processes

MDPI

Article

An Efficient ECC-Based CP-ABE Scheme for Power IoT

Rui Cheng [1,*], Kehe Wu [1], Yuling Su [1], Wei Li [1], Wenchao Cui [1] and Jie Tong [2]

[1] School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China; wkh@ncepu.edu.cn (K.W.); suyuling@ncepu.edu.cn (Y.S.); liwei@ncepu.edu.cn (W.L.); cuzz@ncepu.edu.cn (W.C.)
[2] China Electric Power Research Institute, No. 15, Qinghe Xiaoying Road, Beijing 100192, China; tongjie1@epri.sgcc.com.cn
* Correspondence: chengrui@ncepu.edu.cn

Abstract: The rapid development of the power Internet of Things (IoT) has greatly enhanced the level of security, quality and efficiency in energy production, energy consumption, and related fields. However, it also puts forward higher requirements for the security and privacy of data. Ciphertext-policy attribute-based encryption (CP-ABE) is considered a suitable method to solve this issue and can implement fine-grained access control. However, its internal bilinear pairing operation is too expensive, which is not suitable for power IoT with limited computing resources. Hence, in this paper, a novel CP-ABE scheme based on elliptic curve cryptography (ECC) is proposed, which replaces the bilinear pairing operation with simple scalar multiplication and outsources most of the decryption work to edge devices. In addition, time and location attributes are combined in the proposed scheme, allowing the data users to access only within the range of time and locations set by the data owners to achieve a more fine-grained access control function. Simultaneously, the scheme uses multiple authorities to manage attributes, thereby solving the performance bottleneck of having a single authority. A performance analysis demonstrates that the proposed scheme is effective and suitable for power IoT.

Keywords: power IoT; CP-ABE; elliptic curve; pairing free; edge computing; outsourcing; multiple authorities; time and location

Citation: Cheng, R.; Wu, K.; Su, Y.; Li, W.; Cui, W.; Tong, J. An Efficient ECC-Based CP-ABE Scheme for Power IoT. *Processes* **2021**, *9*, 1176. https://doi.org/10.3390/pr9071176

Academic Editor: Giampaolo Manzolini

Received: 12 June 2021
Accepted: 5 July 2021
Published: 6 July 2021

1. Introduction

Power Internet of Things (IoT) connects power users, grid enterprises, generation enterprises, suppliers, and their equipment to generate shared data and serve users, power grids, power suppliers, and the government and society in return [1].

With the construction and promotion of the power IoT, hundreds of millions of IoT terminals are deployed in the areas of power generation-transmission-substation-distribution-consumption. These power IoT terminals can collect multidimensional data from the electricity infrastructure and equipment effectively, and then, the data are uploaded to a cloud platform of the state grid for use in other business systems, such as smart energy service platforms, asset management systems, and power markets. Meanwhile, kinds of electric smart devices generate massive data, thus bringing new challenges to the data storage and management for smart grid and promoting the integration of power IoT and smart grid. Hence the privacy security of data storage is becoming an attractive research area in power IoT. The effective access control is the key method to achieve the privacy security of the cloud storage. In addition, the traditional power grid access control technology has been unable to meet the practical needs due to the large number of users and devices, small grain size and large scale of data and distributed characteristics of access control in power IoT.

What is more, the data of power IoT may contain some sensitive information (such as customer electricity usage and voltage data for a certain place) and private information (such as user identity and location information). Therefore, it is necessary to protect the

security of data generating in power generation–transmission–substation–distribution–consumption. Due to the opening of power IoT, the network of power IoT has lots of potential attack points, and a breach of one device could leave the entire grid vulnerable to cyber-attack. Therefore, the power IoT is vulnerable to malicious damage and illegal access. It is also necessary to limit the access of authorized users by time and location. For example, a legitimate employee of an electric power company can only access certain user data in the office during working hours. Therefore, the fine-grained access control for power IoT needs to meet stricter requirements. The traditional one-to-one access mode between data and users by public key encryption schemes cannot satisfy the requirements of complex power IoT systems. However, ciphertext-policy attribute-based encryption (CP-ABE) with fine-grained access control can support a one-to-many access mode between data and multiple users, which can solve the problems mentioned above.

However, the implementation of CP-ABE relies on the bilinear pairing operation, which has high computational cost and requires too many computing resources. In contrast, scalar multiplication based on elliptic curve cryptography (ECC) consumes much fewer resources, and the computational overhead of bilinear pairing is two or three times higher than that of scalar multiplication with the same elliptic curve. In addition, because the computing resources of the power IoT terminals are limited, they are not suitable for large data encryption and decryption operations. To reduce the computational overhead of power terminals, the calculation can be outsourced to the edge IoT agent based on edge computing and the framework of power IoT [2]. Therefore, the scheme proposed here, which combines the CP-ABE based on ECC and edge computing, can effectively provide information security protection for power IoT.

The major contributions of this paper include the following:

(1) We propose an efficient CP-ABE scheme, which uses simple scalar multiplication based on ECC instead of complex bilinear pairing to reduce the computational overhead and make it more suitable for power IoT terminals with resource constraints.
(2) The proposed scheme uses multiple authorities to manage the attributes, which avoids the problems of the single point and key escrow of the single authority scheme and improves the security of the system.
(3) The access control of the proposed scheme is more fine-grained by combining the time and location domain information as dynamic attributes into the proposed CP-ABE scheme. The data users can only access the relevant cipher text within the valid range of time and location, thus improving the security of the power data.
(4) We adopt the linear secret sharing scheme (LSSS) access structure to enhance the expressiveness of the access policy and provide an elaborate security and performance analysis between the proposed scheme and existing schemes. The experimental results demonstrate that the proposed scheme is effective.

In this paper, Sections 1 and 2 present the introduction and related work on power IoT and CP-ABE. The preliminaries of the scheme are presented in Section 3. Section 4 introduces the details of design of the proposed scheme based on ECC. The security and performance analysis are given in Sections 5 and 6. Section 7 presents the conclusions of this paper.

2. Related Work

After Bethencourt et al. gave the first concrete construction of CP-ABE [3], there have been many works enhancing the CP-ABE scheme; for example, Lewko et al. presented an ABE scheme in composite order bilinear groups with low practical efficiency [4]. Although these IPE constructions achieve attribute hiding properties, the security of their scheme is not high under well-known standard assumptions. Li et al. presented a new CP-ABE system based on the ordered binary decision diagram (OBDD) [5]. Deng et al. extended ABE to CP-HABE to support hierarchical attributes and focused on the problem of key management [6]. Goyal et al. adopted a bounded access tree structure and proposed a CP-ABE scheme with a more flexible access policy under the DBDH assumption [7]. In

addition, Yan et al. proposed a multi-authority attribute encryption scheme with dynamic policy updates in personal health record systems [8]. These schemes enhance the CP-ABE scheme, but the performance of CP-ABE is not improved or mentioned.

