Future Generation Computer Systems 49 (2015) 104–112

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A lightweight attribute-based encryption scheme for the Internet of Things

Xuanxia Yao [a,*], Zhi Chen [a], Ye Tian [b,c]

[a] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, 100083, China
[b] Computer Network Information Center, Chinese Academy of Sciences, Beijing, 100190, China
[c] DNSLAB, China Internet Network Information Center, Beijing, 100190, China

HIGHLIGHTS

- Propose a lightweight no-pairing ECC-Based ABE scheme for the Internet of Things.
- The security depends on the ECDDH assumption instead of bilinear Diffie–Hellman based assumptions.
- The criteria and metrics for measuring the overhead are defined uniformly.
- Comparisons with the existing ABE schemes in efficiency illustrate its lightweight.

ARTICLE INFO

Article history:
Received 30 April 2014
Received in revised form
2 August 2014
Accepted 8 October 2014
Available online 18 October 2014

Keywords:
Internet of Things
Attribute-based encryption
Elliptic curve cryptography
Decision Diffie–Hellman problem
Selective-set model

ABSTRACT

Internet of Things (IoT) is an emerging network paradigm, which realizes the interconnections among the ubiquitous things and is the foundation of smart society. Since IoT are always related to user's daily life or work, the privacy and security are of great importance. The pervasive, complex and heterogeneous properties of IoT make its security issues very challenging. In addition, the large number of resources-constraint nodes makes a rigid lightweight requirement for IoT security mechanisms. Presently, the attribute-based encryption (ABE) is a popular solution to achieve secure data transmission, storage and sharing in the distributed environment such as IoT. However, the existing ABE schemes are based on expensive bilinear pairing, which make them not suitable for the resources-constraint IoT applications. In this paper, a lightweight no-pairing ABE scheme based on elliptic curve cryptography (ECC) is proposed to address the security and privacy issues in IoT. The security of the proposed scheme is based on the ECDDH assumption instead of bilinear Diffie–Hellman assumption, and is proved in the attribute based selective-set model. By uniformly determining the criteria and defining the metrics for measuring the communication overhead and computational overhead, the comparison analyses with the existing ABE schemes are made in detail. The results show that the proposed scheme has improved execution efficiency and low communication costs. In addition, the limitations and the improving directions of it are also discussed in detail.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

With the booming of wireless communications, micro-electro-mechanical systems (MEMS), digital electronics and mobile computing, IoT has developed vigorously, and been applied not only in the academic research and industrial fields but also in daily life [1], such as smart grid [2], e-health [3], e-home, environment monitoring [4], smart city and so on. By connecting sensors, tiny smart devices and intelligent everyday items with the Internet, the data can be collected or distributed automatically and the virtual information world can be integrated seamlessly with the physical world [5]. Applications based on IoT not only make people live easily and smartly, and also bring many challenges. For one aspect, according to the novel system architecture proposed by H. Ning and H. Liu [6], ubiquitous data collection is indispensable in the perception layer. Moreover, whether the unit or ubiquitous IoT, the application layer should be responsible for data processing, which may require sharing the collected data among users. For the other aspect, with more and more sensors available and able to be linked to the user for gathering data, individuals want to control their

* Corresponding author. Tel.: +86 13671086439.
E-mail address: yaoxuanxia@163.com (X. Yao).

http://dx.doi.org/10.1016/j.future.2014.10.010
0167-739X/© 2014 Elsevier B.V. All rights reserved.

personal data and make high requirements for data security and privacy preservation. The two conflicting aspects make the data collection, distribution and utilization bring severe security challenges for the IoT applications.

For instance, in the ubiquitous IoT application such as smart city, data is usually gathered from various sources owned by different administrative domains (e.g., smart phones, and public or private transportation providers). The data collection may be out of the user's knowledge and data transmitting may be in plaintext. Since the massive collected data is shared among different departments, which may be accessed by unauthorized users to cause serious problems or even be used to harm the owners of the data if no security restriction is made on it. Another example is a unit IoT application, that is health or medical monitoring. Normally, the data collected by the body sensors applied to an elderly person or patient should be always sent to the server of the medical center or hospital and accessible only by the specified doctors, because the body data are all sensitive data. The privacy may be broken if it is transmitted in plaintext or there is no appropriate access control made on it, which may lead to serious result. In addition, the multi-hop wireless broadcast communication mode in IoT is also vulnerable to eavesdropping.

Similar to the traditional (wire or wireless) networks, data security in IoT also includes confidentiality, integrity, authenticity and privacy. As for the privacy and confidentiality, since data are always transmitted in broadcast communication mode in the IoT, storage and dynamically shared through the heterogeneous and distributed networks, encryption and preventing unauthorized entities from accessing are very important [7], which can be achieved by cipher-text based access control mechanism. For data integrity and authenticity, authentication is a fundamental and efficient approach. For instance, H. Ning et al. put forward an aggregated-proof based hierarchical authentication scheme for the Internet of Things [8] in 2013. For the sake of practicability, the lightweight authentication approach should be the first choice of IoT.

Attribute-based encryption (ABE) system has the nature that any user can decrypt the cipher-text as long as it meets the required attributes, which makes it very suitable for cipher-text based access control and broadcast encryption. Unfortunately, it is very difficult to implement the existing ABE schemes in the resources-constraint IoT, because they are all based on the expensive bilinear pairing operations. In order to keep the data privacy and confidentiality in IoT, a lightweight attribute-based encryption scheme is indispensable.

In this paper, considering the fact that ECC algorithm has much stronger bit security than RSA as well as other exponential-based public key cryptographic algorithm, and it is easy to be realized on hardware or a chip, we propose a no-pairing ECC-Based ABE scheme to deal with the data security and privacy issues in IoT. Since it replaces the expensive bilinear pairing operation with point scalar multiplication on elliptic curve, it can meet the lightweight requirement and is suitable for IoT.

The main contributions are as follows: (1) A lightweight no-pairing ECC-Based ABE scheme is proposed to address the data security and privacy issues in the IoT. (2) The proposed ABE scheme's security depends on the ECDDH problem instead of bilinear Diffie–Hellman assumption, which can reduce the computation overhead and communication overhead. The security proof is performed in attribute based selective-set model. (3) The criteria and metrics for measuring the communication overhead and computational overhead are defined uniformly. (4) The lightweight feature is illustrated by comparing it with the existing ABE schemes, which indicates that it is more practical for IoT than others.

The remainder of this paper is organized as follows: In Section 2, we review the related works on attribute-based encryption and the related applications in IoT. Section 3 presents the preliminaries related to the proposed ABE scheme. Section 4 gives a detail description of the lightweight ABE scheme for IoT. The security proof is made in Section 5, and the performance is analyzed in Section 6. Finally, Section 7 draws a conclusion.

