

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/334164705>

Meddah N., Jebrane A., Toumanari A. (2018) Scalable Lightweight ABAC Scheme for Secure Sharing PHR in Cloud Computing.

Article in Lecture Notes in Computer Science · July 2019

CITATIONS

2

READS

157

1 author:



Meddah Naima

national school of applied science, agadir, morocco

11 PUBLICATIONS 28 CITATIONS

SEE PROFILE

Scalable lightweight ABAC scheme for secure sharing PHR in cloud computing

Naima Meddah¹ and Asma Jebrane² Ahmed Toumanari¹

¹ National School of Applied Sciences, ENSA, Laboratory of engineering, sciences and technology information, LISTI Ibno ZOHR University, 80000 Agadir, Morocco.

² LETSMP, Faculty of sciences of Ibn Zohr 80000 Agadir, Morocco

Abstract. Data access control is of critical importance in cloud computing, in particular for e-health systems, where a patient Personal Health Records (PHR) data, have a serious privacy concerns about outsourcing to the cloud servers. Presently Key policy attribute based encryption (KP-ABE) is promising advanced cryptographic system for fine-grained access control in cloud computing systems. Yet, Existing access control schemes based on attribute based encryption (ABE), are no longer applicable due to the heavy cryptographic computation and communication overhead of key management. Existing ABE schemes are based on expensive bilinear pairing that make its not scalable and not suitable for cloud e-health systems. In this paper we propose a new Scalable lightweight LKP-ABE scheme based on elliptic curve integrated encryption scheme (ECIES), The best known encryption scheme based on Elliptic Curve Cryptography, applied in e-health system, in order to ensure fine grained access control and data confidentiality of personal health records, and present an advanced secure and scalable encryption/decryption system based on Key Policy Attribute Based Encryption (KP-ABE) for PHR's. Our scheme provide semantic security against chosen cipher-text attacks (CCAs), guaranteed resistance collusion and provide high level data confidentiality of sharing PHR, by using elliptic curve integrated encryption scheme (ECIES) that has much stronger bit security than RSA as well as other exponential-based public key algorithm and the advanced attribute based encryption KP-ABE. The proof security, performance comparison among LKP-ABE and related schemes is given to prove the performance, low cost communication and execution efficiency of LKP-ABE.

Keywords : cloud computing, access control, attribute based encryption (ABE), Personal health records (PHR), Elliptic Curve Cryptography (ECC), ECIES, Chosen Cipher-text Attacks (CCAs).

1 Introduction

The term of personal health record (PHR) has undergone substantial changes along with the emergence of cloud computing. The ultimate goals of e-health system's is to deliver best possible health services by using Body Sensor Network (BSN)[1]. The body sensor network has brought forth to the advancement of today's medical industry, called as e-health systems [2]. Many research works have been carried out to counteract the security issues in personal health records and ensure fine-grained access control for PHR's [3][4][5][6]. Cloud computing is an emerging paradigm that

provide technology and computer resources as a service, which has potential to bring great benefits to information and communication technology (ICT) for companies, organizations and even countries [7]. Promising as it is, this paradigm also brings forth new challenges issues for data security and privacy when users outsource sensitive data for sharing on cloud servers. Due to cloud storage services requirement, fine-grained access control is needed to provide users permission management when dealing with complex users hierarchy and large amount of data [8]. beside access control challenge in cloud-based services, we face another challenge, which is the surge in attacks such as chosen cipher-text attacks (CCAs). Then the confidentiality of the data becomes a problem. At present, encryption is the primary mechanism to implement data protection [14]. However, traditional encryption schemes are not suitable in such a situation for their lack of ability in access control and huge overhead of key management. Aiming at providing fine-grained access control over encrypted data, Sahai and Waters (2005) made some initial steps to solving this problem by introducing the concept of attributed-based encryption (ABE) [9]. In KP-ABE scheme there is an authority that is responsible for attribute management and key distribution [6]. The authority can be social security administration, the health service provider (HSP)...[2] the data owner encrypt the data under a set of attributes and each user defines the access policies, each user can decrypt the cipher-text if and only if its attributes satisfy the access policy. The feature of ABE that any user can decrypt the cipher-text as long as its meet the required attribute, which makes it very suitable for fine-grained access control. However it very difficult to implement the existing ABE schemes in cloud computing, because they are all based on the expensive bilinear pairing operation [10]. In order to ensure fine-grained access control based on ABE and keep data privacy and confidentiality in cloud computing by reducing communication overhead, a lightweight attribute based encryption is crucial. In this paper, considering the fact that ECC algorithm has much stronger bit security than RSA as well as exponential-based public key cryptography algorithm [11], we propose a first KP-ABE based on ECIES scheme, to address data privacy and security issues, and fine-grained access control in cloud e-health. The new KPL-ABE scheme based on no-pairing ECC, replaces the expensive bilinear pairing operation with point scalar multiplication on elliptic curve, it can address the lightweight attribute access control in cloud Computing e-health systems. The main contributions in this work is summarized as follow:

- To the best of our knowledge, the first lightweight LKP-ABE based on ECIES that can be applied in cloud e-health, is proposed to ensure fine-grained access control, data privacy and privacy issues for PHR's in cloud e-health.
- The proposed scheme ensure security semantic against CCAs (Chosen Cipher-Text Attacks) and CCP (Chosen Plain-Text Attacks).
- The security proof is performed in attribute based selective-set model.
- The new LKP-ABE scheme's security depends on the ECDDH (Elliptic Curve Decisional Diffie-Hellman) problem instead of bilinear Diffie-Hellman assumption, which can diminish the computation and communication overhead.

- The lightweight feature is proved by comparing it with the existing ABE schemes, which indicate that can be applied in cloud e-health.

The rest of this paper is organized as follows: In section 2, we examine the related works on attribute based access control in Cloud computing. In section 3 we give the necessary technique preliminaries pertaining to our proposed scheme. Section 4 we present the description of the LKP-ABE scheme for cloud computing. The security proof is made in section 5, and the performance analysis is discussed in section 6. Finally draws a conclusion.

2 Related Work

This paper is primarily related to works in cryptographically ensuring fine-grained access control for outsourced data and attribute based encryption. Attribute based encryption (ABE) is a promising technique that designed for fine-grained access control for encrypted data. The notion of attribute based encryption was first introduced by sahai and waters [12]. It's an extension of Identity-based Encryption (IBE), which can ensure fuzzy identity by combining the user's identity with a series of attributes and achieve data preserving [1][13]. The ABE based access control has attracted many researchers attention and a myriad of data access control based on ABE [7][10][15][16][17], have been proposed to construct a secure fine-grained access control and data privacy in semi-trusted cloud computing. Yet, based on the Delov-Yao model [18], security goals such as chosen cipher-text attacks (CCAs) resistance, data confidentiality and low cost overhead computation and execution efficiently, of the most solution designs are not perfectly guaranteed. Furthermore to face challenges in expressive access control policy, many variant of access control based on ABE have been proposed to achieve an expressive access control by constructing constant size cipher-text [6][10][15][19] to limit the size of the cipher-text. Though some achievements have been made at the expense of increasing overheads, they do not meet the lightweight requirement of Cloud Computing yet. The research community is mostly focused on the design of fine-grained access control for encrypted data which can applicable and suitable for cloud environments without trying to minimize the high computational complexity of attribute based encryption systems [20]. Our contribution is to construct a new lightweight LKP-ABE based on ECC, for fine-grained access control with chosen cipher-text security and resistance collusion with minimal cryptographic computation that can be applied in cloud e-health systems.

3 Preliminaries

Our scheme is based on elliptic curve cryptosystem and its related primitives, key-policy attribute based encryption, secret sharing shamir scheme SSSS [9] and access structure in ABE. The main notation used in our paper are summarize in Table.1.

Table 1. Notations used in our paper

Notation	Notations Meaning
q	A large prime, the finite field with p elements F_p
$\mathbb{E}$	An elliptic curve over the finite field F_p , of large prime order q
q	A large prime, used to denote the order of G in $\mathbb{E}$ over F_p
$\mathbb{Z}_q$	A finite integer field, whose elements set is $\{0, 1, \dots, q - 1\}$
G	A base point on the elliptic curve $\mathbb{E}$
$\mathbb{G}_E$	A subgroup of $\mathbb{E}$ with the order of q
O	The zero element of an elliptic curve group
$MAC()$	Message Authentication Code
$Hash()$	A hash function, used within the KDF and the MAC functions
MSK	The master private key of the ABE scheme
MPK	The master public key of the ABE scheme
τ	The access policy
$PPrm$	The public parameters of the ABE scheme
ENC	A symmetric encryption algorithm, using KDF
DEC	A symmetric decryption algorithm
k	The number of the attributes used to encrypt data
n	The number of the attributes in a system
P_S	One point scalar multiplication

3.1 Elliptic Curve Cryptography

Elliptic curve cryptographic ECC schemes are public-key mechanisms that provide encryption, digital signature and key exchange capabilities, it was introduced in 1985 by Victor Miller and Neal Koblitz [11], whose security relies on the elliptic curve discrete logarithm problem (ECDLP) problem. 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 . $\mathbb{Z}_p$ is a prime Galois Field F_p , and an Elliptic curve over $\mathbb{Z}_p$ is defined by a cubic equation $y^2 = x^3 + a.x + b$ and can be described by a set of parameters (q, a, b, G, p) , where $(a, b) \in \mathbb{Z}_p$, and $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. 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 [11][20]. ECC security is based on ECDH and actually no algorithm is known that solves the ECDLP in an efficient way. Moreover, the ECDLP is regarded as the

hardest of these three problems. From this fact derives one of the most important benefits of ECC: the key size. Keys in ECC are significantly shorter than in other cryptosystems such as RSA [11]. A shorter key implies easier data management, lower hardware requirements (in terms of buffers, memory, data storage, etc.), less bandwidth when transmitting the keys over a network [11][21].