The CP-ABE scheme usually requires the calculation of bilinear pairing, which demands a very large amount of computation resources. In the IoT system, edge computing technology can reduce the resources consumption of terminals by outsourcing encryption and decryption to edge devices. Belguith et al. proposed a multi-authority access control scheme with hidden access policies and outsourced decryption computing to the cloud [9]. The concept of user groups was adopted by Li et al. to solve the permission revocation problem and outsource the computation to improve the efficiency and performance of the scheme [10]. Yu et al. proposed a scheme that allows the data owner to delegate most of the computation to untrusted cloud servers without any information disclosing by combining techniques of ABE with proxy re-encryption and lazy re-encryption [11]. However, these schemes increase the overhead of the communication and encryption/decryption of the cloud service provider.

Green et al. proposed a CP-ABE scheme with outsourcing decryption computing [12]. In this scheme, the cipher text is sent to the decryption outsourcing server. Then, the decryption outsourcing server pre-decrypts the cipher text to obtain the intermediate cipher text, which is sent to the data user, thus reducing the user's computation. However, the revoked user is still able to decrypt the new cipher text. Furthermore, this scheme cannot defend against the attack of forward security. Li et al. proposed an improved CP-ABE scheme for hybrid cloud computing, which supports outsourcing encryption and decryption and provides a data validation mechanism to ensure the correctness of outsourced data [13]. However, the performance of encryption and decryption is still limited by the number of attributes. Zhang et al. proposed an access control scheme that outsourced the encryption and decryption to fog nodes, which reduced the encryption and decryption operations of terminals [14]. The scheme can update system attributes effectively. However, the fog nodes are close to the terminal side, so they are easily attacked. Zuo et al. proposed a more secure outsourcing decryption scheme, which can resist the attack of selective cipher text [15]. Fan et al. proposed an efficient and privacy-preserving outsourced access control scheme with multiple authorities, named PPO-MACS [16]. All attributes of users are transformed to be anonymous and authenticable to realize privacy preservation. Zhong et al. also proposed an efficient ABE scheme that can outsource part of the encryption and decryption to the edge nodes and support the update of attributes, making access control flexible [17]. Although these schemes achieve computing outsourcing, terminals still need to compute bilinear pairing, and the performance bottleneck of CP-ABE remains.

With the research of elliptic curves, many researchers have combined elliptic curves with ABE and adopted elliptic curve algorithms to replace complex bilinear pair operations so that they can be applied in resource-constrained IoT systems. Table 1 illustrates the feature-based comparison of some pairing free ABE schemes, highlighting the advantages and disadvantages of the respective works. Odelu et al. proposed a CP-ABE scheme based on ECC with constant key size and applied it to the designed lightweight CP-ABE scheme for battery-limited mobile devices in the IoT based on cloud computing [18]. However, the AND GATE access structure adopted by Odelu et al. is not well expressed and is not suitable for complex access structures [19]. Yao et al. proposed an ECC-based lightweight KPABE technique for IoT without bilinear pairing, but there are some limitations in their scheme; it is unable to support outsourcing decryption and has poor scalability [20]. Sowjanya et al. proposed a lightweight ECC-based key-policy ABE without bilinear pairing and with a key refresh/update mechanism. However, KP-ABE is not suitable for IoT systems with many terminals [21]. Qin et al. proposed a scheme that integrates an elliptic curve Qu-Vanstone implicit certificate with the ELGamal encryption algorithm to achieve both mutual authentication and conditional privacy protection [22]. Ding et al. proposed a scheme that replaces complicated bilinear pairing with simple scalar multiplication on elliptic

curves, thereby reducing the overall computational overhead [23]. Samarati et al. [24] proposed a CP-ABE scheme based on the ECC with a constant-size secret key, which is capable of addressing the collusion attack security issue. A lightweight attribute-based security scheme based on ECC was proposed by Junejo et al. for fog-enabled cyber physical systems (Fog-CPS) [25]. Tian et al. proposed a scheme that replaces complicated bilinear pairing with simple scalar multiplication on elliptic curves to realize cipher text policy attribute-based encryption of cloud data while solving the security problem of shared data [26].

Table 1. Feature-based comparison.

Pairing Free ABE Schemes	Advantages	Disadvantages
Odelu et al. [18]	Bilinear pairing free and ECC based CP-ABE scheme with constant size ciphertext and keys. The time complexity for encryption and decryption is O(1).	The AND GATE access structure is not well expressed. Since the fully-trusted Attribute Authority generates the secret master keys, this scheme suffers from the key-escrow problem.
Yao et al. [20]	An ECC based lightweight ABE scheme without bilinear pairing operations. Selectively secured against CPA under Elliptic Curve Decisional Diffie—Hellman assumption.	Access tree access structure is less insufficient. Poor flexibility in revoking attribute.Poor scalability and generality.
Sowjanya et al. [21]	A lightweight ECC-based key-policy ABE without bilinear pairing and with a key refresh/update mechanism.	KP-ABE is not suitable for IoT systems with many terminals. The AND GATE access structure is not well expressed.
Qin et al. [22]	Lightweight KP-ABE based on ECC and ELGamal. Can provide mutual authentication and conditional anonymity.	The performance is worse than traditional ECQV certificate scheme.
Ding et al. [23]	Lightweight without pairing ECC based CP-ABE scheme with LSSS access matrix. Resistant to collusion attack.	Suffers from the key-escrow problem.
Samarati et al. [24]	A CP-ABE scheme based on ECCwith a constant-size secret key. Can be capable of addressing the collusion attack.	The extra validate phase may be the bottleneck while the device's amount increase.
Junejo et al. [25]	A leightweight ABE scheme Based on ECC and fog computing. Provide secure key pair update approach.	The constraints of access time and location are not being taken into consideration. AND GATE access control structure is not well expressed.

However, the access policies of these schemes are only based on regular attributes (such as the department and occupation, etc.) of users to generate access policies while ignoring the access constraints of time and location, so they are not applicable to meet the real-time and mobility requirements of edge computing. To share time-sensitive data, Hong et al. proposed an access control scheme combining time and attributes [27]. If an attribute has a time limit, the CA generates a time token that is used to transform the state of the time trap gate generated by the data owner at the cloud server. However, if the CA is maliciously corrupted, the time token and the private key of the property is leaked, causing the whole system to crash.

3. Preliminaries

3.1. Elliptic Curve Cryptography

ECC was first proposed by Neal Koblitz and Victor Miller in 1985. ECC is an important branch of public key cryptography, and its security is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). An elliptic curve E defined on the finite field $FG(p)$ can be expressed as $y^2 = x^3 + ax + b(mod\ p)$ and $4a^3 + 27b^2 \neq 0$. If G is a generator of the group with prime order r, it is extremely difficult to compute k in polynomial time for the given point $Q = kG$. Compared with RSA, ECC is able to ensure the same security with smaller key sizes because it is more difficult to solve ECDLP than to decompose integers in RSA. ECC encryption protocols are generally divided into three steps. First, the plain text data are mapped to the point Q on the elliptic curve. Then, the encryption protocol between the two entities, such as Alice and Bob, performs as follows:

(1) Key Generation
   (a) Alice and Bob agree to use the same elliptic curve $y^2 = x^3 + ax + b(mod\ p)$ and a generator G.
   (b) Alice selects an integer $S_a \in Z_p$ randomly as the private key, calculates $P_a = S_aG$ as the corresponding public key and makes it public.
   (c) Bob also selects an integer $S_b \in Z_p$ randomly as the private key, calculates $P_b = S_bG$ as the corresponding public key and exposes it.

