (g^{b_k s})^{\frac{1}{x_i - x_j}}) \cdot e(g^{-\frac{r_{k,i}}{\tau}}, \prod_{x_j \in \mathcal{A}_u^k} (g^{b_k^2 s x_j \cdot \frac{1}{x_i - x_j}} h^{b_k s \cdot \frac{1}{x_i - x_j}}))} \\
&= \frac{e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}} e(g, g)^{\frac{b_k^2 r_{k,i} s}{\tau}}}{e(g^{\frac{r_{k,i} b_k x_i}{\tau}} h^{\frac{r_{k,i}}{\tau}}, g^{b_k s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{1}{x_i - x_j}}) \cdot e(g^{-\frac{r_{k,i}}{\tau}}, g^{b_k^2 s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{x_j}{x_i - x_j}} h^{b_k s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{1}{x_i - x_j}})} \\
&= \frac{e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}} e(g, g)^{\frac{b_k^2 r_{k,i} s}{\tau}}}{e(g,g)^{\frac{r_{k,i} b_k^2 s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{x_i}{x_i - x_j}}{\tau}} \cdot e(h,g)^{\frac{r_{k,i} b_k s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{1}{x_i - x_j}}{\tau}} \cdot e(g,g)^{\frac{r_{k,i} b_k^2 s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{-x_j}{x_i - x_j}}{\tau}} \cdot e(g,h)^{\frac{-r_{k,i} b_k s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{1}{x_i - x_j}}{\tau}}} \\
&= \frac{e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}} e(g, g)^{\frac{b_k^2 r_{k,i} s}{\tau}}}{e(g,g)^{\frac{r_{k,i} b_k^2 s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{x_i}{x_i - x_j}}{\tau}} \cdot e(g,g)^{\frac{r_{k,i} b_k^2 s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{-x_j}{x_i - x_j}}{\tau}}} \\
&= \frac{e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}} e(g, g)^{\frac{b_k^2 r_{k,i} s}{\tau}}}{e(g,g)^{\frac{r_{k,i} b_k^2 s \cdot \sum_{x_j \in \mathcal{A}_u^k} \frac{x_i - x_j}{x_i - x_j}}{\tau}}} \\
&= \frac{e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}} e(g, g)^{\frac{b_k^2 r_{k,i} s}{\tau}}}{e(g,g)^{\frac{r_{k,i} b_k^2 s}{\tau}}} \\
&= e(g_{k2}, g)^{\frac{\lambda_{k,i} s}{\tau}} e(F(GID), g)^{\frac{\omega_{k,i} s}{\tau}}.
\end{aligned}
$$

Since $\mathcal{A}_u^{k\prime} = N(\mathcal{A}_u^k) \in \mathbb{A}_k$, the decryptor can choose constants c_i such that $\sum_i c_i M_i = (1, 0, \cdots, 0)$. Computing $Z_k = \prod_{x_i \in \mathcal{A}_u^k} Z_{k,i}{}^{c_i} = e(g^{\alpha_{k2}}, g)^{\frac{\alpha_{k1} \cdot s}{\tau}} = e(g,g)^{\frac{\alpha_k \cdot s}{\tau}}$, we obtain

$$
Z = \prod_{k=1}^{K} Z_k = \prod_{k=1}^{K} e(g,g)^{\frac{\alpha_k \cdot s}{\tau}} = e(g,g)^{\frac{s}{\tau} \cdot \sum_{k=1}^{K} \alpha_k},
$$

output $TCT = \{Z, C^{(1)\prime}\}$.

(9) **Decrypt.user(RK, TCT).** By $\frac{C^{(1)\prime}}{Z^\tau} = \frac{m \cdot e(g,g)^{s \cdot (\sum_{k=1}^{K} \alpha_k)}}{(e(g,g)^{\frac{s}{\tau} \cdot (\sum_{k=1}^{K} \alpha_k)})^\tau}$, we can obtain the plaintext m.

Theorem 1. *If the KP-ABE scheme of [28] is selective CPA-secure, then the OO-MA-KP-ABE scheme is also selective CPA-secure.*

Proof. The MA-KP-ABE scheme is constructed based on the KP-ABE scheme of [28]. We adopt the multi-authority technique of [29] and introduce user identity GID in the construction of the MA-KP-ABE scheme. Compared with [28], our MA-KP-ABE scheme generates the same public parameters and ciphertext as [28] during the Setup and Encrypt steps, and the Decrypt step is also the same as [28]. However, the decryption key generated in the KeyGen step is slightly different from [28]. The $D_{k,i}^{(1)\prime} = g_{k2}^{\lambda_{k,i}} H(x_i)^{r_{k,i}} F(GID)^{\omega_{k,i}}$, $D_{k,i}^{(3)\prime} = g_{k2}^{\lambda_{k,i}} g^{b_k^2 r_{k,i}} F(GID)^{\omega_{k,i}}$, which has more $F(GID)^{\omega_{k,i}}$ than the decryption key in [28]. Here, $\omega_{k,i}$ represents linear secret sharing for 0, and 0 is publicly known, so there is no unknown quantity about $F(GID)^{\omega_{k,i}}$ for the challenger. Therefore, the challenger can construct a semi-functional key similar to the structure in the security proof of [28]. Therefore,

the MA-KP-ABE scheme is secure. Furthermore, we utilize the key blinding technique of [30], and the proof follows a similar approach as presented in [30]. Therefore, it is easy to see that the theorem holds. □

5.2. Construction of OO-MA-KP-ABE-CRF

The system initially runs algorithm $Global.\text{Setup}(\lambda) \rightarrow GP$. Firstly, GP is sent to $\mathcal{W}_{\text{GA}}$. After running the following algorithm, $\mathcal{W}_{\text{GA}}$ sends the updated GP' to the other participants.

① $\mathcal{W}_{\text{GA}}.Global.\text{Setup}(GP) \rightarrow GP'$. After receiving GP from GA, the $\mathcal{W}_{\text{GA}}$ selects random $a, c \leftarrow \mathbb{Z}_p$, computes $g' = g^a$, $h' = h^c$, and outputs the updated global parameters $GP' = \{g', h', H(\cdot), F(\cdot)\}$.
After receiving GP', the attribute authority AA_k runs algorithm $\text{AA.Setup}(GP') \rightarrow (PK_k, SK_k)$, and sends the (PK_k, SK_k) to $\mathcal{W}_{\text{AA}}$. $\mathcal{W}_{\text{AA}}$ performs the following operations.