3.2 Elliptic Curve Integrated Encryption Scheme

The most extended encryption and decryption scheme based on ECC is the Elliptic Curve Integrated Encryption Scheme (ECIES) [11]. This scheme is used to ensure data confidentiality and data integrity for each users, which uses the following functions [11]:

- Key Agreement (KA): Function used for the generation of a shared secret by two parties.
- Key Derivation Function (KDF): Mechanism that produces a set of keys from keying material and some optional parameters.
- Encryption (ENC): Symmetric encryption algorithm.
- Message Authentication Code (MAC): Data used in order to authenticate messages.
- Hash (HASH): Digest function, used within the KDF and the MAC functions.

The encryption and decryption algorithm of ECIES is described in Fig.1 and Fig.2.

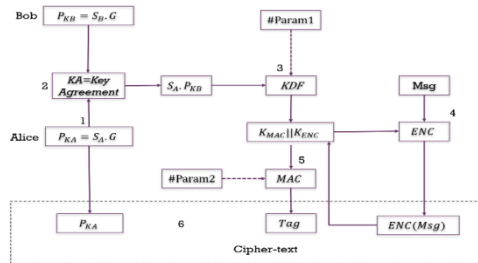


Fig. 1. ECIES encryption diagram

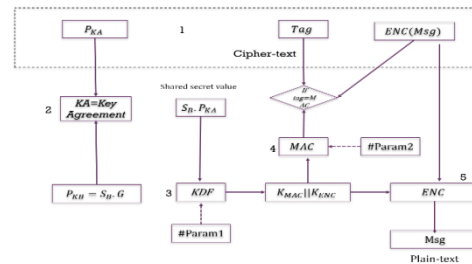


Fig. 2. ECIES decryption diagram

3.3 Access Structure

The access structure defines the access policy in the attribute based encryption scheme the access structure can be defined as definition 1[17].

Definition.1 Let $\{P_1, P_2, \dots, P_n\}$ be a set of parties or attributes. A collection $\mathbb{A} = 2^{\{P_1, P_2, \dots, P_n\}}$ is a monotone if $\forall B, C : \text{if } B \in \mathbb{A} \text{ and } B \subseteq C \text{ then } C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, \dots, P_n\}$, i.e., $\mathbb{A} \subseteq$

$2^{\{P_1, P_2, \dots, P_n\}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.

3.4 Secret Sharing Scheme

The secret sharing refers to distributing a secret amongst a group of parties. The first secret sharing schemes were proposed by Shamir [8] who employs the fact that an n degree polynomial can be determined by $P(x)_n = \sum_{k=1}^n f(x)_k \cdot y_k$ in the case that $(n+1)$ points are given, where $f(x)$ is called Lagrange coefficient. Assume that there are $(n+1)$ points (x_i, y_i) for $i = \{0, \dots, (n-1)\}$, $f(x)_k$ can be computed by $f(x)_k = \prod_{j=0, j \neq k}^n \frac{x - x_j}{x_k - x_j}$. The method to construct the polynomial is called Lagrange interpolation, the polynomial $P(x)_n$ is called Lagrange interpolation polynomial. In order to share the secret a_0 among n parties and reconstruct it at least by r parties, a $(r-1)$ degree polynomial $P_{(r-1)}(x) = \sum_{i=0}^{r-1} a_i x_i$ should be defined, where, the coefficients $\{a_1, a_2, \dots, a_{(r-1)}\}$ 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 $P_{(r-1)}(x)$ can be reconstructed by Lagrange interpolation, and the secret a_0 can be accordingly determined [8].

4 Proposed Scheme

Our proposed lightweight ABE is KP-ABE single authority, which implies a single certificate authority that is responsible for key generation for attributes and key management. In this section, we describe the system architecture model, system overview and highlith, and algorithm of LKP-ABE.

4.1 Key-Policy Attribute Based Encryption scheme

KP-ABE encryption scheme is composed of the following four algorithms, namely, Setup, Encrypt, KeyGen, and Decrypt [22].