(2) Encryption

To encrypt Q, Alice first selects an integer $k \in Z_p$ at random, then calculates the cipher text with two parts: $C_1 = kG$, $C_2 = Q + kP_b$ and sends C_1 and C_2 to Bob.

(3) Decryption

After receiving the cipher text, Bob obtains Q by calculating $C_2 - S_bC_1 = Q + kP_b - S_bkG = Q$. Finally, Bob can obtain the plain text data by mapping the point Q on the elliptic curve.

3.2. Decisional Diffie–Hellman Assumption

The definition of the decisional Diffie–Hellman (DDH) problem is described below: The challenger chooses a cyclic group P with prime order r. G is one generator of cyclic group P, and a and b are randomly selected from Z_r. If the challenger gives the adversary a tuple (G, aG, bG), it is difficult for the adversary to distinguish the valid element $abG \in P$ from a random element $R \in P$ in polynomial time. The advantage of algorithm $\mathcal{B}$ to solve the DDH problem under P is ε if $|Pr[\mathcal{B}(G, aG, bG, Z = abG) = 0] - Pr[\mathcal{B}(G, aG, bG, Z = R) = 0]| \geq \varepsilon$, which indicates that algorithm $\mathcal{B}$ can overcome the DDH problem with the advantage of ε.

Definition 1. *The DDH assumption holds if the advantage of the algorithms in solving the DDH problem in polynomial time is negligible.*

3.3. Linear Secret Sharing Scheme

If a secret sharing scheme Π based on a member set P satisfies the following conditions, then scheme Π is called a LSSS on Z_p.

(1) The secret shares of all participating members constitute a vector on ${Z_p}^*$
(2) In the secret sharing scheme Π, there is a sharing $l \times n$ matrix M. The row i in M represents the member i of the set P where $i = 1, 2, \ldots l$, and this member can be found through the $\rho(i)$, $\rho(i)$ is a function that maps from $\{1, 2, \ldots l\}$ to P. Let $\vec{v} = (s, y_2, y_3, \ldots, y_n)$ be a random vector, where $s \in {Z_p}^*$ is the shared secret message and $y_2, y_3, \ldots, y_n \in {Z_p}^*$ is an arbitrary random number. Then, $(M \cdot \vec{v})_i$ divides the secret s into l parts according to the sharing scheme Π, where $(M \cdot \vec{v})_i$ belongs to i.
(3) The linear secret sharing scheme defined above should also satisfy the linear reconstruction property. For any authorized set $S \in \Lambda$, $I \subset \{1, 2, \ldots l\}$ and $I = \{i : \rho(i) \in S\}$

where Λ is the access structure, a constant set $\{w_i \in Z_p{}^*\}_{i\in I}$ can be found in polynomial time, and the secret s can be recovered by computing $\sum_{i\in I} w_i\left(M\cdot\vec{v}\right) = \varepsilon\cdot\vec{v} = s$ and $\varepsilon = (1,0,\ldots,0)$. For the unauthorized set, there exists vector $\{\omega_i \in Z_p{}^*\}_{i\in I}$ leading to $\omega_i \cdot M^T = 0$.

3.4. System Model

The architecture of the proposed scheme in this paper includes power terminals/users, edge IoT agents, and clouds of state grids. There are six roles in the scheme, including cloud server provider (CSP), central authority (CA), attribute authority (AA), edge node (EN), data owner (DO), and data user (DU). The framework of the scheme is shown in Figure 1. The functions of each role are as follows:

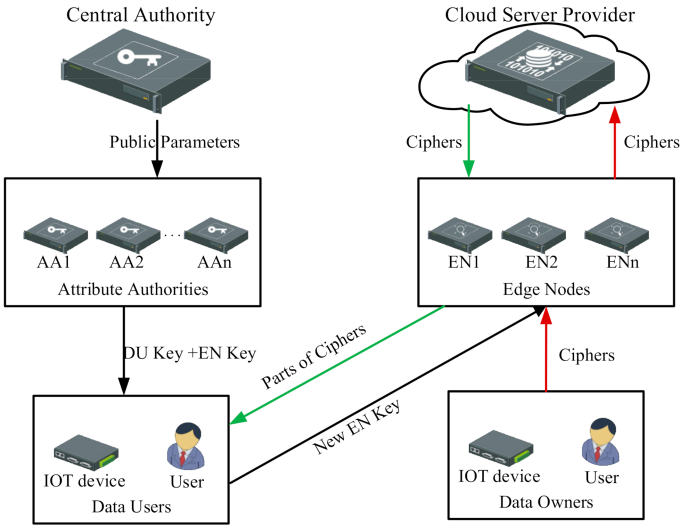


Figure 1. Framework of the proposed scheme.

(1) CSP: The CSP is an "honest but curious" data storage organization that honestly performs the tasks assigned by the system and provides services reliably. However, it may be interested in the information stored by users and may try to steal some privacy data.
(2) CA: The CA is fully trusted and generates public parameters for the entire system.
(3) AA: The AAs are fully reliable as well. Each AA is responsible for managing attributes that belong to its own domain. The AA generates a pair of public and private key pairs for its attributes in the domain. The public key is sent to the DO for encryption, while the private key generates the attribute private key for the DU. The AA decides to generate and distribute the private key of the relevant attributes to the DU depending on the validity of the request time and location of the DU.
(4) EN: The ENs are capable of storage and computation, filling the gap between users and cloud servers. They can process the requests of a DU in real time and retrieve cipher text from adjacent nodes or cloud servers when necessary. In addition, they are also responsible for pre-decrypting the cipher text and then returning the results to DU.
(5) DO: The DO is in charge of formulating the access structure, calculating the cipher text and uploading the cipher text to the CSP.
(6) DU: The DU can obtain the pre-decrypted results from the EN and then decrypt the data to obtain the plain text data.

The algorithms of the scheme are defined below:

(1) Global Initialization $(k) \rightarrow PP$: The CA chooses a security parameter k and executes the global initialization algorithm and then outputs the system public parameter PP for the system.
(2) Authority Initialization $(PP) \rightarrow (PK, MSK)$: The Attribute Authority inputs the public parameter PP and outputs the public key (PK) and master secret key (MSK) for the authority and its attributes.
(3) Data Encrypt $(PP, PK, M, (\Lambda, \rho)) \rightarrow CT$: The data owner inputs the public parameter PP, the corresponding PK, the given plain message M and the access policy (Λ, ρ), and then the cipher text CT is output.
(4) General Key Generation $(PP, S_{i,GID}, GID, MSK) \rightarrow USK_{i,GID}$: The algorithm is executed by AA_i. Then, AA_i can obtain the general attribute key $USK_{i,GID}$ by inputting PP, general attribute set $S_{i,GID}$ of AA_i, and GID of the data user and master key MSK.
(5) Time Key Generation $(PP, ST_{i,GID}, GID, MSK) \rightarrow TSK_{i,GID}$: AA_i is able to obtain the time attribute key $TSK_{i,GID}$ by the PP, time attribute set of $ST_{i,GID}$, GID of data user and master secret key MSK.
(6) Location key generation $(PP, SL_{i,GID}, GID, MSK) \rightarrow LSK_{i,GID}$: AA_i takes the public parameter PP, location attribute set $SL_{i,GID}$, and GID of the data user and master key MSK as input and then outputs the attribute key $LSK_{i,GID}$ of the location.
(7) Edge IoT agent pre-decryption $(PP, PK, SK, CT) \rightarrow CT'$: The edge IoT agent terminals perform the pre-decryption operation and input the pre-decryption key and cipher text to obtain the cipher text CT'.
(8) Local Decryption $(DSK, CT') \rightarrow M$: The data user performs the decryption operation, inputs DSK and CT', and calculates the final plain text M.