② $\mathcal{W}_{\text{AA}}.\text{Setup}(GP', PK_k, SK_k) \rightarrow (PK_k{}', SK_k{}')$. $\mathcal{W}_{\text{AA}}$ randomly selects $\hat{\alpha}'_{k1}, \hat{\alpha}'_{k2}, \hat{b}_k \leftarrow \mathbb{Z}_p$, and sets $\alpha_{k1}{}' = \alpha_{k1} + \hat{\alpha}'_{k1}$, $\alpha_{k2}{}' = \alpha_{k2} + \hat{\alpha}'_{k2}$, $\alpha_k{}' = \alpha_{k1}{}' \cdot \alpha_{k2}{}'$, and $b_k{}' = b_k + \hat{b}_k$. Then, we calculate $g_{k1}{}' = g'^{\alpha_{k1}{}'}$, $g_{k2}{}' = g'^{\alpha_{k2}{}'}$, and $e(g', g')^{\alpha_k{}'}$. Finally, the updated $PK_k{}' = \{g_{k1}{}', g_{k2}{}', g'^{b_k{}'}, g'^{b_k{}'^2}, h'^{b_k{}'}, e(g', g')^{\alpha_k{}'}\}$ and $SK_k{}' = \{\alpha_{k1}{}', \alpha_{k2}{}', b_k{}'\}$ are outputted.
When receiving the updated $PK_k{}'$ and $SK_k{}'$, AA_k runs $\text{KeyGen.off}(GP', PK'_k, \mathcal{A}^k_C) \rightarrow D_{k.off}$ and $\text{KeyGen.on}(GP', D_{k,off}, SK_k{}', \tilde{\mathbb{A}}) \rightarrow D_{GID,k}$. Before sending $D_{GID,k}$ to user GID, it is sent to $\mathcal{W}_{\text{AA}}$. The following operations are performed.

③ $\mathcal{W}_{\text{AA}}.\text{KeyGen.off}(GP', PK'_k, \mathcal{A}^k_C) \rightarrow D'_{k.off}$. For $\forall x_i \in \mathcal{A}^k_c$, $\mathcal{W}_{\text{AA}}$ randomly selects $\hat{r}_{k,i} \leftarrow \mathbb{Z}_p$, computes $\hat{D}^{(1)}_{k,i} = H(x_i)^{\hat{r}_{k,i}}$, $\hat{D}^{(2)}_{k,i} = g'^{\hat{r}_{k,i}}$, $\hat{D}^{(3)}_{k,i} = g'^{b_k{}'^2 \hat{r}_{k,i}}$, $\hat{D}^{(4)}_{k,i} = g'^{\hat{r}_{k,i} b_k{}' x_i} h'^{\hat{r}_{k,i}}$, and $\hat{D}^{(5)}_{k,i} = g'^{-\hat{r}_{k,i}}$, and outputs $D'_{k,off} = (\hat{D}^{(1)}_{k,i}, \hat{D}^{(2)}_{k,i}, \hat{D}^{(3)}_{k,i}, \hat{D}^{(4)}_{k,i}, \hat{D}^{(5)}_{k,i})$.

④ $\mathcal{W}_{\text{AA}}.\text{KeyGen.on}(GP', D'_{k.off}, D_{GID,k}) \rightarrow D'_{GID,k}$. $\mathcal{W}_{\text{AA}}$ sets $r_{k,i}{}' = r_{k,i} + \hat{r}_{k,i}$, computes $\hat{D}^{(1)\prime}_{k,i} = D^{(1)\prime}_{k,i} \cdot \hat{D}^{(1)}_{k,i} = g_{k2}{}'^{\lambda_{k,i}} F(GID)^{\omega_{k,i}} H(x_i)^{r_{k,i}{}'}$, $\hat{D}^{(2)\prime}_{k,i} = D^{(2)\prime}_{k,i} \cdot \hat{D}^{(2)}_{k,i} = g'^{r_{k,i}{}'}$, $\hat{D}^{(3)\prime}_{k,i} = D^{(3)\prime}_{k,i} \cdot \hat{D}^{(3)}_{k,i} = g_{k2}{}'^{\lambda_{k,i}} F(GID)^{\omega_{k,i}} g'^{b_k{}'^2 r_{k,i}{}'}$, $\hat{D}^{(4)\prime}_{k,i} = D^{(4)\prime}_{k,i} \cdot \hat{D}^{(4)}_{k,i} = g'^{r_{k,i}{}' b_k{}' x_i} h'^{r_{k,i}{}'}$, $\hat{D}^{(5)\prime}_{k,i} = g'^{-r_{k,i}{}'}$. If $\rho(i) = x_i$ is non-negative, output $D'_{GID.k} = (\hat{D}^{(1)\prime}_{k,i}, \hat{D}^{(2)\prime}_{k,i})$. If $\rho(i) = x_i$ is negative, output $D'_{GID.k} = (\hat{D}^{(3)\prime}_{k,i}, \hat{D}^{(4)\prime}_{k,i}, \hat{D}^{(5)\prime}_{k,i})$.
$\mathcal{W}_{\text{AA}}$ sends $D'_{GID,k}$ to the users (DO and DU). DO generates ciphertext, CT, by running $\text{Encrypt.off}(GP', PK_k{}') \rightarrow CT_{off}$ and $\text{Encrypt.on}(m, CT_{off}, \mathcal{A}_u) \rightarrow CT$ and sends CT to $\mathcal{W}_{\text{DO}}$. The following operations are performed.

⑤ $\mathcal{W}_{\text{DO}}.\text{Encrypt.off}(GP', PK_k{}') \rightarrow IT$. For $\forall x_i \in \mathcal{A}_u$, the $\mathcal{W}_{\text{DO}}$ computes $\hat{C}^{(1)}_k = \sum_{k=1}^{K} e(g, g)^{\alpha'_k}, \hat{C}^{(5)}_{k,i} = \{g^{b'^2_k x_i} h^{b'_k}\}_{k \in [K]}$ and outputs $\hat{C}T_{off} = \{(\hat{C}^{(1)}_k, \hat{C}^{(5)}_{k,i})\}_{x_i \in \mathcal{A}_u}$.

⑥ $\mathcal{W}_{\text{DO}}.\text{Encrypt.on}(CT, IT) \rightarrow CT'$. For $\forall x_i \in \mathcal{A}_u$, the $\mathcal{W}_{\text{DO}}$ selects random $\hat{s}_i \leftarrow \mathbb{Z}_p$. $\mathcal{W}_{\text{DO}}$ sets $\hat{s} = \sum_{x_i \in \mathcal{A}_u} \hat{s}_i$ and $s' = s + \hat{s}$, computes $\hat{C}^{(1)\prime} = (C^{(1)\prime} \hat{C}^{(1)}_{k,i})^{s'} = m \cdot e(g', g')^{s' \cdot (\sum_{k=1}^{K} \alpha_k{}')}$, $\hat{C}^{(2)\prime} = g'^{s'}, \hat{C}^{(3)}_i{}\prime = H(x_i)^{s'}, \hat{C}^{(4)}_k{}' = g'^{b_k{}' s'}, \hat{C}^{(5)\prime}_{k,i} = C^{(5)}_{k,i}{}' \cdot (\hat{C}^{(5)}_{k,i})^{\hat{s}} = g'^{b_k{}'^2 s' x_i} h'^{b_k{}' s'}$, and outputs $CT' = (\hat{C}^{(1)\prime}, \hat{C}^{(2)\prime}, \hat{C}^{(3)\prime}_i, \hat{C}^{(4)\prime}_k, \hat{C}^{(5)\prime}_{k,i})$.
DU runs $\text{KeyGen.ran}(D'_{GID}) \rightarrow (TK, RK)$, and sends TK to $\mathcal{W}_{\text{DU}}$. $\mathcal{W}_{\text{DU}}$ performs the following operations:

⑦ $\mathcal{W}_{\text{DU}}.\text{TKUpdate}(TK) \rightarrow TK'$. $\mathcal{W}_{\text{DU}}$ randomly selects $\delta \leftarrow \mathbb{Z}_p$, computes $\tilde{D}^{(1)}_{k,i} = \hat{D}^{(1)\frac{1}{\delta}}_{k,i} = g_{k2}{}'^{\frac{\lambda_{k,i}}{\tau\delta}} \cdot F(GID)^{\frac{\omega_{k,i}}{\tau\delta}} \cdot H(x_i)^{\frac{r_{k,i}{}'}{\tau\delta}}$, $\tilde{D}^{(2)}_{k,i} = \hat{D}^{(2)\frac{1}{\delta}}_{k,i} = g'^{\frac{r_{k,i}{}'}{\tau\delta}}$, $\tilde{D}^{(3)}_{k,i} = \hat{D}^{(3)\frac{1}{\delta}}_{k,i} = g_{k2}{}'^{\frac{\lambda_{k,i}}{\tau\delta}} \cdot F(GID)^{\frac{\omega_{k,i}}{\tau\delta}} \cdot g'^{\frac{b_k{}'^2 r_{k,i}{}'}{\tau\delta}}$, $\tilde{D}^{(4)}_{k,i} = \hat{D}^{(4)\frac{1}{\delta}}_{k,i} = g'^{\frac{r_{k,i}{}' b_k{}' x_i}{\tau\delta}} h'^{\frac{r_{k,i}{}'}{\tau\delta}}$, $\tilde{D}^{(5)}_{k,i} = \hat{D}^{(5)\frac{1}{\delta}}_{k,i} = g'^{-\frac{r_{k,i}{}'}{\tau\delta}}$, and outputs the updated conversion key $TK' = \{\tilde{D}^{(1)}_{k,i}, \tilde{D}^{(2)}_{k,i}, \tilde{D}^{(3)}_{k,i}, \tilde{D}^{(4)}_{k,i}, \tilde{D}^{(5)}_{k,i}\}$. TK' is then sent to the CSP, while δ is retained.

The CSP executes algorithm Decrypt.out$(TK', CT') \rightarrow TCT$ and sends TCT to $\mathcal{W}_{\mathrm{DU}}$. $\mathcal{W}_{\mathrm{DU}}$ performs the following operations.

⑧ $\mathcal{W}_{\mathrm{DU}}$.Decrypt$(TCT, \delta) \rightarrow TCT'$. $\mathcal{W}_{\mathrm{DU}}$ computes $Z' = Z^{\delta} = e(g', g')^{\frac{s'}{\tau}\sum_{k=1}^{K}\alpha_k{}'}$ and outputs $TCT' = (Z', \hat{C}^{(1)\prime})$.
Upon receiving TCT', DU executes algorithm Decrypt.user to obtain m.

5.3. Security Analysis

Theorem 2. *The proposed OO-MA-KP-ABE-CRF is selective-set CPA-secure and contains reverse firewalls for GA, AAs, DO and DU, which maintains functionality, weakly preserves security, and weakly resists exfiltration if the basic structure of OO-MA-KP-ABE in Section 5.1 is selective-set CPA-secure.*

Proof. We prove the security through the following parts.

Functionality maintenance. Let the attribute set $\mathcal{A}_u = \mathcal{A}_u^1, \cdots, \mathcal{A}_u^K$. If $\mathcal{A}_u^k \notin \tilde{\mathbb{A}}_k$, terminate the process and output $\perp$. If $\mathcal{A}_u^k \in \tilde{\mathbb{A}}_k$, then $\mathcal{A}_u^{k\prime} = N(\mathcal{A}_u^k) \in \mathbb{A}_k$, where $\tilde{\mathbb{A}}_k$ is the corresponding non-monotonic access structure of $\mathbb{A}_k$. Let $I = \{i : \rho(i) \in \mathcal{A}_u^{k\prime}\}$. Algorithm $\mathcal{W}_{\mathrm{DU}}$.TKUpdate$(TK) \rightarrow TK'$ is executed to decrypt CT'.

If $\rho(i) = x$, calculate $Z_{k,i}{}' = \frac{e(\tilde{D}_{k,i}^{(1)}, \hat{C}^{(2)\prime})}{e(\tilde{D}_{k,i}^{(2)}, \hat{C}_i^{(3)\prime})} = \frac{e(g_{k2}{}'^{\frac{\lambda_{k,i}}{\tau\sigma}} F(GID)^{\frac{\omega_{k,i}}{\tau\sigma}} H(x_i)^{\frac{r_{k,i}{}'}{\tau\sigma}}, g'^{s'})}{e(g'^{\frac{r_{k,i}{}'}{\tau\sigma}}, H(x_i)^{s'})}$

$= \frac{e(g_{k2}{}', g')^{\frac{s'\cdot\lambda_{k,i}}{\tau\sigma}} \cdot e(F(GID), g')^{\frac{s'\cdot\omega_{k,i}}{\tau\sigma}} \cdot e(H(x_i), g')^{\frac{s'\cdot r_{k,i}{}'}{\tau\sigma}}}{e(g', H(x_i))^{\frac{s'\cdot r_{k,i}{}'}{\tau\sigma}}} = e(g_{k2}{}', g')^{\frac{s'\cdot\lambda_{k,i}}{\tau\sigma}} \cdot e(F(GID), g')^{\frac{s'\cdot\omega_{k,i}}{\tau\sigma}}.$

If $\rho(i) = x'$, then we can get

$$Z_{k,i}{}' = \frac{e(\tilde{D}_{k,i}^{(3)}, \hat{C}^{(2)\prime})}{e(\tilde{D}_{k,i}^{(4)}, \prod\limits_{x_j \in \mathcal{A}_u^k} \hat{C}_k^{(4)\prime\,\frac{1}{x_i - x_j}}) \cdot e(\tilde{D}_{k,i}^{(5)}, \prod\limits_{x_j \in \mathcal{A}_u^k} \hat{C}_{k,j}^{(5)\prime\,\frac{1}{x_i - x_j}})}$$

$$= \frac{e(g_{k2}{}'^{\frac{\lambda_{k,i}}{\tau\delta}} F(GID)^{\frac{\omega_{k,i}}{\tau\delta}} g'^{\frac{b_k{}'^2 r_{k,i}{}'}{\tau\delta}}, g'^{s'})}{e(g'^{\frac{r_{k,i}{}' b_k{}' x_i}{\tau\sigma}} h'^{\frac{r_{k,i}{}'}{\tau\sigma}}, \prod\limits_{x_j \in \mathcal{A}_u^k} (g'^{b_k{}' s'})^{\frac{1}{x_i - x_j}}) \cdot e(g'^{-\frac{r_{k,i}{}'}{\tau\sigma}}, \prod\limits_{x_j \in \mathcal{A}_u^k} (g'^{b_k{}'^2 s' x_j} h'^{b_k{}' s'})^{\frac{1}{x_i - x_j}})}$$