- **Setup** : The Setup algorithm is a randomized algorithm, which is run by the CA and outputs the master public key MPK and the master secret key MSK. The master public key and set of parameters are published and the master key secret is kept secret by the certificate authority. Also CA define the attribute universe.
- **Encrypt (M, μ , MPK)**: 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 μ that the data user should satisfy, and the master public key MPK as input.
- **KeyGen (τ , MSK)**: The Key-Generation algorithm is a randomized algorithm too, which is run by the CA and takes an access structure τ and the master secret key MK as input. It outputs the decryption key D corresponding to the access structure.

- **Decrypt (CT, D, MPK):** The Decrypt algorithm is run by the receiver, which takes the cipher-text CT encrypted under the attributes set μ , the decryption key D for access control structure τ , along with the master public key MPK as input. If $\tau(\mu) = 1$, it decrypt the cipher-text CT and outputs message M.

4.2 System Model

Our system model is defined as following:

Health Care Staffs (HCS) : are the data users in e-Health system. Each data user has a set of attributes, such as affiliation, department and type of health-care staff, and is authorized to search on encrypted PHRs based on his set of attributes or access policy.

CA : Certificate authority which is the fully trusted authority in the system. It sets up the system by defining the attribute universe and validate the registration of all users and HCS's. For each registered user in the system, the CA assigns a global unique identity and generates a pair master secret key MSK and master public key MPK and also a set of public parameters PPrm.

Data owner (Patient): define the access policy τ , and encrypt data under the access policy and upload the cipher-text to the cloud servers if he use the CP-ABE, or he use the set of attribute to encrypt her vitals signs by using KP-ABE.

CSP : Cloud Service Provider , cloud servers store the patient's data (PHR) and provide access service to users by contacting CA and validate the global unique identity of all user issuing by CA.

Health insurance and Health –care are added to complete the whole system, and ensure the general communication and sharing the patient PHR's between the different parties of e-health systems.

The diagram illustrates the proposed secure PHR sharing scheme, involving the following components and steps:

- Components:** Patient, CA (Cloud), Health Care Staff, Health Insurance, and Central Hospital.
- Steps:**
 - Request register:** The Patient sends a request to the CA.
 - Guidance:** The CA sends guidance information (PK_{AC}, MK_{AC}, SPR) to the Patient.
 - Upload cipher-text:** The Patient uploads the cipher-text to the cloud server.
 - Request register:** The Health Care Staff sends a request to the CA.
 - Gold SK/Access policy:** The CA sends the Gold SK/Access policy to the Health Care Staff.
 - Download encrypted PHR:** The Health Care Staff downloads the encrypted PHR from the cloud server.
 - Upload encrypted PHR:** The Health Care Staff uploads the encrypted PHR to the Health Insurance.
 - Sharing encrypted PHR:** The Health Insurance shares the encrypted PHR with the Central Hospital.
 - Decryption:** The Central Hospital decrypts the PHR data using the LCP-ABE key.
 - Decrypted PHR Data:** The Central Hospital sends the decrypted PHR data back to the Health Insurance.
 - Decrypted PHR Data:** The Health Insurance sends the decrypted PHR data back to the Health Care Staff.
 - Decrypted PHR Data:** The Health Care Staff sends the decrypted PHR data back to the Patient.

Encryption : Here we have two possibilities, we can encrypt the message M by using the lightweight KP-ABE, or we can use ECIES to encrypt the message M , and use the LKP-ABE to encrypt the secret sharing.

For more lightness and more security we use the method 2.

The owner use ECIEC to encrypt the Message M , see the **fig.1**

Encrypt the secret sharing by LKP-ABE, following the steps:

Specify the set of attributes μ

Choose a random $k \in \mathbb{Z}_q^*$ and compute $C_i = k \cdot PK_i / PK_i$: public key for each attribute, $i \in \mu$

For $k \in \mathbb{Z}_q^*$ compute $C' = k \cdot MPK$

Use KDF function we have $C' = k \cdot MPK = (K_x, K_y)$

Let K_x be the encryption key and K_y the integrity key for the message, here we have M =secret sharing

$C_{SP} = ENC(SP, K_x)$, $MAC_{SP} = Hash(SP, K_y)$.

Output $CT_{SP/KP-ABE} = (\mu, C_{SP}, MAC_{SP}, C_i, i \in \mu)$ (1)

Finally output the cipher-text $CT_{LKP-ABE}$ $CT_{LKP-ABE} = (CM_{ECIES}, CT_{SP/KP-ABE})$
 $CT_{LKP-ABE} = (CM_{ECIES}, \mu, C_{SP}, MAC_{SP}, C_i, i \in \mu)$ (2)

Key-Generation (τ , MSK): This algorithm is used by the certificate authority to generate the decryption key of message under set of attribute μ if and only if $\mathcal{G}(\mu)=1$. This algorithm output a private key (decryption key) embedded with an access structure τ . The decryption key must satisfy $\tau(\mu) = 1$. For this purpose we should define an access structure by following steps:

Each non-leaf node is defined as a Shamir Threshold Scheme. Set the degree of secret polynomial $P_u(x)$ to be $d_u = k_u - 1$.