2. Related work

The concept of attribute-based encryption was first introduced in Advances in Cryptology EUROCRYPT 2005 [9]. It is an extension or generalization of identity-based cryptosystem, which can realize fuzzy identity by combining the user's identity with a series of attributes and achieve the aim of privacy preserving. In ABE system, a user's identity is composed of a set of strings which serve as descriptive attributes of the user. Messages are encrypted under a set of attributes describing the intended receivers, and the secret or private key of these users is also associated with the attributes set for encryption. Attribute-based encryption schemes allow any user to decrypt cipher-text as long as it has the attributes satisfying a threshold policy. This feature makes ABE a very popular solution to provide data security in loosely coupled, distributed environments and can be used as a perfect cryptographic building block to realize broadcast encryption [10] and cipher-text access control.

According to whether the private key or the cipher-text being associated with the access control policy, attribute-based encryption schemes can be further classified into Key-Policy ABE schemes (KP-ABE) [11] and Ciphertext-Policy ABE (CP-ABE) [12]. In KP-ABE, the message is encrypted under an attributes set, the access control policy that the receivers' attributes set should satisfy is embedded into the private keys. For basic KP-ABE, only the threshold gates can be used to express the access policy. In order to express the access policy flexibly, Goyal et al. also extends the KP-ABE to allow users' private keys to include any policy consisting of AND, OR threshold gates [11]. Ostrovsky et al. further extended KP-ABE to allow access policy including negative constraints [13]. In CP-ABE, the access policy is specified by the sender and embedded into the cipher-text, the encryption attributes set is associated with the private key [12]. CP-ABE is conceptually closer to the role based access control model, which make it more appealing than KP-ABE.

In recent years, the ABE based access control has drawn many researchers attention and many schemes have been proposed. Most of them focus on establishing expressive access control policies [11,13–15] to deal with the challenges in expressing access control policy, constructing constant size cipher-text [15–17] to limit the size of the cipher-text. Although some achievements have been made at the expense of increasing overheads, they do not meet the lightweight requirement of IoT yet. Meanwhile, as the broadcast is a main communication mode in perception layer of IoT, ABE based broadcast encryption is also hot topic [18,19]. Compared with existing one-to-one encryption schemes, these ABE based broadcast encryption schemes are efficient, because they can avoid sending messages encrypted with each individual recipient's public key. Considering the decryption efficiency, there are some researches on speeding up decryption [20] and improving efficiency. In addition, considering that different attributes are usually issued by different authorities, Chase proposed a multi-authority ABE scheme [21]. As far as security, all the ABE schemes are all proved selective security.

At present, ABE is mainly used to prevent unauthorized users from accessing the confidential data in cloud. Cloud computing is a main support technology of IoT. In addition, broadcast encryption is always required to secure data transmission in IoT. Although the existing traditional cryptography based solutions can meet the requirements in theory, they are usually realized by combining public key cryptography and/or symmetric cryptography and

Table 1
Notations.

Notations	Meaning
p	A large prime, the finite field with p elements is denoted by F_p.
E	An elliptic curve over the finite field F_p, which has a subgroup of large prime order q.
q	A large prime, which is used to denote the order of G in E over F_p.
Z_q	A finite integer field, whose elements set is $\{0, 1, \ldots, q-1\}$.
Z_q^*	$Z_q^* = Z_q - \{0\}$.
G	A base point on the elliptic curve E.
G_E	A subgroup of E with the order of q.
O	The zero element of an elliptic curve group.
HMAC(M, IK)	A cryptographic hash function to generate the hash-based message authentication code for M according to the integrity key *IK*.
$H(M)$	A hash function.
MK	The master private key of the ABE scheme.
PK	The master public key of the ABE scheme.
Params	The public key parameters of the ABE scheme.
ENC(M, EK)	A symmetric encryption algorithm, which encrypt the message M with the key *EK*.
DEC(C, EK)	A symmetric decryption algorithm, which decrypt the cipher-text C with the key *EK*.
k	The number of the attributes used to encrypt data.
n	The number of the attributes in a system.
PS	One point scalar multiplication.

need infrastructure for security mechanisms, which make them unfeasible in the distributed and dynamic environment of IoT. ABE can realize both broadcast encryption and cipher-text access control in distributed environment and has the natural advantage in assuring IoT data security. Researchers has begun to try using ABE in IoT. Nevertheless, the existing ABE schemes are all based on bilinear pairing, which is too expensive for IoT.

In this work, a lightweight ECC-Based ABE scheme is designed for performing cipher-text access control and broadcast encryption in IoT applications. Differing from other related work, it is based on ECC and its security is based on ECDDH problem instead of the bilinear pairing based assumption.

3. Preliminaries

The preliminaries related to the proposed ABE scheme include elliptic curve cryptosystem and its related primitives, Lagrange secret sharing and the access structure in attribute based encryption system. For the sake of description, the main notations used in this paper are listed in Table 1.

3.1. Elliptic curve cryptosystem and its related primitives

3.1.1. Elliptic curve cryptosystem

Elliptic curve cryptosystem (ECC) was introduced by Victor Miller and Neal Koblitz in 1985. The base of ECC operations is finite field (Galois Field) algebra with focus on prime Galois Fields F_p or binary extension Galois Fields F_2^m. Z_p is a prime Galois Field F_p, and an Elliptic curve over Z_p is defined by a cubic equation $y^2 = x^3 + a \cdot x + b$ and can be described by a set of parameters (q, a, b, G, p), where $a, b \in Z_p$, and $4a^3 + 27b^2 \neq (\text{mod } p)$. The operations in ECC consist of basic prime field operations and point operation. The former operations are simple, the latter operation refers to point scalar multiplication, which can be further refined by point add and point double operations. The point scalar multiplication is the fundamental and most time-consuming operation in ECC.

The security of ECC is based upon a hard number theoretic problem called Elliptic Curve Discrete Logarithms (ECDLP), which means that it is hard to find k such that $Q = k*P$ for a given elliptic curve and points P and Q on the curve. The hardness of ECDLP defines the security level of all ECC protocols, and no sub-exponential algorithm which can solve the ECDLP is known.

ECC can provide security based on the known public key cryptography primitives, which are Elliptic Curve Digital Signature Algorithm (ECDSA), key exchange/agreement (ECDH, Elliptic Curve Diffie–Hellman) and Elliptic Curve Integrated Encryption Standard (ECIES). Compared with other public key cryptography schemes, ECC has 3 distinguished features, which make it very fit for resources-constrained environments [22].

- It only requires significantly smaller key size than RSA and the modular exponent based public key schemes on the same level of security.
- Its point scalar multiplication operation is much faster than modular exponent operation and bilinear mapping operation.
- It is easy to be implemented in hardware.

In this paper, we take these advantages of ECC and the features of ABE to construct an ABE scheme for IoT, where Elliptic Curve Decisional Diffie–Hellman Problem (ECDDHP) serves as the complexity assumption, and the Elliptic Curve Integrated Encryption Standard (ECIES) is adopted to encrypt the data.

3.1.2. ECDDHP

ECDDH assumption is the decisional Diffie–Hellman over elliptic curve, which is related to both ECDLP and elliptic curve computational Diffie–Hellman Problem (ECCDHP, or ECDH).