3.5. Security Model

To prove the security under a chosen-cipher text attack, we now give the security model of our CP-ABE scheme. The model between adversary ϑ and challenger $\mathcal{B}$ is described as follows:

Initialization. The adversary ϑ outputs the challenge as an access structure (Λ^*, ρ) and sends it to the challenger $\mathcal{B}$.

Setup. Challenger $\mathcal{B}$ runs the initialization algorithm to generate the necessary public parameter for the system as well as the public and secret key pair for each attribute. The challenger gives the public keys to the adversary ϑ.

Phase 1. The adversary ϑ can adaptively make queries for the secret keys of the attributes with the restriction that no set of the keys can decrypt the challenge's cipher text. The challenger records the attributes in the attribute list corresponding to the adversary's GID.

Challenge Phase. In this phase, adversary ϑ outputs (M_0, M_1) for challenge, and $M_0, M_1 \in Z_p$ are two equal-length messages. Then, the challenger picks a coin $\beta \in \{0, 1\}$ and sends the encryption of M_β under access matrix (Λ^*, ρ) to adversary ϑ.

Phase 2. The adversary ϑ can continue with the secret key queries and decryption queries with the same restriction in Phase 1.

Guess. The adversary may output a guess β_0 of β.

The advantage of the adversary in this game is defined as $\left| Pr[\beta_0 = \beta] - \frac{1}{2} \right|$.

Our CP-ABE would be selective CPA secure if the adversary can win this security game with a negligible advantage in polynomial time.

4. Proposed Scheme

In this paper, we propose a novel outsourced CP-ABE scheme that supports multi-authority and dynamic time and location attributes. The scheme not only considers the general attributes of data users but also incorporates time and location domain information into the attributes of access time and location so that the data users can only access legitimate data according to their own existing attributes, making access control more

flexible and fine-grained. We simplify the calculation process by using simple scalar multiplication based on ECC instead of complex bilinear pairings. Our scheme is composed of the following five parts: global initialization, authority initialization, data encryption, key generation, and data decryption. Data decryption consists of two processes: pre-decryption on the edge IoT agent and user decryption. The algorithms can be reformulated in more detail as follows.

1. Global Initialization

The algorithm is executed by CA, CA inputs the security parameter k and selects a finite field $GF(q)$ of order r, E is an elliptic curve defined over the finite field $GF(q)$, and G is a generator of cyclic subgroups with prime order r on the elliptic curve E, where the ECDLP is difficult to solve.

In addition, the hash function $H : \{0,1\}^* \rightarrow Z_r^*$ is chosen to map the GID of the user to the elements in Z_r. Define the set of global attributes $\Lambda = \{a_1, \cdots, a_n\}$, and these attributes are managed by multiple authorities and generate keys for users associated with their attributes.

The public parameter is $PP = \{GF(q), G, E, \Lambda, H\}$, and the CA sends PP to AA_i in the system.

2. Authority Initialization

The algorithm is run by each authority in the system, and the input is the public parameter PP that is initialized by CA. The system has multiple authorities, and each authority takes attributes that do not overlap with others and needs to maintain a list of attributes corresponding to the GID of the user. The authority selects two random values $y_i, k_i \in Z_r$ to generate the master secret key $MSK = \{y_i, k_i, \forall i\}$ and public key $PK = \{y_i G, k_i G, \forall i\}$ for attribute i.

3. Data Encryption

(1) The DO uses a symmetric encryption algorithm E (such as SM1/SM4) and randomly symmetric key ck to encrypt the message M, calculating $CT_{DATA} = E_{ck}(M)$ to obtain the cipher text CT_{DATA} and calculating $H_{CT} = H(CT_{DATA})G$ to ensure the integrity of the data.

(2) The DO selects a unique number $DATA_{ID}$ for the cipher text CT_{DATA}; if the data cipher text $DATA_{ID}$ has limited the access time, then the DO should add the valid time range $\left[T_{begin},\ T_{end}\right]$ to the time attributes $ST_{i,DATA_{ID}}$ belonging to cipher text $DATA_{ID}$. The DO selects a random value $t_i \in Z_p$ to encrypt the symmetric key and calculates $t_i G$ to generate the private key for the time attributes. Similarly, if $DATA_{ID}$ has a limited access location, then the DO should add the valid time range $\left[L_{begin},\ L_{end}\right]$ to the location attributes $SL_{i,DATA_{ID}}$ belonging to $DATA_{ID}$. The DO selects $l_i \in Z_p$ to encrypt the symmetric key and calculates $l_i G$ to generate the private key for the location attributes.

(3) The DO defines an LSSS access structure (Λ, ρ) to restrict the user who can decrypt data with corresponding attributes. Λ is the $l * m$ access matrix, and $\rho(x)$ represents the attribute corresponding to row x of access matrix Λ. Then, the data owner sends the access structure (Λ, ρ) to the edge IoT agent.

The encryption algorithm consists of the following stages:

a. Calculate $C_0 = ck + sG$ where $s \in Z_p$ is a random number.

b. Select two random vectors $\vec{v} = (s, v_2, \ldots, v_m) \in Z_p$ and $\vec{u} = (0, u_2, \ldots, u_m) \in Z_p$, then calculate $\lambda_x = \Lambda_x \cdot \vec{v}$, $\omega_x = \Lambda_x \cdot \vec{u}$ and $\Big(C_{1,x} = \lambda_x G + \gamma_x y_{\rho(x)} G, C_{2,x} = \gamma_x G, C_{3,x}$

$= \left\{ \begin{array}{l} \omega_x G + \gamma_x k_{\rho(x)} G, \ if \rho(x) \in normal\ attrs \\ \omega_x G + \gamma_x (k_{\rho(x)} + t_{\rho(x)}) G, \ if \rho(x) \in time\ attrs \\ \omega_x G + \gamma_x (k_{\rho(x)} + l_{\rho(x)}) G, \ if \rho(x) \in location\ attrs \end{array} \right)$, $\gamma_x \in Z_p$ is a random number, where $x \in [1, l]$ and Λ_x is the row x of Λ.

Finally, the cipher text is $CT = \{(\Lambda, \rho), C_0, \{C_{1,x}, C_{2,x}, C_{3,x}\}, CT_{DATA}, H_{CT}\}$. DO uploads the cipher text CT to the cloud server.

4. Key Generation

The key generation algorithm is executed by AA_i and DU. The key includes the general key, time key and location key.