For root node r , set $P_r(0) = s$. And randomly choose d_r element in $\mathbb{Z}_q^*$ to completely define P_r . For any other non-leaf node u , set its secret to be one secret share of its parent node, that is $P_u(0) = P_{parent(u)}(index(u))$. And randomly choose d_u element in $\mathbb{Z}_q^*$ to completely define P_u .

- For each leaf node u , assign the following value $D_u = P_u(0)/r_i, i = attrib(u), r_i \in \mathbb{Z}_q^*$ is randomly chosen in CA-Setup. The decryption key can denoted by $D = \{\tau, D_u = P_u(0)/r_i, i = attrib(u), i \in \mu\}$.

Decryption-Alg : To decrypt the Message, we first begin by decrypting the secret sharing encrypted under LKP-ABE, and use the secret sharing to decrypt the cipher-text under ECIES. Decrypt $CT_{SP/LKP-ABE}$ Similar to all ABE schemes:

- For each non-leaf node u , all nodes v , are children of u . Let μ_u be an arbitrary d_u – sized set of child nodes u such that $\text{DecryptNode}\{CT_{SP/LKP-ABE}, D, u\} \neq \perp$, if there is not such a μ_u , $\text{DecryptNode}\{CT_{SP/LKP-ABE}, D, u\} = \perp$, in other, $\text{DecryptNode}(CT_{SP/LKP-ABE}, D, u) = \sum_{v \in \mu_u} (\Delta_{i,u'}(0)) \cdot \text{DecryptNode}(CT_{SP/LKP-ABE}, D, v)$ where $i = \text{index}(v)$, $U'_u = \text{index}(v)$, $v \in U_u$
 $\text{DecryptNode}(CT_{SP/LKP-ABE}, D, u) = \sum_{v \in \mu_u} (\Delta_{i,u'}(0)) \cdot P_u(0) \cdot k \cdot G$
 $\text{DecryptNode}(CT_{SP/LKP-ABE}, D, u) = \sum_{v \in \mu_u} (\Delta_{i,u'}(0)) \cdot P_{\text{parent}(v)}(\text{index}(v)) \cdot k \cdot G$
 $\text{DecryptNode}(CT_{SP/LKP-ABE}, D, u) = \sum_{v \in \mu_u} (\Delta_{i,u'}(0)) \cdot P_u(i) \cdot k \cdot G$
 $\text{DecryptNode}(CT_{SP/LKP-ABE}, D, u) = P_u(0) \cdot k \cdot G$

Consequently, for the root node R of access tree, there should be $\text{DecryptNode}(CT_{SP/LKP-ABE}, D, r) = P_r(0) \cdot k \cdot G = r \cdot k \cdot G = (K'_x, K'_y)$. Here, K_x is considered to be the decryption key for the message CT and K_y is the integrity key for the message. The encrypted Message M' can be decrypted by $M' = \text{DEC}(C, K'_x)$. if $\text{Hash}(M', K'_y) = \text{MAC}(M)$, 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 $\text{MAC}(M)$.

- for a leaf node u ,

$$\text{DecryptNode}(CT_{SP/LKP-ABE}, D, u) = \begin{cases} D_u \cdot C_i \cdot r_i^{-1} \cdot P_i \\ P_u(0) \cdot r_i^{-1} \cdot k \cdot r_i \cdot G \\ P_u(0) \cdot k \cdot G \quad (i \in u) \\ \perp \quad \text{Otherwise} \end{cases}$$

N.B: the output of $\text{DecryptNode}(CT_{SP/LKP-ABE}, D, u)$ is an element in elliptic curve group $\mathbb{G}_E$ or

Decrypt CM_{ECIES} : after decrypting the $CT_{SP/LKP-ABE}$, the user can use the secret sharing to decrypt the cipher-text by using ECIES.

5 Security analysis

5.1 Security model

The selective-Set Security game for a KP-ABE scheme as defined in [9] is used to prove the security of all ABE scheme's CP-ABE/KP-ABE. Key Policy Attribute-based Encryption game captures the indistinguishability of messages under Chosen Plain-text Attacks and the collision resistance of user secret keys, namely, the attackers cannot generate a new secret key by combining their secret keys. To capture

the collision-resistance, the multiple secret key queries can be issued by an adversary A after the challenge phase. the game is described as indicated [9].