ECDH is the Diffie–Hellman key exchange protocol over elliptic curves, which can help two parties with elliptic curve public–private key pairs to generate a shared secret key over an insecure channel. The shared secret can be directly used as a key or derive a new key to encrypt the subsequent communication by a symmetric key cryptography algorithm. Assumed that Alice and Bob use the same ECC system (q, a, b, G, p) to get their key pairs $(S_A, P_A = S_A \cdot G)$ and $(S_B, P_B = S_B \cdot G)$ respectively, a sharing secret $K_{A,B}$ can be generated by

$$K_{A,B} = S_A \cdot P_B = S_B \cdot P_A = S_A \cdot S_B \cdot G.$$

Similar to computational Diffie–Hellman (CDH assumption), for an elliptic curve group G_E with the order of q over a finite prime field F_p, ECDH problem states that, given $(G, c \cdot G, d \cdot G,)$ for a randomly chosen generator G and $c, d \in Z_q^*$, it is computationally intractable to get $c \cdot d \cdot G$. It can be seen that ECDH is related to ECDLP but much stronger than ECDLP.

The elliptic curve decisional Diffie–Hellman problem (DDHP) is the most significant variant of ECDH assumption, which can be described as follows.

For an elliptic curve group G_E of order q with generator G, the Decisional Diffie–Hellman assumption states that, given $c \cdot G$ and $d \cdot G$, where c and d are chosen from Z_q^* randomly, uniformly and independently, $c \cdot d \cdot G$ is a random element in G_E. Two probability distributions $(c \cdot G, d \cdot G, c \cdot d \cdot G)$ and $(c \cdot G, d \cdot G, Z)$ are computationally indistinguishable, here f is also chosen from Z_q^* randomly, uniformly and independently. That is to say that for the given triples $(c \cdot G, d \cdot G, c \cdot d \cdot G)$ and $(c \cdot G, d \cdot G, Z)$, it is impossible to decide whether $Z = c \cdot d \cdot G$. The triple $(c \cdot G, d \cdot G, c \cdot d \cdot G)$ is often called a ECDDH triple, and $(c \cdot G, d \cdot G, Z)$ is usually called a random triple.

ECDDH is more stronger than ECDH and ECDLP, because there are elliptic curve groups for which detecting ECDDH tuple is easy, but computing discrete logs or derive the key generated by CDH over them is believed to be hard. Thus, requiring that the ECDDH assumption holds in a group is an elliptic curve more restricting requirement.

3.1.3. Elliptic curve integrated encryption scheme

Elliptic Curve Integrated Encryption Scheme (ECIES) is used to provide data confidentiality and data integrity for users, which adopts ECDH to generate a sharing secret, from which the encryption key and the MAC key are derived respectively. Essentially, data

Table 2
Encryption algorithm of ECIES.

Encryption: input message M to be encrypted and the public key P_B of the receiver	
1	Select a random integer r from $[1, p-1]$.
2	Compute $R = r \cdot G$.
3	Compute $K = r \cdot P_B = (K_X, K_Y)$.
4	Check whether $K = O$ or not, if yes, go to Step 1.
5	Compute $k_{\mathrm{ENC}} \parallel k_{\mathrm{MAC}} = KDF(K_X)$, here, KDF is a key derivation function.
6	Compute $C = ENC(k_{ENC}, M)$ and $MAC_M = HMAC(k_{\mathrm{MAC}}, C)$.
7	Output or return "$R\|C\|MAC_M$".

Table 3
Decryption procedure of ECIES.

Decryption: input the cipher-text "$R\|C\|MAC_M$"	
1	Check whether R is on the elliptic curve, if not, output "$\perp$" and stop.
2	Compute $K = S_B \cdot R = (K_X, K_Y)$ and check whether $K = O$, if yes, output "$\perp$" and stop.
3	Compute $k_{\mathrm{ENC}} \parallel k_{\mathrm{MAC}} = KDF(K_X)$.
4	Verify whether $MAC_M = HMAC(k_{\mathrm{MAC}}, C)$, if not, output "$\perp$" and stop.
5	Compute $M = DEC(k_{ENC}, C)$.
6	Output or return M.

confidentiality is guaranteed by a symmetric cryptography algorithm with the encryption key and data integrity is guaranteed by a MAC function with the MAC key [23].

For the sake of clarity, the encryption and decryption procedure of ECIES are described respectively in Tables 2 and 3.

3.2. Secret sharing

The secret sharing refers to distributing a secret amongst a group of parties. The first secret sharing schemes were proposed by Shamir [9], who employs the fact that an n degree polynomial can be determined by $P_n(x) = \sum_{k=0}^{n} l_k(x) \cdot y_k$ in the case that $(n+1)$ points are given, where $l_k(x)$ is called Lagrange coefficient. Assume that there are $(n+1)$ points (x_i, y_i) for $i = \{0, \ldots, (n-1)\}$, $l_k(x)$ can be computed by $l_k(x) = \prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{x - x_j}{x_k - x_j}$. The method to construct the polynomial is called Lagrange interpolation, the polynomial $P_n(x)$ is called Lagrange interpolation polynomial.

In order to share the secret a_0 among n parties and reconstruct it at least by t parties, a $(t-1)$-degree polynomial $P_{(t-1)}(x) = \sum_{i=0}^{t-1} a_i x^i$ should be defined, where, the coefficients $\{a_1, a_2, \ldots, a_{t-1}\}$ are assigned as random values in a finite field. The value $P(ID_i)$ is a share of the secret and given to user i. When t two-tuples $(ID_i,\ P(ID_i))$ are put together, the polynomial $P_{(t-1)}(x)$ can be reconstructed by Lagrange interpolation, and the secret a_0 can be accordingly determined.

In the proposed ABE scheme, Shamir secret sharing scheme based on Lagrange interpolation over Z_p^* is used to reconstruct the decryption key or decrypt the cipher-text directly.

3.3. Access structure

The access structure is used to describe the access policy [11]. In ABE, the access structure can be defined analogously as Definition 1. An access structure can be represented by an access tree, which is also defined in [11].

Definition 1 (*Access Structure [11]*)**.** Let $\{A_1, A_2, \ldots, A_n\}$ be a set of attributes. A collection $\mathbb{A} = 2^{\{A_1, A_2, \ldots, A_n\}}$ is monotone, for $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure (respectively, monotone) is a collection (respectively, monotone) $\mathbb{A}$ of non-empty subsets of $\{A_1, A_2, \ldots, A_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{A_1, A_2, \ldots, A_n\}} \setminus \{\Phi\}$. The sets in A are called the authorized attributes sets, and the sets not in A are called the unauthorized attributes sets.

Definition 2 (*Access Tree [11]*)**.** In an access tree Γ, each non-leaf node of the access tree is a threshold gate, which is described by its children and a threshold value. If num_x is the number of children of a node x and d_x is its threshold value, then $0 < d_x \leq num_x$. When $d_x = 1$, the threshold gate is an "OR" gate, and when $d_x = num_x$, it is an "AND" gate. Each leaf node x of the access tree is described by an attribute and a threshold value $d_x = 1$.