(1) Key Generation for General Attributes

AA_i generates the general key $USK_{i,GID}{}' = y_i + H(GID)k_i$ of attribute i for the DU with GID and records it in the list of GID. Then, the temporary conversion key $USK_{EN,GID}{}' = \{USK_{i,GID}{}', i \in S_{j,GID}\}$ is generated for the edge IoT agent. AA_i sends the generated $USK_{EN,GID}{}'$ to the corresponding DU, and the DU calculates $USK_{i,GID} = y_i + H(GID)k_i + z$ by choosing a random $z \in Z_r$ to obtain the private key $USK_{EN,GID} = \{USK_{i,GID}, i \in S_{j,GID}\}$ for the general attribute i.

(2) Key Generation for Time and Location Attributes

If a cipher text has a limited access time and location, the DU needs to request the private key of the time and location from the corresponding AA_i within the valid time and location range. AA_i calculates $TSK_{i,GID}{}' = y_i + H(GID)(k_i + t_i)$ for time attributes and $LSK_{i,GID}{}' = y_i + H(GID)(k_i + l_i)$ for location attributes. Similarly, DU uses the temporary keys $TSK_{EN,GID}{}' = \{TSK_{i,GID}{}', i \in ST_{j,GID}\}$ and $LSK_{EN,GID}{}' = \{LSK_{i,GID}{}', i \in SL_{j,GID}\}$ to calculate the private key $TSK_{i,GID} = y_i + H(GID)(k_i + t_i) + z$ and $LSK_{i,GID} = y_i + H(GID)(k_i + l_i) + z$ for the time and location attribute i.

5. Data Decryption

Due to the limited resources of power IoT terminals, we divide the decryption process into two stages: pre-decryption on the IoT agent and local decryption at the DU.

First, the DU and edge node obtain the cipher text CT from the cloud server. The edge node runs the pre-decryption algorithm to decrypt the cipher text and sends the partial decryption result to the DU. Then, the DU obtains the correct message by one simple scalar multiplication.

(1) Pre-decryption

The edge IoT agent inputs the attribute set S of the DU and generates the set $X = \{x | \rho(x) \in S\}$. If the DU's attributes satisfy the access structure, then there must exist a constant set $\{c_x \in Z_r\}_{x \in X}$ that can be found in polynomial time, making $\sum_{x \in X} c_x \Lambda_x = \varepsilon = (1, 0, \ldots, 0)$, which means $\sum_{x \in X} c_x \lambda_x = s$ and $\sum_{x \in X} c_x \omega_x = 0$. The edge IoT agent obtains the result $D_x = C_{1,x} - SK_{\rho(x),GID} C_{2,x} + H(GID)C_{3,x}$ since there are three types of attributes; the calculation is as follows:

(a) If $\rho(x)$ is a general attribute

$$\begin{aligned} P_x = D_x &= C_{1,x} - SK_{\rho(x),GID} C_{2,x} + H(GID)C_{3,x} \\ &= \lambda_x G + \gamma_x y_{\rho(x)} G - (y_i + H(GID)k_i + z)\gamma_x G + H(GID)\left(\omega_x G + \gamma_x k_{\rho(x)} G\right) \\ &= \lambda_x G + H(GID)\omega_x G - z\gamma_x G \end{aligned}$$

(b) If $\rho(x)$ is a time attribute

$$\begin{aligned} P_x = D_x &= C_{1,x} - SK_{\rho(x),GID} C_{2,x} + H(GID)C_{3,x} \\ &= \lambda_x G + \gamma_x y_{\rho(x)} G - (y_i + H(GID)(k_i + t_i) + z)\gamma_x G + H(GID)\left(\omega_x G + \gamma_x \left(k_{\rho(x)} + t_{\rho(x)}\right) G\right) \\ &= \lambda_x G + H(GID)\omega_x G - z\gamma_x G \end{aligned}$$

(c) If $\rho(x)$ is a location attribute

$$\begin{aligned} P_x &= D_x = C_{1,x} - SK_{\rho(x),GID}C_{2,x} + H(GID)C_{3,x} \\ &= \lambda_x G + \gamma_x y_{\rho(x)} G - (y_i + H(GID)(k_i + l_i) + z)\gamma_x G + H(GID)\left(\omega_x G + \gamma_x\left(k_{\rho(x)} + l_{\rho(x)}\right)G\right) \\ &= \lambda_x G + H(GID)\omega_x G - z\gamma_x G \end{aligned}$$

The edge IoT agent calculates $T_1 = \sum_{x\in X} c_x D_x = sG - z\sum_{x\in X} c_x\gamma_x G$ and $T_2 = \sum_{x\in X} c_x C_{2,x} = \sum_{x\in X} c_x\gamma_x G$ and sends the result $CT' = \{C_0, CT_{DATA}, H_{CT}, T_1, T_2\}$ to the DU.

(2) DU Decryption

DU only needs one simple scalar multiplication to obtain the plain text. DU calculates $ck' = C_0 - T_1 + zT_2$ and calculates $H_{CT}{}' = H(E_{ck'}(M))G$ by using ck'. If $H_{CT}{}' = H_{CT}$, it means the plain text is correct.

5. Security Analysis

This section proves the proposed CP-ABE access control scheme for power IoT systems to be secure under the DDH assumption.

Theorem 1. *If there is no adversary ϑ that can win the security game with a non-negligible advantage in polynomial time, then there is no simulator $\mathcal{B}$ that can selectively break the DDH assumption in polynomial time.*

We can use apagoge to prove it, assume the adversary ϑ defined in the security game proposed in 3.2.3 has a non-negligible advantage $\varepsilon > 0$ to win the game, and ϑ can perform any private key query, but a limitation exists that obtained private keys still do not satisfy the requirements in the access structure. Therefore, the secure game of the multi-authority scheme is equivalent to the secure game of the single authority scheme under this constraint. We could challenge the DDH assumption by building a simulator $\mathcal{B}$.

(1) Initialization

Adversary ϑ sends the DDH challenge to simulator $\mathcal{B}$ and selects the access structure (Λ^*, ρ) for attacking.

(2) Setup

Simulator $\mathcal{B}$ runs the authority initialization and selects two random numbers $k_i, y_i \in Z_r$ and exposes the public key $PK_i = \{k_i G,\ y_i G\}$ for each attribute i in the system.

(3) Phase 1

Adversary ϑ adaptively submits pairs (i, GID) to $\mathcal{B}$ to request the corresponding secret key. However, there is a limitation that all obtained secret keys cannot satisfy the requirements in the access structure. Then, $\mathcal{B}$ chooses a random $z \in Z_r$ and computes $SK_{i,GID}$ SK as the secret key of i with *GID*.

$$SK_{i,GID} = \begin{cases} USK_{i,GID} = y_i a + H(GID)k_i + z, \ if\ i \in normal\ attrs \\ TSK_{i,GID} = y_i a + H(GID)(k_i + t_i) + z, \ if\ i \in time\ attrs \\ LSK_{i,GID} = y_i a + H(GID)(k_i + l_i) + z, \ if\ i \in location\ attrs \end{cases}$$