$$= \frac{e(g_{k2}{}', g')^{\frac{s'\cdot\lambda_{k,i}}{\tau\sigma}} \cdot e(F(GID), g')^{\frac{s'\cdot\omega_{k,i}}{\tau\sigma}} \cdot e(g', g')^{\frac{s'\cdot b_k{}'^2 r_{k,i}{}'}{\tau\sigma}}}{e(g'^{\frac{r_{k,i}{}' b_k{}' x_i}{\tau\sigma}} h'^{\frac{r_{k,i}{}'}{\tau\sigma}}, (g'^{b_k{}' s'})^{\sum\limits_{x_j \in \mathcal{A}_u^k} \frac{1}{x_i - x_j}}) \cdot e(g'^{-\frac{r_{k,i}{}'}{\tau\sigma}}, \prod\limits_{x_j \in \mathcal{A}_u^k} (g'^{b_k{}'^2 s' x_j})^{\frac{1}{x_i - x_j}} \cdot \prod\limits_{x_j \in \mathcal{A}_u^k} (h'^{b_k{}' s'})^{\frac{1}{x_i - x_j}})}$$

$$= \frac{e(g_{k2}{}', g')^{\frac{s'\cdot\lambda_{k,i}}{\tau\sigma}} \cdot e(F(GID), g')^{\frac{s'\cdot\omega_{k,i}}{\tau\sigma}} \cdot e(g', g')^{\frac{s'\cdot b_k{}'^2 r_{k,i}{}'}{\tau\sigma}}}{e(g'^{\frac{r_{k,i}{}' b_k{}' x_i}{\tau\sigma}} h'^{\frac{r_{k,i}{}'}{\tau\sigma}}, g'^{b_k{}' s' \cdot \sum\limits_{x_j \in \mathcal{A}_u^k} \frac{1}{x_i - x_j}}) \cdot e(g'^{-\frac{r_{k,i}{}'}{\tau\sigma}}, g'^{b_k{}'^2 s' \cdot \sum\limits_{x_j \in \mathcal{A}_u^k} \frac{x_j}{x_i - x_j}} \cdot h'^{b_k{}' s' \cdot \sum\limits_{x_j \in \mathcal{A}_u^k} \frac{1}{x_i - x_j}})}$$

$$= \frac{e(g_{k2}{}', g')^{\frac{s'\cdot\lambda_{k,i}}{\tau\sigma}} \cdot e(F(GID), g')^{\frac{s'\cdot\omega_{k,i}}{\tau\sigma}} \cdot e(g', g')^{\frac{s'\cdot b_k{}'^2 r_{k,i}{}'}{\tau\sigma}}}{e(g', g')^{\frac{r_{k,i}{}' b_k{}'^2 s'}{\tau\sigma} \cdot \sum\limits_{x_j \in \mathcal{A}_u^k} \frac{x_i - x_j}{x_i - x_j}}}$$

$$= e(g_{k2}{}', g')^{\frac{s'\cdot\lambda_{k,i}}{\tau\sigma}} \cdot e(F(GID), g')^{\frac{s'\cdot\omega_{k,i}}{\tau\sigma}}$$

Since $\mathcal{A}_u^{k\prime} = N(\mathcal{A}_u^k) \in \mathbb{A}_k$, the decryptor can choose constants c_i such that $\sum_i c_i M_i = (1, 0, \cdots, 0)$. then $Z_k{}' = \prod\limits_{x_i \in \mathcal{A}_u^k} Z'^{\,c_i}_{k,i} = e(g', g')^{\frac{s'\cdot\alpha_{k1}{}'\cdot\alpha_{k2}{}'}{\tau\sigma}} = e(g', g')^{\frac{s'\cdot\alpha_k{}'}{\tau\sigma}}$ and $Z' = \prod\limits_{k=1}^{K} Z_k{}' =$

$e(g', g')^{\frac{s'}{\tau\sigma} \cdot \sum_{k=1}^{K} \alpha_k'}$. Finally, we can execute $\frac{\hat{C}^{(1)\prime}}{((Z')^{\sigma})^{\tau}} = \frac{m \cdot e(g', g')^{s' \cdot \sum_{k=1}^{K} \alpha_k'}}{((e(g', g')^{\frac{s'}{\tau\sigma} \cdot \sum_{k=1}^{K} \alpha_k'})^{\sigma})^{\tau}} = m$ to successfully recover the plaintext.

Selectibe-set CPA-secure. We show through game hopping that the security game of OO-MA-KP-ABE-CRF is indistinguishable from that of OO-MA-KP-ABE. Based on the security of OO-MA-KP-ABE in Section 5.1, we find the selective-set CPA security of the proposed OO-MA-KP-ABE-CRF scheme.

Game 0. The security game is the same as the security game of OO-MA-KP-ABE-CRF presented in Section 4.3.

Game 1. The only difference from Game 0 is that GP, SK, and PK are generated by the setup, independent of *Global*.Setup*, $\mathcal{W}_{\mathrm{GA}}$.*Global*.Setup, AA.Setup*, and $\mathcal{W}_{\mathrm{AA}}$.Setup.

Game 2. The only difference from Game 1 is that in Phase 1 and Phase 2, the decryption key D_{GID} is generated by KeyGen.off and KeyGen.on, independent of algorithms KeyGen.off*, KeyGen.on*, $\mathcal{W}_{\mathrm{AA}}$.KeyGen.off, and $\mathcal{W}_{\mathrm{AA}}$.KeyGen.on. Additionally, the conversion key TK is generated by KeyGen.ran, independent of KeyGen.ran* and $\mathcal{W}_{\mathrm{DU}}$.TKUpdate.

Game 3. Apart from the challenge phase, the rest is the same as Game 2. The challenge ciphertext CT_b is generated by Encrypt.off and Encrypt.on, independent of Encrypt.off*, Encrypt.on*, $\mathcal{W}_{\mathrm{DO}}$.Encrypt.off, and $\mathcal{W}_{\mathrm{DO}}$.Encrypt.on. Note that Game 3 is the same as the security game of OO-MA-KP-ABE.

For any tampered *Global*.Setup*, because of $a, c \leftarrow \mathbb{Z}_p$, it can be known from key malleability that the GP' generated by $\mathcal{W}_{\mathrm{GA}}$.*Global*.Setup has the same uniform random distribution as the GP generated by *Global*.Setup in the basic construction. Similarly, due to $\hat{\alpha}_{k1}, \hat{\alpha}_{k2}, \hat{b}_k \leftarrow \mathbb{Z}_p$, for any tampered AA.Setup*, the (PK_k', SK_k')generated by $\mathcal{W}_{\mathrm{AA}}$.Setup has the same uniform random distribution as (PK_k, SK_k) generated by AA.Setup. So, we claim that Game 0 and Game 1 cannot be distinguished. Because $\hat{r}_{ki} \leftarrow \mathbb{Z}_p$, the LSSS is re-randomizable and D_{GID} and TK have key malleability, and Game 1 and Game 2 cannot be distinguished. For any tampered Encrypt.off* and Encrypt.on*, because of $\hat{s}_{k,i} \leftarrow \mathbb{Z}_p$, it can be known that the ciphertext generated by $\mathcal{W}_{\mathrm{DO}}$.Encrypt.off and $\mathcal{W}_{\mathrm{DO}}$.Encrypt.on is uniformly random, which is consistent with the distribution of ciphertext generated by the basic scheme. Therefore, based on the fact that Game 2 and Game 3 cannot be distinguished, we can find that Game 0 and Game 3 cannot be distinguished. Furthermore, since the basic scheme is selective-set CPA-secure, it follows that the proposed OO-MA-KP-ABE-CRF is selective-set CPA-secure.