5.2 Security analysis of LKP-ABE

The formal security analysis of LKP-ABE, is given to prove that our LKP-ABE can achieve, security Chosen Cipher-text Attacks (CCAs), Chosen Plain-text Attacks (CPAs), Data confidentiality under attribute security selective-set model with minimal cryptographic computation.

Theorem.1 *The LKP-ABE scheme is secure under attribute selective security model. If there is an adversary who breaks our scheme in selective-set security model in polynomial-time, a simulator Λ can be constructed to solve the ECDDH problem with a non-negligible advantage.*

Suppose we have an adversary A with non-negligible advantage $\xi/2$ in the selective security game, a simulator Λ can be constructed to gain the ECDDH game with advantage $\xi/2$. The constructed simulator is described as indicated in [20]

Init The simulator Λ get the attributes set Φ , which is the adversary Θ wishing to attack upon. It is assumed that the access structure corresponding to the attributes set Θ is Γ Setup The simulator Λ runs the Setup algorithm of the proposed scheme to set the system public key parameters and sends them to the adversary Θ . According to the DDHA, Λ sets the system parameter $Y = A = c \cdot G$, and sets $Y_i, \forall i \in U$ and, $c \in \mathbb{Z}_q$:

If $i \in \Theta$, Λ randomly chooses $s_i \in \mathbb{Z}_q$ and sets $Y_i = s_i \cdot G$ and $Y_i = s_i$.

If $i \in (U - \Theta)$, Λ randomly chooses $\rho_i \in \mathbb{Z}_q$, and sets $Y_i = \rho_i \cdot B = d \cdot \rho_i \cdot G$ and $Y_i = d \cdot \rho_i$

The simulator sends the system public key parameters $Y, Y_i, i \in U$ to Θ . It is obvious that Y, Y_i corresponds to PK, P_i of the proposed LKP-ABE scheme.

Phase 1 The adversary Θ can make many queries for the decryption key corresponding to any access structure γ , where the challenge set ρ does not satisfy γ , that is $\gamma(\rho) = 0$. The simulator Λ needs to assign a polynomial P_u with degree of d_u to every node u in the access tree Γ . The polynomial P_u for each node u in Γ is defined as $P_u(x)$ to be $p_u(x)$ in the proposed scheme. The shared secret is set to be the constant of the root's polynomial, that is $P_u(0) = c$. The secret key corresponding to each leaf node x in Γ is given by its polynomial as follows:

$$D_x = P_x(0)/s_i$$

$$D_x = \begin{cases} \frac{p_x(0)}{r_i}, & \text{if } (attr(x) \in \theta) \\ \frac{p_x(0)}{\delta_i \cdot d} & \text{if } (attr(x) \notin \theta) \end{cases} \quad \text{for } i = attr(x).$$

The secret key for access structure is $(D_x, x \in \Gamma)$, which is distributed to the adversary.

Challenge: like the challenge steps in Selective-set game of ABE [17], the adversary will submit two challenge messages M_0 and M_1 the simulator Λ , who flips a fair binary coin u , and compute the cipher-text M_u . To encrypt the message M_0 , in order to encrypt the message M_u the simulator execute the Encryption algorithm as indicated in section 4.3. The cipher-text is $CT(\rho, C, MACMu_0, C_i, i \in \rho)$ and sent to the adversary. more details in [18]

Phase 2 : Both of the simulator and adversary Execute precisely as they did in phase 1. prediction : the

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

Chosen Cipher-text Attacks Security

Elliptic Curve Integrated Encryption Standard (ECIES), provides semantic security against an adversary who's allowed to use "chosen plain-text attack CPA" and "chosen cipher-text attacks CCA.

Theorem.2 : *ECIES is secure against CCA adversaries.*

Proof. Indeed, let A be an adversary that computes the Diffie-Hellman function after n queries to an ECDDH oracle, with probability ξ . Then from any $\rho - ECDDH$ oracle we can build a $\rho' - ECDDH$ oracle, achieving $\rho' \leq \xi/2$. Therefore, if one simulates the perfect oracle, called by Adversary, using this $\rho - ECDDH$ simulator, then A succeeds in solving the computational Diffie-Hellman problem with probability $(\xi - n)\rho' \geq \xi/2$. Still, even if bot problems are polynomially equivalent, the computational cost of the above reduction may be huge, depending on the original value of ρ . [21]