(4) Challenge

Adversary ϑ selects two messages M_0, M_1 with equal length and sends them to simulator $\mathcal{B}$. Simulator $\mathcal{B}$ randomly selects a vector $\vec{v} = (s, v_2, \ldots, v_m) \in Z_p$ and calculates $\lambda_x = \Lambda^*{}_x \cdot \vec{v}$, where $\Lambda_x{}^*$ is the row x of matrix Λ^*. Then, $\mathcal{B}$ selects a random vector $\vec{u} = (0, u_2, \ldots, u_m) \in Z_p$ and calculates $\omega_x = \Lambda^*{}_x \cdot \vec{u}$. Simulator $\mathcal{B}$ then obtains $\beta \in \{0, 1\}$

by flipping a coin and calculates $C_0 = M_\beta + sG$. Finally, simulator $\mathcal{B}$ generates a challenge cipher text according to the scheme and sends it to adversary ϑ.

$$\left(C_{1,x} = \lambda_x G + \gamma_x y_{\rho(x)} Z, C_{2,x} = \gamma_x bG, C_{3,x} = \begin{cases} \omega_x G + \gamma_x k_{\rho(x)} bG \\ \omega_x G + \gamma_x \left(k_{\rho(x)} + t_{\rho(x)} \right) bG \\ \omega_x G + \gamma_x \left(k_{\rho(x)} + l_{\rho(x)} \right) bG \end{cases} \right)$$

(5) Phase 2

Adversary ϑ can continue submitting (i, GID) to simulator $\mathcal{B}$ for the secret key corresponding to i without violating the constraints defined in Phase 1.

(6) Guess

Adversary ϑ submits a guess value $\beta' \in \{0, 1\}$. If $\beta' = \beta$, simulator $\mathcal{B}$ outputs 0 to indicate that the guess result is $Z = abG$, which means adversary ϑ has won the game; otherwise, simulator $\mathcal{B}$ outputs 1 to indicate that the guess is $Z = R$. The advantage of attacker A is ε, as defined in Theorem 1. Therefore, the probability that adversary ϑ guesses β correctly in this case is $Pr[\mathcal{B}(G, aG, bG, Z = abG) = 0] = \frac{1}{2} + \varepsilon$. If $Z = R$, adversary ϑ is not able to obtain any valuable information about β since R is selected at random. Therefore, the probability that adversary ϑ is correct about guessing β is $Pr[\mathcal{B}(G, aG, bG, Z = R) = 0] = \frac{1}{2}$ in this case. The advantage of simulator $\mathcal{B}$ to solve this security problem is

$$\begin{aligned} \mathcal{B} &= \tfrac{1}{2}(Pr[\mathcal{B}(G, aG, bG, Z = abG) = 0] \\ &+ Pr[\mathcal{B}(G, aG, bG, Z = R) = 0]) - \tfrac{1}{2} \\ &= \tfrac{1}{2}\left(\tfrac{1}{2} + \varepsilon + \tfrac{1}{2}\right) - \tfrac{1}{2} = \tfrac{\varepsilon}{2} \end{aligned}$$

In the hypothesis, the advantage ε of adversary ϑ is not negligible, so the advantage $\frac{\varepsilon}{2}$ of simulator $\mathcal{B}$ is also not negligible. However, there is no algorithm that can solve DDH difficult problems with a non-negligible advantage in polynomial time, so there is no adversary that can break the proposed scheme with a non-negligible advantage in polynomial time. Therefore, the proposed scheme satisfies the selective plain text security under the DDH assumption.

5.1. Data Security

In this paper, the ECC algorithm based on ECDLP can ensure that users without corresponding attributes cannot obtain any information about their secret key $\{y_i, k_i, t_i, l_i\}$ from the corresponding public key $\{y_i G, k_i G, t_i G, l_i G\}$ in polynomial time. The data M are encrypted through the symmetric key ck, which is implied in the cipher text C_0. Assuming the symmetric key ck can be mapped to cG, where $c \in Z_r$, as s is randomly selected by the data owner, $C_0 = (c + s)G$ is a random point on the elliptic curve. The adversary is unable to obtain any valuable information about ck and M according to the ECDLP. In addition, s is a shared secret divided by λ_x and can only be recovered with enough parts, so the cipher text can only be decrypted if the access structure (Λ, ρ) is satisfied with the data user's attributes. Any invalid user who does not have an attribute declared by the access policy does not have the attribute corresponding to row of Λ_x making $\sum_{x \in X} c_x \Lambda_x = \varepsilon = (1, 0, \ldots, 0)$, so the first element s of vector $\overrightarrow{v}$ cannot be calculated. Therefore, the proposed scheme can ensure the security of the data.

5.2. Forward Safety

Forward security ensures that the revoked user cannot access the data again. The proposed scheme uses GID to identify the data user and saves his attributes by the attribute list. When a user is revoked, the authority only needs to delete the attributes from the list corresponding to GID. When the revoked user tries to decrypt the data, the authority rejects his request because his GID is not in the system, and the authority cannot determine whether the user has the attributes according to the attribute list. To revoke a user's

attributes, the authority can simply modify his attributes list. The decryption request is also rejected because the declared attributes are not in the list. Therefore, forward security is guaranteed in this scheme.

5.3. Collusion Attack

To ensure the security of data, the proposed scheme must be able to resist collusion attacks. In other words, if multiple users collude with each other, they cannot decrypt the cipher text unless at least one of them can decrypt the cipher text independently. In the stage of key generation, the scheme uses GID to associate the attributes with the corresponding user so that the attributes cannot be combined successfully with other attributes during the decryption stage. For example, Alice intends to collude with Bob to decrypt the cipher text under the access policy $A \wedge B \wedge (C \vee D)$. Alice only owns properties A and B, and Bob only owns C. It is obvious that neither of them can decrypt the cipher text independently. If they collude with each other, Alice can only obtain part of the pre-decryption cipher text of x from the edge IoT agent: $\lambda_x G + H(GID_{Alice})\omega_x G + z\gamma_x G$. Bob can only get part of the cipher text $\lambda_x G + H(GID_{Bob})\omega_x G + z\gamma_x G$ as well. As the users are unique in the system, which means $GID_{Alice} \neq GID_{Bob}$, Alice and Bob cannot collude to obtain $\{c_x \in Z_r\}_{x \in X}$ and make $\sum_{x \in X} c_x \Lambda_x = \varepsilon = (1, 0, \ldots, 0)$ workable. In this way, collusion attack resistance is realized in the proposed scheme.

6. Performance Analysis

In this section, a detailed comparative analysis of the overhead of computation and cryptographic operations between the previous and proposed schemes is presented, which can evaluate the efficiency and security of the proposed CP-ABE scheme. First, we compare and depict the security and system features of the schemes in Table 2.

Table 2. Comparison of the schemes.

Scheme	Access Structure	Pairing Free	Multi-Authority	Time and Location	Decryption Outsourcing	Environment
Odelu [18]	AND GATE	Yes	No	No	No	
Yao [20]	access tree	Yes	No	No	No	Cloud
Ding [23]	linear secret sharing scheme (LSSS)	Yes	No	No	No	Cloud
Junejo [25]	AND GATE	Yes	No	No	Yes	Fog + Cloud
Our scheme	LSSS	Yes	Yes	Yes	Yes	Edge + Cloud

It can be observed from Table 2 that the schemes are all pairing free and ECC based, [18,20,25] adopt access tree and gate access which is less insufficient than LSSS to handle the fine-grained access control. The scheme proposed by Ding [23] and our scheme both adopt the LSSS access strategy, which has rich and flexible expression ability and meets the needs of fine-grained access control in the practical application of the IoT system. However, Ding's scheme does not support multi-authority and is not capable of decryption outsourcing. The scheme proposed by [25] realizes an ECC-based attribute encryption scheme based on the fog environment. However, in the IoT environment, the constraints of access time and location also need to be taken into consideration. Our scheme is more suitable for resource-constrained power IoT by using edge computing technology to implement outsourcing encryption and decryption. Obviously, the system performance of our scheme in this chapter is better than that of the other four schemes.