Here, we also use the notations in [9] to describe an access tree. The parent of node x in an access tree is denoted by parent(x). The function index(x) returns the order number in its parent of node x, which is defined by the access tree, the children of a node x are numbered from 1 to num_x and the index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner. The function att(x) is defined only for a leaf node x, which denotes the attribute associated with the leaf node x in the access tree. An access tree with root r is denoted by Γ_r. If an attributes set γ satisfies the access tree Γ_x, it is denoted by $\Gamma_x(\gamma) = 1$. $\Gamma_x(\gamma)$ is computed recursively. If x is a non-leaf node, evaluate $\Gamma_{x'}(\gamma)$ for all children x' of node x. $\Gamma_x(\gamma)$ returns 1 if and only if at least d_x children return 1. If x is a leaf node, then $\Gamma_x(\gamma)$ returns 1 if and only if att$(x) \in \gamma$.

4. Scheme description

The proposed lightweight ABE scheme is a KP-ABE one, which involves a central attribute authority (responsible for key generation for attributes) and users. In this section, the formal definition for a KP-ABE system and the construction procedure for the proposed ABE scheme are given.

4.1. The formal definition for a KP-ABE scheme

A KP-ABE scheme consists of four algorithms of Setup, Encryption, Key-Generation, and Decryption [11].

- **Setup**: The Setup algorithm is a randomized algorithm, which is run by the authority and outputs the public key parameters PK and the master key MK. The public key parameters are published and the master key secret is kept secret by the authority.
- **Encrypt** $(M, \gamma, Params)$: The Encrypt algorithm is also a randomized algorithm, which is run by the sender and outputs cipher-text CM by taking the message M to be encrypted, the attributes set γ that the data user should satisfy, and the public key parameters PK as input.
- **Key-Generation** (Γ, MK): The Key-Generation algorithm is a randomized algorithm too, which is run by the authority and takes an access structure Γ and the master key MK as input. It outputs the decryption key D corresponding to the access structure.
- **Decrypt** $(CM, D, Params)$: The Decrypt algorithm is run by the receiver, which takes the cipher-text CM encrypted under the attributes set γ, the decryption key D for access control structure Γ, along with the public key parameters PK as input. If $\Gamma(\gamma) = 1$, it decrypt the cipher-text CM and outputs message M.

4.2. The proposed lightweight ABE scheme

The proposed lightweight ABE scheme is based on elliptic curve cryptography. Given an ECC scheme defined by a set of parameters (q, a, b, G, p). It is assumed that all the parameters are secure enough to meet the requirements of the applications.

For the attributes set ω, the secret key is constructed by secret sharing based on Lagrange interpolation. The Lagrange coefficient $\triangle_{i,\omega}$ for $i \in Z_q^*$ and a set ω, of elements in Z_q^* is determined by

$\triangle_{i,\omega} = l_i(x) = \prod_{j\in\omega, j\neq i} \frac{x-j}{i-j}$. Each attribute will be associated with a unique element in Z_q^*.

In addition, it should be stated that the authority in the proposed scheme is also an ECC-based key generator center.

(A) Setup

The attribute space in the system is defined as the universe of attributes $U = \{1, 2, \ldots, n\}$. For each attribute $i \in U$, choose a number s_i uniformly at random from Z_q^*. The public key of each attribute i is $P_i = s_i \cdot G$. Thereafter, choose s uniformly at random from Z_q^* to be the master (private) key MK, accordingly, the master public key PK is $PK = s \cdot G$. The public parameters are denoted by $Params = \{PK, P_1, \ldots, P_{|U|}\}$.

(B) Encryption $(M, \omega, Params)$

Different from the existing ABE schemes, the message M is encrypted by a secure symmetric cryptographic algorithm (ECIES) instead of being encrypted by modular exponent or bilinear pairing operation. The encryption key is derived from a random number by the ECC, which can be reconstructed under the attribute set, ω.

To encrypt a message M under the set of attributes, ω, randomly choose k from Z_q^* to compute C',

$$C' = k \cdot PK = (K\_x, K\_y).$$

If $C' = O$, re-choose k randomly from Z_q^* to compute C' until $C' \neq O$. Thereafter, compute C_i respectively

$$C_i = k \cdot P_i, \quad i \in \omega.$$

Let K_x be the encryption key and K_yx be the integrity key for message M, C and MAC_M can be computed respectively.

$$C = ENC(M, K\_x)$$
$$MAC_M = HMAC(M, K\_y).$$

The cipher-text is denoted by $CM = (\omega, C, MAC_M,\ C_i,\ i \in \omega)$.

(C) KeyGeneration (Γ, MK)

The KeyGeneration algorithm is used to output a key for decrypting the message encrypted under the attributes set ω if and only if $\Gamma(\omega) = 1$. For this purpose, a polynomial $q_u(x)$ with order of $(d_u - 1)$ should be defined for each node u in the access tree Γ in top-down manner, where d_u is the threshold of the node u. For the root R of the access tree Γ, set $q_R(0) = s$ and choose $(d_R - 1)$ other points for the polynomial $q_R(x)$ randomly to determine it uniquely. For any other node (including leaf node) u, $q_u(0) = q_{\text{parent}(u)}(\text{index}(u))$, similar to $q_R(x)$, $(d_u - 1)$ other points also need to be chosen randomly to define polynomial $q_u(x)$ uniquely.

When the polynomial of a leaf node u in the access tree is defined, a secret share of the decryption key for the leaf node u is defined as: $D_u = q_u(0)/s_i$, here, $i = \text{attr}(u)$ and s_i is the randomly chosen number from Z_q^* in Setup phase, s_i^{-1} is the inverse element of s_i over finite field Z_q^*. In this way, once all leaf nodes' polynomials are determined, their secret shares of the decryption key are determined respectively. That is to say that the decryption key is embedded in the access tree.

The decryption key can be denoted by $D = (D_u = q_u(0)/s_i,\ i = \text{attr}(u) \text{ and } i \in \omega)$.

(D) Decryption $(CM, D, Params)$

Similar to other ABE schemes, the decryption algorithm $\text{DecryptNode}(CM, D, u)$ for a node u in the access tree is defined as a recursive procedure.

For a leaf node u, Let $i = \text{attr}(u)$, $\text{DecryptNode}(CM, D, u)$ is defined as:

$$\text{DecryptNode}(CM, D, u) = \begin{cases} D_u \cdot C_i = q_u(0) \cdot s_i^{-1} \cdot k \cdot P_i \\ \quad = q_u(0) \cdot s_i^{-1} \cdot k \cdot s_i \cdot G \\ \quad = q_u(0) \cdot k \cdot G, \quad (i \in \omega) \\ \perp, \quad \text{Otherwise.} \end{cases}$$

It should be stated that the output of $\text{DecryptNode}(CM, D, u)$ is an element in elliptic curve group G_E or $\perp$.