6 Performance comparison of our scheme

in this section, we compare the performance of our LKP-ABE scheme with the related existing schemes. All the existing ABE scheme are based on bilinear pairing group $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Since the basic operation of $\mathbb{G}_1$ and $\mathbb{G}_2$ are modular exponentiation similar to RSA system, which make the ABE scheme based on bilinear pairing group very complex with high computational overhead of encryption and decryption key. According to the survey of ECC algorithm in [11], we have 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 our LKP-ABE scheme. based on above assumption, let δ_1 be the security level, the size of a point on elliptic curve of the 160-bit is $2\delta_1$, the size of its private key is δ_1 and the size of its public key is $2\delta_1$. Accordingly, both the public and private

key size of the 1024-bit RSA are $6,4\delta_1$, and the size of an element in $\mathbb{G}_1$ of a RSA based ABE scheme is $6,4\delta_1$ and the size of element in $\mathbb{G}_2$ of it is $12,8\delta_1$ [20]. In our LKP-ABE scheme for securing and sharing PHR we have:

the cipher-text $CT_{LKP-ABE} = (CM_{ECIES}, \mu, C_{SP}, MAC_{SP}, C_i, i \in \mu)$, compute the length of $CM_{ECIES}, \mu, C_{SP}, MAC_{SP}, C_i, i \in \mu$:

$$C_i = k \cdot P \cdot K_i, i \in \mathbb{E}, C_i \in \mathbb{E} \Rightarrow \text{length}(C_i) = 2\delta_1$$

$$\text{length}(C_{SP}) = \delta_1 + \delta_1 + k \cdot 2\delta_1 \Rightarrow \text{length}(C_{SP}) = \delta_1(2k + \delta_1)$$

$$\text{length}(MPK, P_{k_1}, P_{k_2}, P_{k_3}, \dots, P_{k_U}), U: \text{universofattribtes}, P_{k_i} \in \mathbb{E} \Rightarrow \text{length}(P_{k_i}) = 2\delta_1 \Rightarrow \text{length}(PPrm) = (2n + 1)\delta_1$$

$$\text{length of decryption key}, D = \gamma, D_u = P_u(0)/r_i, i = \text{attrib}(u), i \in \mu, \text{ where } \gamma \text{ is an access structure and } u \text{ is user attributes.} \Rightarrow \text{length}(D) = k \cdot \delta_1$$

The computational overhead is measured by the costs for bilinear mapping, the public key based encryption and decryption operation .in our LKP-ABE scheme no bilinear mapping is involved.The overhead and efficiency of the LKP-ABE scheme in cloud e-health is described in the graphs fig.4, fig.5 fig.6 and fig.7.

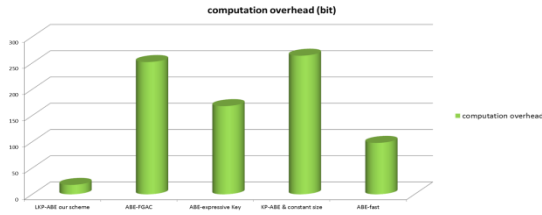


Fig.4. LKP-ABE computation overhead

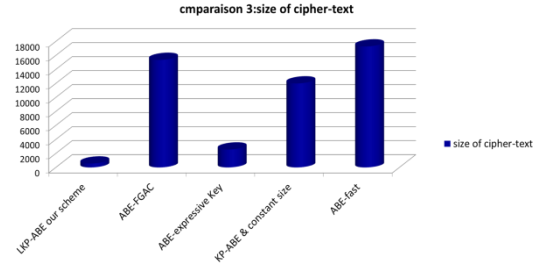


Fig.7. size of LKP-ABE cipher-text

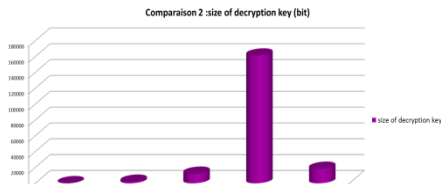


Fig.6. size of LKP-ABE decryption key

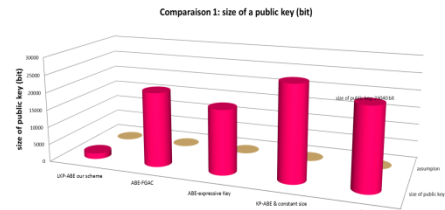


Fig.5. size of LKP-ABE Public key

7 Conclusion

In this work we proposed a new and effective lightweight data access control scheme for secure sharing personal health records PHR in cloud computing based on no-pairing attribute based encryption, which ensure fine-grained access control, Data

confidentiality and secure data transfer in cloud computing . As the best of our knowledge, Our scheme is more suitable and applicable in the cloud environment - because it provide low cost communication overhead and execution efficiency- than other attribute based access control scheme applied in e-health cloud computing. The proposed scheme provide semantic security against chosen cipher- text attacks (CCAs), and resistance collusion attacks security, by using a combination of elliptic curve integrated encryption scheme (ECIES) which has much stronger bit security than RSA as well as other exponential-based public key algorithm, and key policy attribute based encryption KP- ABE which is regarded as one of the most suitable technologies for fine-grained access control in cloud environments, because it gives the data user more direct control access policies. As indicated in section 7 the proposed scheme is lightweight KP-ABE for one trusted authority (CA) and very convenient for cloud computing e-health, our algorithm is highly scalable, secure and adapted to the cloud e-health system's and can be generalized for the multi-authority cloud e-health.