Weak security preservation and weak exfiltration resistance. The selective-set CPA security of the OO-MA-KP-ABE-CRF scheme indicates that CRFs for GA, AA, DO, and DU maintain weak security preservation. Additionally, the indistinguishability between Game 0 and Game 3 suggests that $\mathcal{W}_{\mathrm{GA}}$, $\mathcal{W}_{\mathrm{AA}}$, $\mathcal{W}_{\mathrm{DO}}$ and $\mathcal{W}_{\mathrm{DU}}$ can weakly resist data exfiltration attacks.

With this discussion, we have successfully completed the proof of the scheme. □

6. Performance Evaluations

This section compares the proposed OO-MA-KP-ABE-CRF scheme with other ABE schemes from the perspectives of property comparison and performance analysis.

6.1. Property Comparison

We chose KP-ABE schemes [16,21,26] to compare their properties with the proposed schemes, as shown in Table 1. Although both the scheme presented in [16] and our proposed scheme are multi-authority, there is no central attribute authority to coordinate key distribution between attribute authorities in our scheme, which greatly reduces the time and cost associated with the setup phase. On the other hand, considering Edward Snowden's disclosure of backdoor attacks in known security schemes, the scheme presented in [16] and our proposed scheme adopt CRF to resist such attacks. To reduce the high

computational overhead caused by the combination of MA-ABE and CRF, Refs. [16,21] and our scheme adopt online/offline technology to improve the efficiency of the scheme. However, only our scheme considers both MA-ABE, online/offline technology and CRF.

Table 1. Comparison of properties.

Schemes	Multi-Authority	Online/Offline Key Generation	Online/Offline Encryption	CRF	Computation Outsourcing
[16]	✓	×	×	✓	×
[21]	×	×	×	×	✓
[26]	×	×	×	×	×
Proposed	✓	✓	✓	✓	✓

6.2. Performance Analysis

We compare [16,21,26], and our proposed scheme in terms of computational and storage costs. The comparison of the computational cost of system setup, user key generation, user encryption, and user decryption is shown in Table 2, and the comparison of the storage cost of public parameters, ciphertext, and user decryption key is shown in Table 3, where P represents the bilinear pairing operation, E represents the exponentiation operation on group $\mathbb{G}$, and M represents the multiplication operation on group $\mathbb{G}$. U represents the attribute universe, K denotes the number of attribute authorities, S indicates the number of attributes associated with the ciphertext, l represents the number of attributes involved in the access structure, and I represents the actual number of attributes used for decryption. $|\mathbb{G}|$ represents the elements in group $\mathbb{G}$, and $|\mathbb{G}_T|$ represents the elements in group $\mathbb{G}_T$.

Table 2. Comparison of computational costs.

Schemes	System Setup	Online User Key Generation	Online User Encryption	Online User Decryption
[16]	$1\mathrm{P}+(2U+14)\mathrm{E}+U\mathrm{M}$	$5l\mathrm{E}+2l\mathrm{M}$	$(5S+2)\mathrm{E}+S\mathrm{M}$	$4\mathrm{P}+3I\mathrm{E}+(2K+3I-2)\mathrm{M}$
[21]	5E	$7l\mathrm{E}+2l\mathrm{M}$	$1\mathrm{P}+(S+4)\mathrm{E}+2\mathrm{M}$	$1\mathrm{E}+1\mathrm{M}$
[26]	$1\mathrm{P}+(U+1)\mathrm{E}$	$(l+1)\mathrm{E}$	$1\mathrm{P}+(S+3)\mathrm{E}+S\mathrm{M}$	$3\mathrm{P}+I\mathrm{E}+2I\mathrm{M}$
Proposed	$K\mathrm{P}+(12K+2)\mathrm{E}$	$2l\mathrm{E}+2l\mathrm{M}$	$(KS+K+S+2)\mathrm{E}$	$1\mathrm{E}+1\mathrm{M}$

In real-world applications, the computational cost of the offline phase can be preworked when the user is idle. Therefore, during testing, we only focus on the computational cost incurred during the online phase. Due to the integration of online/offline technology, it can be seen from Table 2 that our proposed scheme has lower computational costs in key generation and encryption compared to [16,26]. In addition, due to the adoption of outsourced decryption, our proposed scheme and [21] shift a large number of decryption calculations to cloud servers, thus having greater advantages in decryption compared to the schemes in [16,26]. Therefore, the proposed scheme may be applicable to lightweight devices such as mobile phones with limited computing resources. Based on the analysis from Table 3, our scheme has successfully reduced the storage overhead to a certain extent compared to [16]. However, there is still a noticeable gap compared to [21,26] due to the multi-authority aspect.

Table 3. Comparison of storage costs.

Schemes	Public Parameters	Ciphertext	User Decryption Key
[16]	$(U+6)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$(4S+1)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$3l\lvert\mathbb{G}\rvert$
[21]	$7\lvert\mathbb{G}\rvert$	$(S+1)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$5l\lvert\mathbb{G}\rvert$
[26]	$(U+2)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$4\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$(2l+1)\lvert\mathbb{G}\rvert$
Proposed	$(5K+2)\lvert\mathbb{G}\rvert+K\lvert\mathbb{G}_T\rvert$	$(K+1)(S+1)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_T\rvert$	$3l\lvert\mathbb{G}\rvert$

We implemented the OO-MA-KP-ABE-CRF scheme using the Python programming language in the Charm-Crypto cryptographic library. The algorithm was thoroughly evaluated on a computer running the Linux Ubuntu 18.04.6 operating system, equipped with a 2.30 GHz 12th Gen Intel(R) Core(TM) i7-12700H CPU and 32 GB RAM. During the experimental phase, we deployed an Ubuntu virtual machine on the Windows 11 operating system and introduced the PYPBC module to provide the underlying mathematical foundation for the algorithm. Additionally, we initialized the parameter values "SS512" and "type A" curve to generate a prime-order bilinear group $\mathbb{G}$. It is worth noting that we categorized the computational operations involved in the algorithm's computational cost, including bilinear pairing operations, multiplication operations, and exponentiation operations performed on group elements. Furthermore, to ensure the feasibility and practicality of the algorithm, we repeated the experiments multiple times and recorded the time cost of bilinear pairing operations as 2.05 ms, the time cost of exponentiation operations on group $\mathbb{G}$ as 2.80 ms, and the time cost of multiplication operations on group $\mathbb{G}$ as 2.82 ms. We assume that the number of attribute universes U is 5 and the number of attribute institutions K is 1, because scheme [21,26] is a single-authority scheme, while [16] and our scheme are multi-authority.