For a non-leaf node u, it calls $\text{DecryptNode}(CM, D, v)$ for each of its child node v. Let ω_u be a set with arbitrary d_u child nodes of u, and for each node v in set ω_u, $\text{DecryptNode}(CM, D, v) \neq \perp$. If there is not such a ω_u, $\text{DecryptNode}(CM, D, u) = \perp$, otherwise,

$$\begin{aligned} &\text{DecryptNode}(CM, D, u) \\ &= \sum_{v\in\omega_u} \Delta_{i,\omega_u'}(0) \cdot \text{DecryptNode}(CM, D, v) \\ &\text{where } i = \text{index}(v), \omega_u' = \{\text{index}(v),\ v \in \omega_u\} \\ &= \sum_{v\in\omega_u} \Delta_{i,\omega_u'}(0) \cdot q_v(0) \cdot k \cdot G \\ &= \sum_{v\in\omega_u} \Delta_{i,\omega_u'}(0) \cdot q_{\text{parent}(v)}(\text{index}(v)) \cdot k \cdot G \\ &= \sum_{v\in\omega_u} \Delta_{i,\omega_u'}(0) \cdot q_u(i) \cdot k \cdot G \\ &= q_u(0) \cdot k \cdot G. \end{aligned}$$

Accordingly, for the root node R of the access tree, there should be $\text{DecryptNode}(CM, D, R) = q_R(0) \cdot k \cdot G = s \cdot k \cdot G = (K'\_x,\ K'\_y)$. Here, K'_x is considered to be the decryption key for message M and K'_y is the integrity key for message M. The encrypted message M can be decrypted by $M' = DEC(C, K'\_x)$.

If $HMAC(M', K'\_y) = MAC_M$, it indicates that message M is correctly decrypted and is not tampered. That is to say that the correctness, integrity and authenticity are all verified by MAC_M. The difference from the original ECIES is the MAC_M, which is calculated on the data directly instead of the cipher-text.

5. Security proof

5.1. Security model

At present, the Selective-Set security model is always used to prove the security of an ABE scheme, in which the two message encrypted by a KP-ABE are indistinguishable under chosen plaintext and attribute-set attack. The attribute-based Selective-Set model is based on a game, which is played by a challenger and an adversary. The game is described as follows [9].

- **Initialization**: The adversary declares the attributes set θ that he wants to attack on.
- **Setup**: The challenger runs the Setup algorithm in ABE scheme and sends the public key parameters to the adversary.
- **Phase 1**: The adversary is permitted to make many queries for the decryption keys for many access structures $\mathbb{A}_j$, where $\mathbb{A}_j(\theta) = 0$, for all j.
- **Challenge**: The adversary submits two equal length messages M_0 and M_1 to challenger. The challenger flips a random coin v and encrypts M_v under the attributes set θ. Thereafter, the cipher-text is sent to the adversary.
- **Phase 2**: Repeat phase 1.
- **Guess**: The adversary outputs a guess v' of v.

In the game, the advantage of the adversary is defined as $\varepsilon = \Pr[v' = v] - 1/2$. A KP-ABE scheme is secure in the attribute-based Selective-Set model, if an adversary can win the game in polynomial time with at most a negligible advantage.

5.2. Security proof

The security of the proposed ABE scheme is proved in the attribute-based Selective-Set model. Similar to the existing ABE schemes, the method of reduction to absurdity is used to prove the scheme's security. Since the security of our scheme depends on the Elliptic Curve Decisional Diffie–Hellman problem, reducing the hardness of the ECDDH assumption is made.

Theorem 1. *If an adversary $\mathcal{A}$ can attack our scheme successfully in the attribute-based selective-set model in polynomial-time, a simulator $\mathcal{B}$ can be constructed to solve the ECDDH problem with a non-negligible advantage.*

Proof. In the attribute-based selective-set model, if there is an adversary $\mathcal{A}$, who can attack our scheme in polynomial-time with an advantage ε, a simulator $\mathcal{B}$ can be constructed to gain the ECDDH game with advantage $\varepsilon/2$. The procedure for constructing such a simulator $\mathcal{B}$ is described as follows.

Firstly, the challenger sets the elliptic curve group G_E with the order of q over F_p and generator G. Then, the challenger flips a fair binary coin μ and randomly chooses a, b, z from Z_p^*. If $\mu = 0$, it sets $(A, B, Z) = (c \cdot G,\ d \cdot G,\ c \cdot d \cdot G)$; otherwise, it sets $(A, B, Z) = (c \cdot G,\ d \cdot G,\ z \cdot G)$. It is assumed that the universe of attributes U is defined.

Initialization: The simulator $\mathcal{B}$ get the attributes set θ, which is the adversary $\mathcal{A}$ wishing to attack upon. It is assumed that the access tree corresponding to the attributes set θ is Γ.

Setup: The simulator $\mathcal{B}$ runs the Setup algorithm of the proposed scheme to set the system public key parameters and sends them to the adversary $\mathcal{A}$.

(1) $\mathcal{B}$ sets the system parameter $Y = A = c \cdot G$.
(2) $\mathcal{B}$ sets Y_i according the following principles for all $i \in U$.
   If $i \in \theta$, $\mathcal{B}$ randomly chooses r_i from Z_q^* and sets $Y_i = r_i \cdot G$ and $y_i = r_i$.
   If $i \in (U - \theta)$, $\mathcal{B}$ randomly chooses β_i from Z_q^*, and sets $Y_i = \beta_i \cdot B = d \cdot \beta_i \cdot G$ and $y_i = d \cdot \beta_i$.
(3) $\mathcal{B}$ sends the system public key parameters $\{Y, Y_i, i \in U\}$ to $\mathcal{A}$.

It is obvious that $\{Y, Y_i\}$ corresponds to $\{PK, P_i\}$ of the proposed ABE scheme.

Phase 1: The adversary $\mathcal{A}$ can make many queries for the decryption key corresponding to any access structure γ, where the challenge set θ does not satisfy γ, that is $\gamma(\theta) = 0$. In other words, The adversary $\mathcal{A}$ can make queries for the decryption key corresponding to any attributes set δ, where $|\delta \cap \theta| < |\delta|$.

In order to make the adversary $\mathcal{A}$ can reconstruct the decryption key for the access structure γ, the simulator $\mathcal{B}$ needs to assign a polynomial Q_u with degree of d_u to every node u in the access tree γ. The polynomial Q_u for each node u in γ is defined as $Q_u(x)$ to be $q_u(x)$ in the proposed scheme. The shared secret is set to be the constant of the root's polynomial, that is $Q_R(0) = c$. The secret key corresponding to each leaf node x in γ is given by its polynomial as follows.

$$D_x = Q_x(0)/r_i = \begin{cases} q_x(0)/r_i, & \text{if } (\text{att}(x) \in \theta) \\ q_x(0)/\beta_i \cdot d, & \text{if } (\text{att}(x) \notin \theta) \end{cases} \quad \text{for } i = \text{att}(x).$$

The set $(D_x, x \in \gamma)$ is the secret key for the access structure γ, which is distributed to the adversary $\mathcal{A}$ in the same security way as that in our original scheme.