References

1. Li, Jin, Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma, et Wenjing Lou. Fine-grained access control system based on outsourced attribute-based encryption . In European Symposium on Research in Computer Security, 592609. Springer, 2013.
2. Kobrinskii, Boris A. E-Health and Telemedicine: Current State and Future Steps . E-Health Telecommunication Systems and Networks 03, n 04 (2014): 5056.
3. Li, Ming, Shucheng Yu, Kui Ren, et Wenjing Lou. Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. In SecureComm, 10:89106. Springer, 2010.
4. Li, Ming, Shucheng Yu, Yao Zheng, Kui Ren, et Wenjing Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption . IEEE transactions on parallel and distributed systems 24, n 1 (2013): 131143.
5. Tan, Yar-Ling, Bok-Min Goi, et Ryoichi Komiya. Real-Time/Store-and-Forward Telemedicine with Patients Data Protection by KP-ABE Encryption . In The International Conference on E-Technologies and Business on the Web (EBW2013), 7984. The Society of Digital Information and Wireless Communication, 2013.
6. Yang, Yang, Ximeng Liu, Robert H. Deng, et Yingjiu Li. Lightweight Sharable and Traceable Secure Mobile Health System . IEEE Transactions on Dependable and Secure Computing, 2017, 11.
7. Meddah, Naima, et Ahmed Toumanari. Reinforce cloud computing access control with key policy attribute-based anonymous proxy reencryption . International Journal of Cloud Computing 5, n 3 (2016): 187 197.
8. R. Rivest, Adi Shamir, (How to Share a Secret), Massachusetts Institute of Technology, Communications of the ACM, November 1979 Volume 22 Number 11.
9. Sahai, Amit, Brent Waters, et others. Fuzzy identity-based encryption. In Eurocrypt, 3494:457473. Springer, 2005.
10. Odelu, Vanga, Ashok Kumar Das, et Adrijit Goswami. An Efficient CP-ABE with Constant Size Secret Keys using ECC for Lightweight Devices. IACR Cryptology ePrint Archive 2015 (2015): 841.
11. Martnez, V. Gayoso, L. Hernandez Encinas, et C. Snchez vila. A survey of the elliptic curve integrated encryption scheme . ratio 80, n 1024 (2010): 160223.
12. J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP07, IEEE Computer Society, Washington, DC, USA, 2007, pp. 321334.

13. 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, SpringerVerlag, Berlin, Heidelberg, 2010, pp. 6291.
14. Sourabh singh, Young-sik Jeong, Jong Hyuk Park, A survey on cloud computing security: Issues, threats and solutions . In journal of Network and computer Applications, 200-222. Elsevier, 2016.
15. N. Attrapadung, B. Libert, E. de Panafieu, Expressive key-policy attribute-based encryption with constant-size ciphertexts, in: PKC 2011, in: LNCS, vol. 6571, 2011, pp. 90108.
16. Niloufer Rafath , Wahaj Ghouri , Syed Raziuddin Security in Cloud using Ciphertext Policy Attribute-Based Encryption with Checkability „International Journal of Innovative Research in Computer and Communication Engineering.Vol. 3, Issue 5, May 2015.
17. Zhen, Yao. Privacy-preserving personal health record system using attribute-based encryption . Worcester Polytechnic Institute, 2011.
18. Delov, D., Yao A. C, On the security of public key protocols, IEEE Trans. Information Theory , vol.IT-29, no.2, pp.98-208, 1983.
19. Vanga Odelu, Ashok Kumar Das, Y. Sreenivasa Rao, Saru Kumari, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment, Computer Standards and Interfaces (2016), doi: 10.1016/j.csi.2016.05.002.
20. Yao, Xuanxia, Zhi Chen, et Ye Tian. A Lightweight Attribute-Based Encryption Scheme for the Internet of Things . Future Generation Computer Systems 49 (aot 2015): 10412. Elsevier.
21. Muthurajan, Vinothkumar, et Balaji Narayanasamy. An Elliptic Curve Based Schnorr Cloud Security Model in Distributed Environment . The Scientific World Journal 2016 (2016): 18.
22. V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for finegrained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS06, ACM, New York, NY, USA, 2006, pp. 8998.