We performed experimental simulations of the online user key generation, online user encryption and online user decryption of these schemes, as shown in Figure 2, to provide a comparison of computational costs. From Figure 2a,b, it can be seen that our OO-MA-KP-ABE-CRF scheme has certain advantages in user key generation and user encryption compared to [16,21], but it is higher than [26]. This is mainly because [26] is a single-authority KP-ABE scheme, and only one attribute organization is considered when generating keys and encrypting, while our scheme is multi-authority, so we need to consider the cost of key generation and encryption. Furthermore, compared to other schemes, Ref. [21] and our proposed scheme have been effectively optimized in decryption by employing outsourced decryption, as shown in Figure 2c.

We analyzed the storage costs of these schemes using ciphertexts and keys, as shown in Figure 3. Based on the analysis in Table 3, it can be seen that each scheme's ciphertext storage contains $|\mathbb{G}_T|$, so the impact of $|\mathbb{G}_T|$ can be ignored when comparing the cost of ciphertext storage. From Figure 3a, it can be seen that our scheme and [16] have a higher cost of ciphertext storage compared to [21,26]. This is because the schemes in [21,26] are both single-authority, and our scheme and [16] are both multi-authority. Therefore, in ciphertext construction, multiple authorities need to be considered, resulting in higher ciphertext storage costs. However, compared to the scheme [16] with multiple authorities, our scheme outperforms [16] in terms of ciphertext storage costs. As shown in Figure 3b, it can be seen that our scheme has the same storage cost in terms of keys as [16], lower than [21], but higher than [26]. This is mainly due to the access structures. The access structure in this scheme and [16] is non-monotonic and has more flexible expressions than the monotonic access structures in [21,26].

In order to provide a more detailed description of the differences between our scheme and other schemes, we conducted a detailed comparison and analysis from the perspectives of energy consumption and communication cost. Based on [31], and Tables 2 and 3, we can calculate the energy consumption and communication cost. From Figure 4a, it can be seen that in the encryption, our scheme has a higher energy consumption compared to [21], mainly due to the presence of multiple authorities, and there is no need for any central authority to coordinate key distribution between various attribute authorities. Therefore, compared to other schemes, it will generate a certain amount of energy consumption. From Figure 4b, it can be seen that our scheme has the same energy consumption as [21] during the decryption phase and is at a lower level, because both [21] and our scheme adopt outsourced decryption.

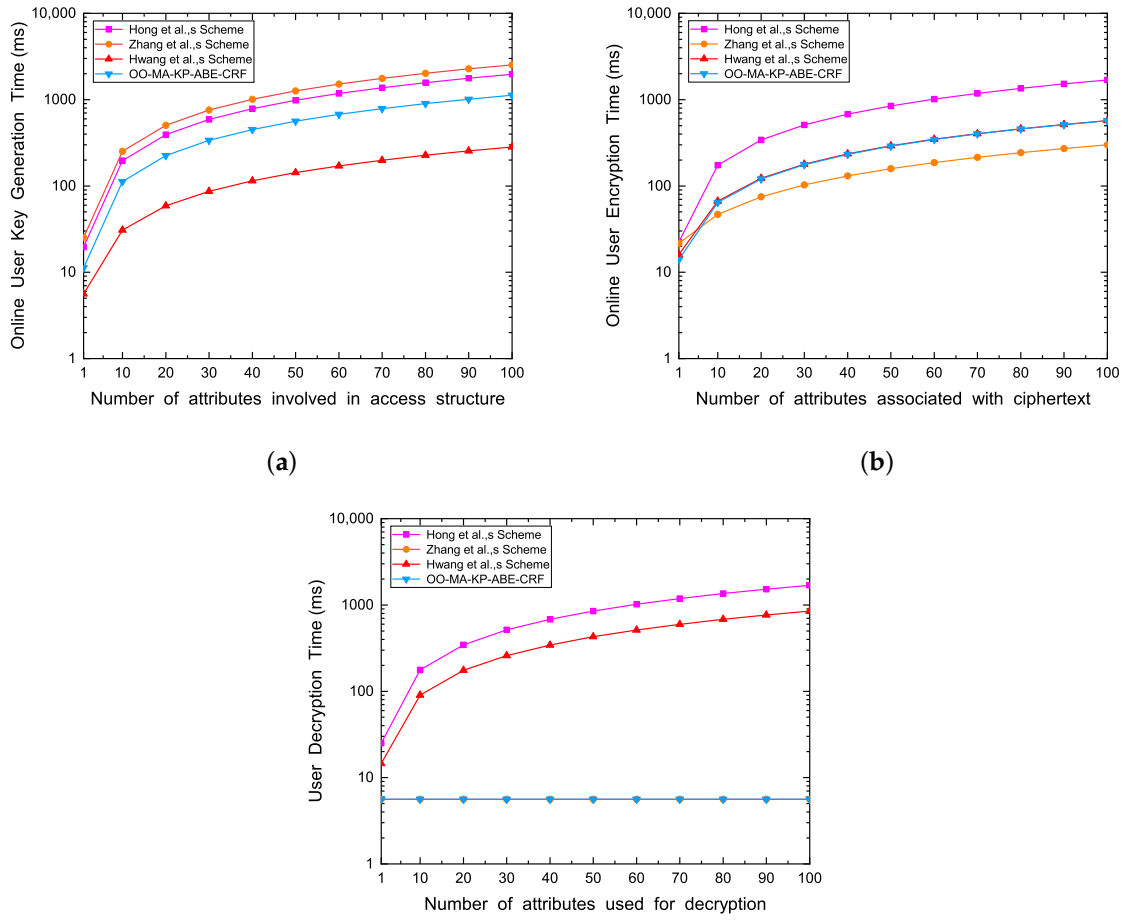


Figure 2. Computational cost comparison of online key generation,encryption and decryption [16,21,26]. (**a**) The online user key generation cost. (**b**) The user encryption cost; (**c**) The user decryption cost.