Challenge: The adversary $\mathcal{A}$ will submit two challenge messages M_0 and M_1 to the simulator $\mathcal{B}$. $\mathcal{B}$ flips a fair binary coin v, and computes the ciphertext of M_v. In order to encrypt the message M_v, $\mathcal{B}$ randomly chooses k from tZ_q^* and computes C'.

$$C' = k \cdot Y = (K\_x, K\_yx).$$

If $C' = O$, re-choose k randomly from Z_q^*, and computes C' until $C' \neq O$. Afterwards, $\mathcal{B}$ computes C_i as follows.

$$C_i = r_i \cdot B, \quad i \in \theta.$$

Let K_x be the encryption key for message M, and K_yx be the integrity key for message M. $\mathcal{B}$ computes C and MAC_{Mv} respectively, and transmits the cipher-text $(\theta, C, MAC_{Mv},\ C_i,\ i \in \theta)$ to $\mathcal{A}$.

$$C = ENC(M_v, K\_x)$$

$$MAC_{Mv} = HMAC(M_v, K\_y).$$

The cipher-text $(\theta, C, MAC_{Mv},\ C_i,\ i \in \theta)$ is sent to the adversary $\mathcal{A}$.

If $\mu = 0$, then $Z = c \cdot d \cdot G$. If k is set to be d, there should be $C' = k \cdot Y = d \cdot c \cdot G = Z$, and $C_i = k \cdot Y_i = d \cdot Y_i = d \cdot r_i \cdot G = r_i \cdot B$, where, $i \in \theta$.

If $\mu = 1$, then $Z = z \cdot G$. If k is set to be z, it turns out that $C' = z \cdot G$.

Since c, d and z are random numbers, C' will be a random element of G_E from the adversary $\mathcal{A}$'s view and it cannot obtain any sensitive information about M_v from the cipher-text.

Phase 2: Both the simulator $\mathcal{B}$ and the adversary $\mathcal{A}$ perform exactly as they did in Phase 1. In other words, Phase 1 is repeated.

Guess: The adversary $\mathcal{A}$ sends a guess v' of v to the he adversary $\mathcal{B}$.

If $(v' = v)$, the simulator $\mathcal{B}$ outputs $\mu' = 0$ to indicate that it was given a valid ECDDH-triple (A, B, Z).

If $(v' \neq v)$, the simulator $\mathcal{B}$ outputs $\mu' = 1$ to indicate that it was given a random triple (A, B, Z).

It is obvious that the construction scheme for the simulator $\mathcal{B}$ to generate the system public parameters and secret private keys are identical to that of the proposed scheme.

According to the game, when $\mu = 1$, the adversary $\mathcal{A}$ cannot gain any information about v. Therefore, we have

$$\Pr[v \neq v' \mid \mu = 1] = \Pr[v = v' \mid \mu = 1] = 1/2.$$

Since the simulator $\mathcal{B}$ outputs $\mu' = 1$ when $v \neq v'$, we have

$$\Pr[\mu' = \mu \mid \mu = 1] = 1/2.$$

When $\mu = 0$, the adversary $\mathcal{A}$ can get a valid cipher-text C of M_v. According to the assumption, the adversary's advantage is ε, therefore, we have

$$\Pr[v = v' \mid \mu = 0] = 1/2 + \varepsilon.$$

Since the simulator $\mathcal{B}$ outputs $\mu' = 0$ when $v' = v$, we have

$$\Pr[\mu' = \mu \mid \mu = 0] = 1/2 + \varepsilon.$$

According to the selective-set model for ABE, the overall advantage of the simulator $\mathcal{B}$ in this game is $(\Pr[v' = v] - 1/2)$. In our ECDDH game, $\Pr[v' = v] = 1/2\Pr[\mu' = \mu \mid \mu = 0] + 1/2\Pr[\mu' = \mu \mid \mu = 1] = 1/2(1/2 + \varepsilon) + 1/2 \cdot 1/2 = 1/2 + \varepsilon/2$. It turns out that the overall advantage of the simulator $\mathcal{B}$ in the ECDDH game is $(\Pr[v' = v] - 1/2 = 1/2 + \varepsilon/2 - 1/2 = \varepsilon/2)$, which is conflict with the fact of ECDDH problem.

6. Performance analysis

In order to assess the lightweight feature of the proposed ABE scheme, comparison analysis is made in two aspects of communication overhead and computational overhead with KP-ABE and CP-ABE.

At the same time, for evaluating the proposed ABE scheme objectively, the limitations of it are also discussed in detail.

6.1. Comparison metrics description

For the sake of comparison, the comparison metrics should not only be determined and defined clearly but also should be unified and kept consistent.

6.1.1. Communication overhead metrics

For communication overhead, it depends on the length of the message to be transmitted. In ABE, the message that should be transmitted mainly consists of the cipher-text, public key and

private key, so we make the lengths of the them as the communication overhead metrics to measure and compare the communication overhead. The three metrics are further relied on the principle of the ABE scheme.

As far as we know, the existing ABE schemes are all based on bilinear pairing, which makes them involve two groups G_1, G_2. Here, G_1 is a bilinear group with large prime order, the bilinear mapping is denoted by $G_1 \times G_1 \rightarrow G_2$. Since the basic operation of G_1 and G_2 are modular exponentiation, which is same as that of RSA, we call these ABE RSA based schemes. Corresponding to it, our scheme is called ECC based ABE scheme.

On the same security level, the key (whether public or private key) size of RSA is much longer than that of ECC, which means that ECC has stronger bit security than RSA. For instance, the security strength of 160-bit ECC is up to that of 1024-bit RSA, and 210-bit ECC is up to 2048-bit RSA. For the sake of comparability, it is assumed that all the schemes to be compared with are at the same security level and under the same attributes set. Moreover, we assume that the security level is equal to the security strength of 160-bit ECC and denoted by l, which is equal to 160. In addition, for the ease of description, we also assume that the length of the value derived from a hash or HMAC function, the key length of a symmetric cryptography algorithm, and the length of the data to be encrypted are all equal to l.

Based on the above assumption, the size of a point on the elliptic curve of the 160-bit ECC is $2l$, the size of its private key is l and the size of its public key is $2l$. Accordingly, both the public and private key size of the 1024-bit RSA are $6.4l$, and the size of an element in G_1 of a RSA based ABE scheme is $6.4l$ and the size of an element in G_2 of it is $12.8l$.

It should be noted that the cipher-texts in ABE schemes have to include the attributes set associated with the cipher-text and the length of it is linear with the number of the attributes. For the sake of comparison, all the ABE schemes to be compared with are assumed to be with the same encryption attributes set, so the length of attributes can be ruled out from the length of the cipher-text. Nevertheless, the length of the encryption attributes set does not always have no relation to the length of the cipher-text, different attribute usually corresponds to different part of the cipher-text. In such circumstances, the size of the attributes set is not only related with the length of the cipher-text but also related with the computational overhead.

6.1.2. Computational overhead metrics

For computational overhead, it is caused by the operations in an ABE scheme, which mainly include encryption, decryption, hash, HMAC, bilinear mapping, arithmetic and logic operations as well. Among these operations, bilinear mapping is the most expensive operation, the public key based encryption and decryption operations take the second place. Compared with the three operations, the costs for the rest operations can be ignored, so we take the costs caused by bilinear mapping, the public key based encryption and decryption as the computational overhead metrics.

According to the analysis in communication overhead metrics, the public key cryptosystem can also be roughly classified into RSA based scheme and ECC based scheme. In a RSA based public key scheme, the most expensive operation is modular exponential, and all other operations can be ignored. In an ECC based public key scheme, the most expensive operation is point scalar multiplication, similarly, all other operations can be ignored. In this way, the computational overhead caused by public key based encryption and decryption can be measured by modular exponential or point scalar multiplication.