The communication overhead depends on the length of the message that is being transmitted between the entities. And generally, this message consists of the ciphertext, public keys and private keys. Therefore, we compared with other CP-ABE schemes by using the size of the ciphertext, public and private keys. For the sake of comparison, it is assumed that all the schemes to be compared are at the same security level and the unit of comparison is considered as ECC based 160-bit, given by $|G|$. Consequently, the size of

the point on 160-bit ECC is $2|G|$. It is assumed for the sake of simplicity, that the length of the attribute set and the tree is $|G|$. Thus, the size of the ECC based public key is $2|G|$ and the size of the private key is given by $|G|$ the communication overhead comparison is presented in Table 3.

Table 3. Communication of computation overhead of the schemes.

Scheme	Ciphertext(Bits)	Public Key(Bits)	Private Key(Bits)
Odelu [18]	$(Na - \|\Lambda\| + 3)\|G\|$	$(3Na + 1)\|G\|$	$2 * \|G\|$
Yao [20]	$(2Nr + 2)\|G\|$	$(2Na + 2)\|G\|$	$(Nr + 1)\|G\|$
Ding [23]	$(2Nr + 1)\|G\|$	$(2Na + 2)\|G\|$	$(\|\Lambda\|)\|G\|$
Junejo [25]	$(Na - \|\Lambda\| + 2)\|G\|$	$(Na + 1)\|G\|$	$1 * \|G\|$
Our scheme	$(3Nr + 1)\|G\|$	$(2Na + 2)\|G\|$	$(\|\Lambda\|)\|G\|$

Note: Nr: Number of rows in access matrix Λ, Na: Total number of attributes in the system, Da: Minimum number of attributes satisfying the access policy, $|\Lambda|$: number of attributes in the access policy, $|G|$: represents 160 bits considered as unit of measurement.

Compared with other schemes, the data user and edge agent in our scheme needs the attribute authority's help to complete the decryption as the secret key is implicitly maintained in the attribute authority. It seems that our scheme increases the communication cost. However, most of the communication work is done by the edge agent and AA_i, and IoT terminals only need to save a private key of $|G|$. In addition, authority can just modify the attribute list of the one to be revoked to complete the attribute revocation without affecting others in the system. Therefore, our scheme reduces the communication pressure of the IoT terminals in fact.

The computational overhead of the schemes is mainly concentrated in the following three stages: encryption, pre-decryption, and local decryption. To compare our scheme with other schemes in terms of computational overhead, we consider scalar multiplication based on ECC as a unit of measurement. The comparison of computation overhead of the schemes is described in Table 4.

Table 4. Comparison of computation overhead of the schemes.

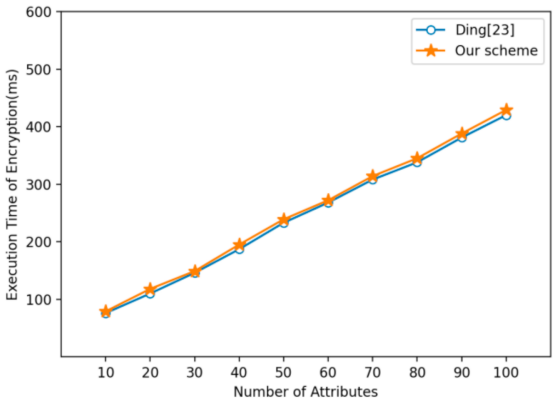
Scheme	Encryption	Pre-Decryption	Local Decryption
Odelu [18]	$(Na - \|\Lambda\| + 2)G$	\	$(Na - \|\Lambda\| + 3)G$
Yao [20]	$(Nr + 1)G$	\	$(Da + 1)G$
Ding [23]	$(3Nr + 1)G$	\	$(Da + 1)G$
Junejo [25]	$(Na - \|\Lambda\| + 1)G$	\	$(Na - \|\Lambda\| + 2)G$
Our scheme	$(4Nr + 1)G$	$(Da + 1)G$	$(1)G$

Note: Nr: Number of rows in access matrix Λ, Na: Total number of attributes in the system, Da: Minimum number of attributes satisfying the access policy, $|\Lambda|$: number of attributes in the access policy, G: scalar multiplication based on ECC.

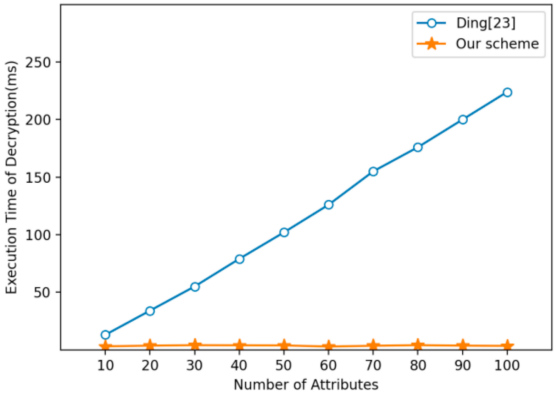
Table 4 shows the computational overhead of several schemes in the process of encryption and decryption. It can be concluded that [18] and [25] cost the least in encryption and decryption, as their computational overhead is independent of the number of attributes. However, the overhead is proportional to the difference between the number of attributes used in the access policy and the total number of attributes defined in the system. To decrease the computational overhead of encryption and decryption, the access policy needs to be quite complicated. Scheme [20] seems to have a higher encryption efficiency than our scheme because it uses the KP-ABE scheme, the devices encrypt the data by the required set of attributes, and the fine-grained access policy cannot be set. Scheme [23] also uses the LSSS structure and ECC algorithm. We take the time and location attributes into consideration in the encryption process, so we need to perform an extra scalar multiplication for the

time and location attributes. To show the efficiency of the two schemes more intuitively, we conducted a simulation experiment on Ubuntu 18.04 x64, where the server is an Intel Xeon E3 at 3.4 GHz and 8 GB RAM. We used Python and Charm libraries, which provide simple scalar multiplication on groups of elliptic curves, to program the test routine. The size of the elliptic curve used was 512 bits, and the order of the elliptic curve group was 160 bits. We implemented [23] and our scheme and recorded the time spent on encryption and decryption in the case of different numbers of attributes. The results illustrated in the following diagrams are the average values of 50 program iterations.

Figure 2 shows that scheme [23] is superior to our scheme in terms of execution time of encryption because we take the time and location attributes into consideration, making access control more fine-grained. The encryption of the time and location attributes costs a few scalar multiplication operations. However, the decryption time of our scheme has no obvious linear relationship with the number of attributes, as we outsource most of the decryption operations to the edge IoT agent, which has powerful computing capacity, so the local decryption only needs to calculate the scalar multiplication operation one time, which greatly reduces the computing overhead of the power terminals. Moreover, in the scenario of power IoT, the terminals are generally set up to upload the data regularly, while users acquire data on demand. Therefore, users or terminals have much higher requirements for decryption performance than encryption performance. In conclusion, the scheme proposed in this paper can effectively improve the performance of the CP-ABE algorithm and is more suitable for power IoT.