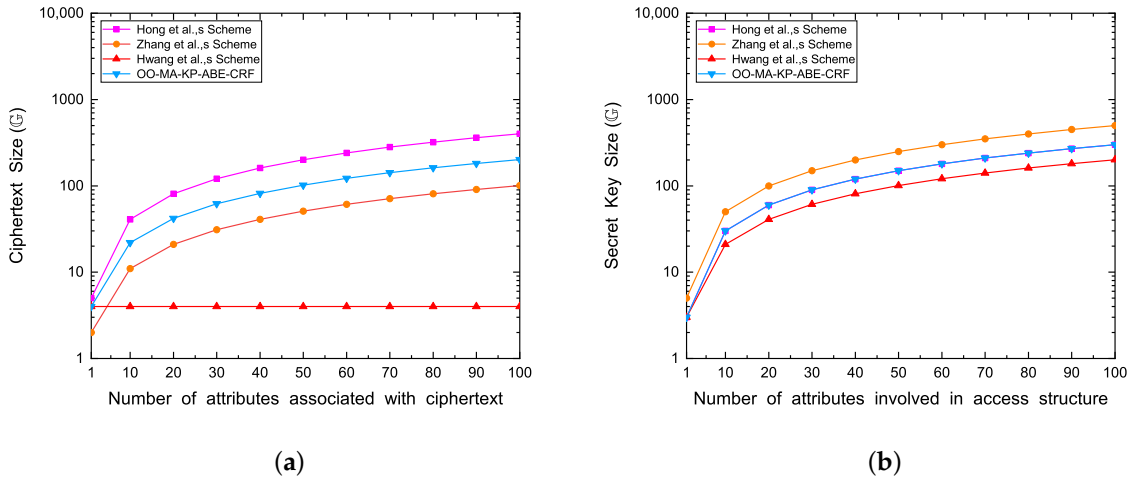
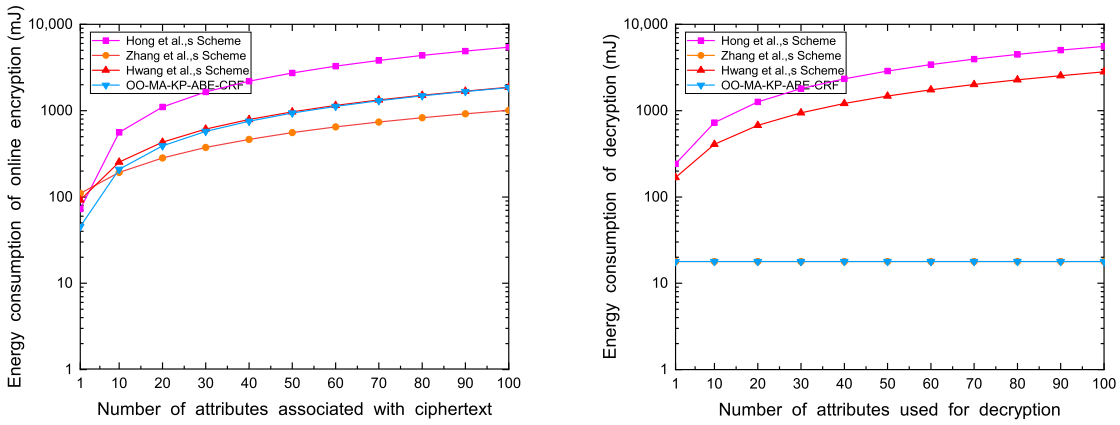


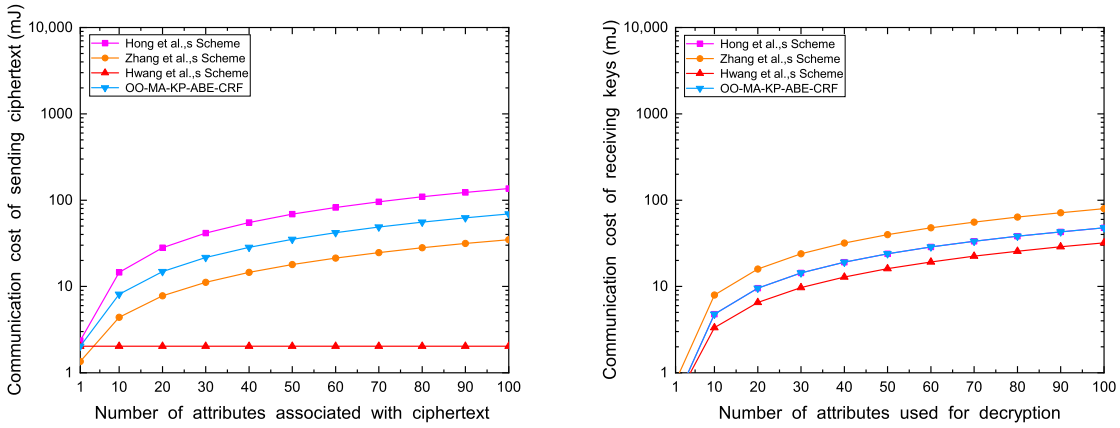
Figure 3. Storage cost comparison of ciphertext and secret key [16,21,26]. (**a**) The ciphertext storage cost. (**b**) The secret key storage cost.



(**a**) (**b**)

Figure 4. Energy consumption. (**a**) The energy consumption of online encryption [16,21,26]. (**b**) The energy consumption of decryption.

In terms of communication cost, according to Figure 5, our scheme has a higher communication cost when sending ciphertext than [21,26], but better than [16]. This is because both our scheme and [16] are multi-authority, but those in [21,26] are single-authority. Therefore, when sending ciphertext, our scheme consumes more than those in [21,26], but it consumes less compared to [16], both being multi-authority. In terms of receiving keys, our scheme is the same as [16], but it consumes more than [26]. This is because our scheme and [16] both support non-monotonic access structures, resulting in a larger scale of keys. Therefore, while achieving complex and diverse access structures, this also increases the cost of key communication.



(**a**) (**b**)

Figure 5. Communication cost. (**a**) The communication cost of sending ciphertext [16,21,26]. (**b**) The communication cost of receiving keys.

7. Conclusions

To effectively ensure the security of students' physical ability data in a cloud-sharing environment, this paper proposes an OO-MA-KP-ABE-CRF scheme. Compared with other schemes, the proposed scheme has a non-monotonic access structure, multiple authorities, CRF, and online/offline capabilities. This not only enables the scheme to support more flexible access structures, but also effectively reduces the risk of single-authority failure, which may be caused by a large number of attributes, and resists backdoor attacks. In addition, we have integrated online/offline encryption, online/offline key generation,

and outsourced decryption to reduce user storage and computing costs. Finally, we proved the security of the proposed scheme, and experimental analysis showed its effectiveness and feasibility.

In future work, we will further optimize the proposed scheme. In terms of security, we will consider the authentication requirement, as well as different attacks, such as MITM and replay attacks. In terms of efficiency, we will further optimize the efficiency of the scheme, through approaches such as optimizing the size of ciphertext, and consider the measurements for practical implementation.

Author Contributions: Conceptualization and validation, Y.F. and X.B.; writing—original draft, Y.Z. and Y.F.; writing—review and editing, Y.Z. and X.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Notations

P	a set of participants
x	positive attribute
x'	negative attribute
$\mathbb{A}$	monotonic access structure
$\tilde{\mathbb{A}}$	non-monotonic access structure
S	a set of attributes
$\tilde{S}$	a set of negative attributes in S
M	a linear secret-sharing matrix
M_i	the i-th row in M
$\rho(\cdot)$	mapping the i-th row to an attribute
s	shared secret
$\mathcal{A}_u$	a set of attributes
GID	the user's global identifier
$\mathcal{W}$	cryptographic reverse firewall
K	the number of AAs
$\mathcal{A}_C^k$	a set of attributes in k-th AA
(PK_k, SK_k)	the public/secret key pair for k-th AA
D_{GID}	the user's decryption key
m	plaintext
CT	ciphertext
TK	conversion key
RK	retrieval key

References

1. Li, J.; Peng, J.; Qiao, Z. A Ring Learning with Errors-Based Ciphertext-Policy Attribute-Based Proxy Re-Encryption Scheme for Secure Big Data Sharing in Cloud Environment. *Big Data* **2022**, *ahead of print*. [CrossRef] [PubMed]
2. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
3. Yamada, S.; Attrapadung, N.; Hanaoka, G.; Kunihiro, N. A framework and compact constructions for non-monotonic attribute-based encryption. In *Public-Key Cryptography—PKC 2014, Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, 26–28 March 2014*; Proceedings 17; Springer: Berlin/Heidelberg, Germany, 2014; pp. 275–292.
4. Attrapadung, N.; Hanaoka, G.; Yamada, S. Conversions among several classes of predicate encryption and applications to ABE with various compactness tradeoffs. In *Advances in Cryptology–ASIACRYPT 2015, Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015*; Proceedings, Part I 21; Springer: Berlin/Heidelberg, Germany, 2015; pp. 575–601.