For the sake of simplicity and computation, the approach in [23] is adopted to measure the computational overhead, according to which, one bilinear pairing is about 20 point scalar multiplication, and one modular exponential operation is 2 point scalar multiplication. Consequently, point scalar multiplication can be taken as the unit of computation overhead in ABE schemes.

6.2. Comparison and analysis

In order to show the lightweight feature of the proposed ABE scheme, we compare it with both the existing KP-ABE schemes and the existing CP-ABE schemes. According to Section 6.1, the communication overhead and computational overhead should be calculated respectively for the proposed scheme and each ABE scheme to be compared with.

Since the process of computing overhead for each ABE scheme is similar to each other, here, we only take the proposed scheme as an example to illustrate how to calculate the communication overhead and computational overhead.

The communication overhead is measured by the lengths of the cipher-text, public key and private key. In the proposed scheme, the cipher-text is $CM = (\omega, C, MAC_M, C_i,\ i \in \omega)$. As the length of encryption attributes set ω has been ruled out of the length of cipher-text according to assumption and analysis in 6.1.1, we just need to calculate the lengths of C, MAC_M and C_i for $i \in \omega$ respectively. According to the encryption process of the proposed scheme, C_i is a point on the elliptic curve and their length should be $2l$. Since the lengths of M and its MAC are assumed to be equal to the security level l, C and MAC_M are also l bit long. In this way, the length of the cipher-text in the propose scheme should be $(l+l+k\cdot 2l) = (2k+2)l$. In addition, the public key is $\{PK,\ P_i,\ i \in U\}$ and each element of it is a point on the elliptic curve, so the length of the public key is $(2l + n \cdot 2l) = (2n+2)l$. The proposed scheme's private key is $\{D_u = q_u(0)/s_i,\ i = \text{attr}(u) \text{ and } i \in \omega\}$, it is obvious that the length of it should be $k \cdot l$.

The computational overhead is measured by the costs for bilinear mapping, the public key based encryption and decryption operations. In our scheme, no bilinear mapping is involved. The process of encryption involves $(1 + k)$ point scalar multiplication, and the process of decryption involves no more than $(2k - 1)$ point scalar multiplication. To sum up, there are at most $3k$ point scalar multiplication.

The overhead or efficiency comparisons with the existing KP-ABE schemes are shown in Table 4. The comparisons with the existing CP-ABE schemes are shown in Table 5.

In the Internet of Things, the size of the encryption attributes set k is usually less than 30. It can be seen from Table 4 that only the cipher-text size in our scheme is longer than that of the scheme with constant size cipher-text [17], but our total size of cipher-text, public key and private key is much shorter than it. In addition, the computation overhead of ours is much lower than other schemes. So we can say that our scheme outperforms other KP-ABE schemes in lightweight. From Table 5, we can see that when the size of the encryption attributes set is no more than 10, our scheme has prominent advantage in lightweight over the existing CP-ABE schemes. When $k > 10$, only the cipher-text size in our scheme is longer than that of the scheme with constant size cipher-text [15], the rest metrics are much lower than those of it and others. Of course, our scheme also outperforms the existing CP-ABE schemes in lightweight.

6.3. The limitation of the proposed ABE schemes

Objectively, although the proposed scheme has remarkable advantages in efficiency, it still has some defects and inherent shortcomings. The limitations of the proposed scheme can be put up in the following 3 aspects.

(1) Poor Flexibility in Revoking Attribute.

Similar to most of the ABE schemes, the proposed ABE scheme is not flexible enough in revoking attribute. In ABE, revoking attribute is essentially revoking the decryption privilege on some files from one or more users, which also refers to changing access policy in nature.

Table 4
Performance comparisons with KP-ABE schemes.

Scheme	Cipher-text size (bit)	Public key size (bit)	Private key size (bit)	Computation overhead (PS)	Assumption
Our scheme	$(2k+2)l$	$(2n+2)l$	$k \cdot l$	$3k$	ECDDH
[11]	$(k+2)6.4l$	$(n+2)6.4l$	$6.4k \cdot l$	$42k$	DBDH
[15]	$32l$	$19.2kl$	$25.6l$	$24k+24$	DBDHE
[16]	$25.6l$	$(n+4)6.4l$	$(n+2)6.4k \cdot l$	$40k+24$	GDDHE
[20]	$(k+3)6.4l$	$(n+2)6.4l$	$19.2k \cdot l$	$6k+62$	DBDH

k is the size of the attributes set, n is the size of the attributes space;
DBDH is the abbreviation of Decisional Bilinear Diffie–Hellman;
DBDHE is the abbreviation of Decisional Bilinear Diffie–Hellman Exponent;
GDDHE is the abbreviation of General Decisional Diffie–Hellman Exponent.

Table 5
Performance comparisons with CP-ABE schemes.

Scheme	Cipher-text size	Public key size	Private key size	Computation overhead	Assumption
Our scheme	$(2k+2)l$	$(2n+2)l$	$k \cdot l$	$3k$	ECDDH
[12]	$(2k+3)6.4l$	$25.6l$	$(2k+1)6.4l$	$44k+2$	DBDH
[14]	$(2k+3)6.4l$	$(n+3)6.4l$	$(k+2)6.4l$	$66k+62$	q parallel-BDHE
[17]	$25.6l$	$38.4nl$	$(k+1)6.4l$	$20k+104$	n-BDHE
[24]	$(2k+3)6.4l$	$(n+3)6.4l$	$(k+2)6.4l$	$66k+62$	n-eDDH

q parallel-BDHE is the abbreviation of the decisional q-parallel Bilinear Diffie–Hellman Exponent;
n-BDHE is the abbreviation of the decision n-Bilinear Diffie–Hellman Exponent;
n-eDDH is the abbreviation of n-Extended Decisional Diffie–Hellman Assumption.

In the proposed ABE scheme, the monotone access structure and secret sharing mechanism are used to describe and generate the key respectively. The "and" and "or" operations are all made on attributes, which make its access policy expressed relatively flexibly, but the negative operation is not available, which makes it difficult in expressing a complicated access policy and revoking privilege directly.

Since it is prerequisite to avoid the impact on the other user's privileges and attributes while revoking an attribute or access privilege from a user, it is difficult to complete it. At present, it usually achieved by re-encryption or proxy re-encryption at the cost of high overhead. In this paper, revoking attribute is not discussed. Designing a lightweight flexible attribute revoking scheme is our future work.

(2) Poor Scalability.

In a ABE scheme, scalability refers to the impact of the encryption attributes number on efficiency. For the proposed scheme, both the communication overhead and the computational overhead are linear with the number of attributes, which can be seen from Tables 4 and 5 clearly. It indicates that its scalability is not good enough. Presently, poor scalability is a common problem in front of most ABE schemes.

(3) Poor Generality.