(**a**) Execution time of encryption



(**b**) Execution time of decryption

Figure 2. Comparison of the schemes' execution time.

7. Conclusions

In this paper, we propose a novel CP-ABE algorithm based on ECC combined with edge computing. The scheme considers the dynamic time and location attributes for fine-grained access control and outsources most computing to the edge IoT agent. The security

of the proposed scheme is also proven under the DHH assumption. To avoid the problems of a single authority and key escrow, multiple authorities are used to manage the attributes. In addition, we restrict the access of the cipher text by the time and location of data users to achieve more fine-grained access control. Finally, the experimental analysis proves that our scheme is effective and suitable for the power IoT.

However, there are also some limits in our scheme. The calculation of ciphertext and key has linear relationship with the number of attributes, that is, the length of the ciphertext and key will increase with the number of attributes of the user and access structure, which causes the system less efficient. In the future, we are planning to enhance the performance of the proposed CP-ABE scheme with the constant-size key and ciphertext.

Author Contributions: Methodology, R.C. and K.W.; project administration, W.L.; writing—original draft, Y.S.; writing—review and editing, R.C. and W.C.; funding acquisition, J.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China, grant number 2020YFB0905900.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Fu, Z.; Li, X.; Yuan, Y. Discussion on key technologies of ubiquitous power Internet of things. *Power Constr.* **2019**, *40*, 1–12.
2. Ahmed, E.; Ahmed, A.; Yaqoob, I.; Shuja, J.; Gani, A.; Imran, M.; Shoaib, M. Bringing Computation Closer toward the User Network: Is Edge Computing the Solution? *IEEE Commun. Mag.* **2017**, *55*, 138–144. [CrossRef]
3. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 20–23 May 2007; pp. 321–334.
4. Lewko, A.; Okamoto, T.; Sahai, A.; Takashima, K.; Waters, B. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In *Proceedings of the Transactions on Petri Nets and Other Models of Concurrency XV*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 62–91.
5. Li, L.; Gu, T.; Chang, L.; Xu, Z.; Liu, Y.; Qian, J. A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram. *IEEE Access* **2017**, *5*, 1137–1145. [CrossRef]
6. Deng, H.; Wu, Q.; Qin, B.; Domingo-Ferrer, J.; Zhang, L.; Liu, J.; Shi, W. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. *Inf. Sci.* **2014**, *275*, 370–384. [CrossRef]
7. Goyal, V.; Jain, A.; Pandey, O.; Sahai, A. Bounded Ciphertext Policy Attribute Based Encryption. In Proceedings of the International Colloquium on Automata, Languages and Programming, Reykjavik, Iceland, 7–11 July 2008; Aceto, L., Damgard, I., Goldberg, L.A., Halldorsson, M.M., Ingolfsdottir, A., Walukiewicz, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2009.
8. Yan, X.; Ni, H.; Liu, Y.; Han, D. Privacy-preserving multi-authority attribute-based encryption with dynamic policy updating in PHR. *Comput. Sci. Inf. Syst.* **2019**, *16*, 831–847. [CrossRef]
9. Belguith, S.; Kaaniche, N.; Laurent, M.; Jemai, A.; Attia, R. PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT. *Comput. Netw.* **2018**, *133*, 141–156. [CrossRef]
10. Li, J.; Yao, W.; Zhang, Y.; Qian, H.; Han, J. Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing. *IEEE Trans. Serv. Comput.* **2017**, *10*, 785–796. [CrossRef]
11. Yu, S.; Wang, C.; Ren, K.; Lou, W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; Institute of Electrical and Electronics Engineers (IEEE): San Diego, CA, USA, 2010; pp. 1–9.
12. Green, M.; Hohenberger, S.; Waters, B. *Outsourcing the Decryption of ABE Ciphertexts*; USENIX Association: San Francisco, CA, USA, 2011.
13. Li, W.-M.; Li, X.-L.; Wen, Q.-Y.; Zhang, S.; Zhang, H. Flexible CP-ABE Based Access Control on Encrypted Data for Mobile Users in Hybrid Cloud System. *J. Comput. Sci. Technol.* **2017**, *32*, 974–990. [CrossRef]
14. Peng, Z.; Chen, Z.; Liu, J.K.; Liu, H. An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 753–762.
15. Zuo, C.; Shao, J.; Wei, G.; Xie, M.; Ji, M. CCA-secure ABE with outsourced decryption for fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 730–738. [CrossRef]

16. Fan, K.; Xu, H.; Gao, L.; Li, H.; Yang, Y. Efficient and privacy preserving access control scheme for fog-enabled IoT. *Future Gener. Comput. Syst.* **2019**, *99*, 134–142. [CrossRef]
17. Zhong, H.; Zhou, Y.; Zhang, Q.; Xu, Y.; Cui, J. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. *Future Gener. Comput. Syst.* **2021**, *115*, 486–496. [CrossRef]
18. Odelu, V.; Das, A.K. Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography. *Secur. Commun. Netw.* **2016**, *9*, 4048–4059. [CrossRef]
19. Odelu, V.; Das, A.K.; Khurram Khan, M.; Choo, K.K.R.; Jo, M. Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts. *IEEE Access* **2017**, *5*, 3273–3283. [CrossRef]
20. Yao, X.; Chen, Z.; Tian, Y. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Gener. Comput. Syst.* **2015**, *49*, 104–112. [CrossRef]
21. Sowjanya, K.; Dasgupta, M.; Ray, S.; Obaidat, M.S. An Efficient Elliptic Curve Cryptography-Based Without Pairing KPABE for Internet of Things. *IEEE Syst. J.* **2019**, *14*, 2154–2163. [CrossRef]
22. Qin, X.; Huang, Y.; Li, X. An ECC-based access control scheme with lightweight decryption and conditional authentication for data sharing in vehicular networks. *Soft Comput.* **2020**, *24*, 18881–18891. [CrossRef]
23. Ding, S.; Li, C.; Lia, H. A Novel Efficient Pairing-Free CP-ABE Based on Elliptic Curve Cryptography for IoT. *IEEE Access* **2018**, *6*, 27336–27345. [CrossRef]
24. Raj, N.; Pais, A. CP-ABE Scheme Satisfying Constant-size Keys based on ECC. In Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, Paris, France, 10 July 2020; SCITEPRESS—Science and Technology Publications: Setúbal, Portugal, 2020; pp. 535–540.
25. Junejo, A.K.; Komninos, N. A Lightweight Attribute-Based Security Scheme for Fog-Enabled Cyber Physical Systems. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 2145829. [CrossRef]
26. Tian, Y.; Shao, T.; Li, Z. An Efficient Scheme of Cloud Data Assured Deletion. *Mob. Netw. Appl.* **2020**. [CrossRef]
27. Hong, J.; Xue, K.; Xue, Y.; Chen, W.; Wei, D.S.L.; Yu, N.; Hong, P. TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud. *IEEE Trans. Serv. Comput.* **2017**, *13*, 158–171. [CrossRef]