5. Zhang, Y.; Deng, R.H.; Xu, S.; Sun, J.; Li, Q.; Zheng, D. Attribute-based encryption for cloud computing access control: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–41. [CrossRef]
6. Rasori, M.; Perazzo, P.; Dini, G.; Yu, S. Indirect revocable kp-abe with revocation undoing resistance. *IEEE Trans. Serv. Comput.* **2021**, *15*, 2854–2868. [CrossRef]
7. Kumar, N.; Samriya, J.K. Secure Data Validation and Transmission in Cloud and IoT Through Ban Logic and KP-ABE. *Int. J. Sensors Wirel. Commun. Control* **2022**, *12*, 79–87. [CrossRef]
8. Jaiswal, R.; Iyer, S.S. Cloud Deployed PHR Using ABE Scheme. *ECS Trans.* **2022**, *107*, 4905. [CrossRef]
9. Nagaraj, S.; Kathole, A.B.; Arya, L.; Tyagi, N.; Goyal, S.; Rajawat, A.S.; Raboaca, M.S.; Mihaltan, T.C.; Verma, C.; Suciu, G. Improved Secure Encryption with Energy Optimization Using Random Permutation Pseudo Algorithm Based on Internet of Thing in Wireless Sensor Networks. *Energies* **2022**, *16*, 8. [CrossRef]
10. Jemihin, Z.B.; Tan, S.F.; Chung, G.C. Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey. *Cryptography* **2022**, *6*, 40. [CrossRef]
11. Parekh, R.; Patel, N.; Gupta, R.; Jadav, N.K.; Tanwar, S.; Alharbi, A.; Tolba, A.; Neagu, B.C.; Raboaca, M.S. Gefl: Gradient encryption-aided privacy preserved federated learning for autonomous vehicles. *IEEE Access* **2023**, *11*, 1825–1839. [CrossRef]
12. Li, C.; Shen, Q.; Xie, Z.; Dong, J.; Feng, X.; Fang, Y.; Wu, Z. Hierarchical and non-monotonic key-policy attribute-based encryption and its application. *Inf. Sci.* **2022**, *611*, 591–627. [CrossRef]
13. Mironov, I.; Stephens-Davidowitz, N. Cryptographic reverse firewalls. In *Advances in Cryptology—EUROCRYPT 2015, Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015*; Proceedings, Part II 34; Springer: Berlin/Heidelberg, Germany, 2015; pp. 657–686.
14. Dodis, Y.; Mironov, I.; Stephens-Davidowitz, N. Message transmission with reverse firewalls—Secure communication on corrupted machines. In *Advances in Cryptology—CRYPTO 2016, Proceedings of the 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016*; Proceedings, Part I; Springer: Berlin/Heidelberg, Germany, 2016; pp. 341–372.
15. Ma, H.; Zhang, R.; Yang, G.; Song, Z.; Sun, S.; Xiao, Y. Concessive online/offline attribute based encryption with cryptographic reverse firewalls—Secure and efficient fine-grained access control on corrupted machines. In *Computer Security, Proceedings of the 23rd European Symposium on Research in Computer Security, ESORICS 2018, Barcelona, Spain, 3–7 September 2018*; Proceedings, Part II 23; Springer: Berlin/Heidelberg, Germany, 2018; pp. 507–526.
16. Hong, B.; Chen, J.; Zhang, K.; Qian, H. Multi-authority non-monotonic KP-ABE with cryptographic reverse firewall. *IEEE Access* **2019**, *7*, 159002–159012. [CrossRef]
17. Zhou, Y.; Hu, Z.; Li, F. Searchable public-key encryption with cryptographic reverse firewalls for cloud storage. *IEEE Trans. Cloud Comput.* **2021**, *11*, 383–396. [CrossRef]
18. Zhao, Y.; Pang, Y.; Ke, X.; Wang, B.; Zhu, G.; Cao, M. A metaverse-oriented CP-ABE scheme with cryptographic reverse firewall. *Future Gener. Comput. Syst.* **2023**, *147*, 195–206. [CrossRef]
19. Hohenberger, S.; Waters, B. Online/offline attribute-based encryption. In *Public-Key Cryptography—PKC 2014, Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, 26–28 March 2014*; Proceedings 17; Springer: Berlin/Heidelberg, Germany, 2014; pp. 293–310.
20. Cui, J.; Zhou, H.; Xu, Y.; Zhong, H. OOABKS: Online/offline attribute-based encryption for keyword search in mobile cloud. *Inf. Sci.* **2019**, *489*, 63–77. [CrossRef]
21. Zhang, S.; Li, W.; Wen, Q.; Zhang, H.; Jin, Z. A flexible KP-ABE suit for mobile user realizing decryption outsourcing and attribute revocation. *Wirel. Pers. Commun.* **2020**, *114*, 2783–2800. [CrossRef]
22. Guo, R.; Yang, G.; Shi, H.; Zhang, Y.; Zheng, D. O 3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system. *IEEE Internet Things J.* **2021**, *8*, 8949–8963. [CrossRef]
23. Lai, J. Attribute-Based Encryption with Offline Computation and Outsourced Decryption. In *Encyclopedia of Cryptography, Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–5.
24. Zhang, Z.; Cao, S.; Yang, X.; Liu, X.; Han, L. An efficient outsourcing attribute-based encryption scheme in 5G mobile network environments. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3488–3501. [CrossRef]
25. Ali, M.; Sadeghi, M.R.; Liu, X.; Miao, Y.; Vasilakos, A.V. Verifiable online/offline multi-keyword search for cloud-assisted industrial internet of things. *J. Inf. Secur. Appl.* **2022**, *65*, 103101. [CrossRef]
26. Hwang, Y.W.; Kim, S.H.; Seo, D.; Lee, I.Y. An SKP-ABE Scheme for Secure and Efficient Data Sharing in Cloud Environments. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1384405. [CrossRef]
27. Li, J.; Fan, Y.; Bian, X.; Yuan, Q. Online/Offline MA-CP-ABE with Cryptographic Reverse Firewalls for IoT. *Entropy* **2023**, *25*, 616. [CrossRef] [PubMed]
28. Lewko, A.; Sahai, A.; Waters, B. Revocation systems with very small private keys. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 273–285.
29. Lewko, A.; Waters, B. Decentralizing attribute-based encryption. In *Advances in Cryptology—EUROCRYPT 2011, Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 15–19 May 2011*; Proceedings 30; Springer: Berlin/Heidelberg, Germany, 2011; pp. 568–588.

30. Green, M.; Hohenberger, S.; Waters, B. Outsourcing the decryption of abe ciphertexts. In Proceedings of the USENIX Security Symposium, San Francisco, CA, USA, 10–12 August 2011; Volume 2011.
31. Li, J.; Qiao, Z.; Peng, J. Asymmetric group key agreement protocol based on blockchain and attribute for industrial internet of things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8326–8335. [CrossRef]