Here, generality refers to application scope. Currently, the applications based on IoT can be found everywhere, and IoT can be further classified into Unit IoT and Ubiquitous IoT two categories according to the number of the involved applications or domains [6]. The unit IoT only is always involved in a single application, and only one authority is needed in the domain. The Ubiquitous IoT refers to cross domain applications, which is usually involved in interrelated local, national and industrial IoTs. Since one authority is needed in one domain, multiple authorities are necessary and prerequisite in cross domain applications. With the popularization of unit IoT, Ubiquitous IoT is becoming more and more popular. Unfortunately, the proposed ABE scheme is designed just for single-authority applications, and not applicable to multi-authority applications. Improving its generality or developing lightweight multi-authority oriented ABE scheme on basis of it is very necessary.

7. Conclusion

In this work, a lightweight no-pairing ECC-based ABE scheme is proposed for the resources-constraint Unit IoT based applications to address secure communication and cipher-text access control. By taking the lightweight advantages of ECC and the primitive syntax of KP-ABE, both lightweight and ABE are achieved in the proposed scheme. Its security depends on the ECDDH problem instead of a generic group with bilinear pairing, and is proved in the attribute-based selective-set model. The comparison analyses on the existing KP-ABE schemes and CP-ABE schemes are made to indicate that the proposed scheme is a lightweight one, which does not only have low communication overhead but also have low computational overhead. In addition, its limitations in flexibility, scalability and multi-authority applications are also discussed in detail. To sum up, the proposed scheme is a lightweight KP-ABE scheme and very suitable for resource-constraint Unit IoT.

Acknowledgments

The work was partly supported by Chinese National Scholarship Fund (2011646515) and National Natural Science Foundation of China under Grant No. 61471035. It was jointly funded by DNSLAB (2014-145), China Internet Network Information Center, Beijing 100190, China.

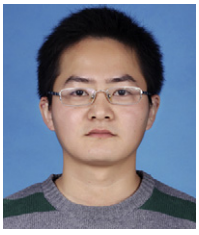
References

[1] J. Gubbia, R. Buyyab, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (2013) 1645–1660.
[2] M. Yun, B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, in: Advances in Energy Engineering, ICAEE, 2010, pp. 69–72.
[3] S.T. Ali, V. Sivaraman, D. Ostry, Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring, Future Gener. Comput. Syst. 35 (2014) 80–90.
[4] N. Dlodlo, Adopting the Internet of Things technologies in environmental management in South Africa.2012, in: Proc. International Conference on Environment Science and Engineering, Singapore, vol. 3, 2012, pp. 45–55.
[5] D. Bandyopadhyay, J. Sen, Internet of Things: applications and challenges in technology and standardization, Wirel. Pers. Commun. 58 (1) (2011) 49–69.
[6] H. Ning, H. Liu, Cyberentity security in the Internet of Things computer, IEEE Comput. Soc. 46 (4) (2013) 46–53.
[7] R. Roman, P. Najera, J. Lpoez, Secure the Internet of Thing, IEEE Comput. 44 (9) (2011) 51–58.
[8] H. Ning, H. Liu, L.T. Yang, Aggregated-proof based hierarchical authentication scheme for the Internet of Things, IEEE Trans. Parallel Distrib. Syst. (99) (2014) 1–11.
[9] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Advances in Cryptology-EUROCRYPT 2005, in: LNCS, vol. 3494, Springer-Verlag, Aarhus, Denmark, Berlin, 2005, pp. 457–473.

[10] A. Fiat, M. Naor, Broadcast encryption, in: Advances in Cryptology-Crypto93, in: Lecture Notes in Computer Science, vol. 773, 1994, pp. 480–491.
[11] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS'06, ACM, New York, NY, USA, 2006, pp. 89–98.
[12] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP'07, IEEE Computer Society, Washington, DC, USA, 2007, pp. 321–334.
[13] R. Ostrovsky, A. Sahai, B. Waters, Attribute-based encryption with nonmonotonic access structures, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195–203.
[14] B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in: D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi (Eds.), PKC 2011, in: LNCS, vol. 6571, Springer, Heidelberg, 2011, pp. 53–70.
[15] N. Attrapadung, B. Liber, E. de Panafieu, Expressive key-policy attribute-based encryption with constant-size ciphertexts, in: PKC 2011, in: LNCS, vol. 6571, 2011, pp. 90–108.
[16] C. Wang, J. Luo, A key-policy attribute-based encryption scheme with constant size ciphertext. in: 2012 Eighth International Conference on Computational Intelligence and Security, pp. 447–451.
[17] C. Chen, Z. Zhang, D. Feng, Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost, in: X. Boyen, X. Chen (Eds.), ProvSec 2011, in: LNCS, vol. 6980, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 84–101.
[18] P. Junod, A. Karlov, An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies, in: DRM'10, Chicago, Illinois, USA, October 4, 2010.
[19] D. Lubicz, T. Sirvent, Attribute-based broadcast encryption scheme made efficient, in: Progress in Cryptology-AFRICACRYPT 2008, in: LNCS, vol. 5023, Springer-Verlag, Berlin, 2008, pp. 325–342.
[20] S. Hohenberger, B. Waters, Attribute-based encryption with fast decryption, in: Public-Key Cryptography—PKC 2013, in: Lecture Notes in Computer Science, vol. 7778, 2013, pp. 162–179.
[21] M. Chase, Multi-authority attribute based encryption, in: Theory of Cryptography, Springer, 2007, pp. 515–534.
[22] D. McGrew, K. Igoe, M. Salter, Fundamental elliptic curve cryptography algorithms, Internet Engineering Task Force (IETF), Request for Comments: 6090, February 2011. http://tools.ietf.org/html/draft-mcgrew-fundamental-ecc-04.
[23] V.G. Martínez, L.H. Encinas, C.S. Ávila, A survey of the elliptic curve integrated encryption scheme, J. Comput. Sci. Eng. 2 (2) (2010) 7–13.
[24] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption, in: Advances in Cryptology-EUROCRYPT 2010, in: LNCS, vol. 6110, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 62–91.

Xuanxia Yao received her B.S. degree in Computer Application from Jiangsu University, M.S. and Ph.D. degree in Computer Application from University of Science and Technology Beijing (USTB), China, in 2002 and 2009. She is a member of CCF (China Computer Federation).

From 1994 to 1999, she was a research assistant with the computer center in Luoyang Mining Machinery Institute of Technology. Since 2009, she has been an associate professor with School of Computer and Communication Engineering, USTB. She is the author of one book, more than 20 articles. Her research interests include network security, Internet of Things and cloud computing.



Zhi Chen received his B.S. degree in Electronic and Information Engineering from Xinyang Normal University in 2009. Now he is a Master candidate in School of Computer & Communication Engineering, University of Science & Technology Beijing. His research interests include intelligent medical, network security and privacy protection.

Ye Tian received his B.S. degree in Computer Communication from Chongqing University of Posts and Telecommunications, Ph.D. degree in Computer Architecture from Institute of Computing Technology Chinese Academy of Sciences, China, in 2001 and 2006. He is a senior member of CCF (China Computer Federation).

From 2006 to 2009, he was an Associate Professor in NEC Labs China. Since 2009, he has been an Associate Professor in Computer Network Information Center, Chinese Academy of Sciences, China. His research interests include Internet of Things, the next generation network, and network security.