Journal of Network Computing and Applications (2016) 1: 33-41
Clausius Scientific Press, Canada

An Improved Encryption Scheme of Short Message Based On CP-ABE

Guangli Xiang*, Yuexin Zhang, Wenna Song

Wuhan University of Technology, Wuhan 410000, China
*glxiang@whut.edu.cn, 380119492@qq.com, 1013370271@qq.com

Keywords: CP-ABE; the short ciphertext; Ciphertext sharing of multi-users; the security model; distinguish ability chosen plaintext attacks

Abstract: In order to solve the problem of short message sharing in multi-user environment, we improve the existing CP-ABE encryption scheme, and propose a high efficient encryption scheme for short message protection. To improve the decryption efficiency, we reduce the number of bilinear operations to a fixed range in the decryption operation. And we use the security model which resists in distinguish ability chosen plaintext attacks in the CP-ABE encryption scheme to carry out a safety proof. Several experiments show that the encryption scheme performs with high efficiency and remains sufficient security.

1. Introduction

With the rapid development of Internet technology, WeChat, Microblog, QQ, BBS, news, and other short message applications have been widely used. At the same time, the storage of massive short message has become a problem which needs to be solved. With the popularity of cloud services and the increase of user's sharing requirements, massive short message has been stored by third parties, which meets the needs of sharing the ciphertext. However, most of the data in short message are sensitive, and if they are stored as plaintexts, it will cause a serious information disaster. In order to solve the security problem of short message storage in third parties, the technology of short message encryption has become the research focus of many scholars.

Liu Hui et al proposed a short message encryption scheme based on RSA public key encryption algorithm [1]. Fang Chuanwei et al proposed a scheme which used 3DES encryption technology to encrypt short message [2]. Sameer Hasan Al-bakri used AES and NTRU algorithm to encrypt short message[3]. Although encryption technology can effectively control the access of a short message, these ciphertexts are only suitable for single user, can't achieve ciphertext sharing requirements and lead to poor performance of short message applications in computing and storage consuming.

In order to meet needs of sharing the ciphertext, this paper proposed a short message encryption scheme based on attribute encryption. Attribute encryption [4] is an encryption algorithm based on access control, which allows to specify a number of users to access the short message. Its concept originates from the idea of identity encryption, and the secret key is refined to a series of attribute sets which can indicate the user's identity [5]. Waters et al proposed a secure and efficient CP-ABE scheme [6]. In this scheme, the access control structure and the ciphertext binding, the users' attribute set and the private key binding, when the user's attribute set satisfies the access control structure with the ciphertext binding, it can decrypt the ciphertext. CP-ABE is suitable for multiple users to share the same ciphertext [7], for example, cloud disk file. However, the computation of the

scheme is linear with the number of attributes, the efficiency is difficult to meet the real-time requirements of short message encryption and q-Bilinear Diffie-Hellman Exponent problem assumption is too strong to promote in practical applications. In this paper, we improve security assumptions in the existing Waters CP-ABE scheme, reduce the number of bilinear operations to a fixed range in the decryption operation, reduce the computational complexity of decryption and improve the decryption efficiency. Based on this scheme, we construct a short message expansion model and propose a short message encryption scheme to meet the needs the sharing of the ciphertext. The biggest innovation of this model is the topic information and category information of short message is embedded into the short message model. Topics and categories can restrict access of short message. We construct the access control structure of short message, according to the attribute information of the short text extended model, to realize the application of the attribute encryption scheme in short message encryption.

2. Short message Expansion Model

2.1 Model Description

Traditional basic model of Short message is as follows:

$$TM = \{T, S, R, m\}. \quad (1)$$

Consisted of short message creation time T, short message sender S, short message receiver R, short message content m [8].Through the basic model, we can clearly know the sender, receiver and transmission time of a short message. However, in the specific application, short message will also cover the other two information - topics and categories. If you do not limit the topics and categories of short message, the user may get a lot of different topics and categories of text when querying. To limit the topic and category of short message, this paper proposes a short message expansion model ETM:

$$ETM= \{T, S, R, m, Z, C\}. \quad (2)$$

Z represents the theme of short message.

C represents the category of short message.

By adding the theme and category of elements in the basic model of short message, you can make access control of the theme and category of short message, making the difference between the short messages more clear, and illustrating the user to quickly query the required text in the text.

2.2 Access control structure of short message

Short message encryption algorithm based on CP-ABE is taking descriptive identity information of the basic model as a property, and builds completed set of attributes $P=\{P_1, P_2, \ldots, P_n\}$. As the access user of short message content, visitors need to build attribute of short message which wanted. A represents the attribute information, is non-null subset of P, $A \subseteq \{P_1, P_2, \ldots, P_n\}$.

The access control structure of short message Γ is non-null subset of P, representing the judgment condition of a short message attribute set. The attribute set in Γ is called an authorization set, otherwise called non authorization set. Only user with an authorized set can get the key and decrypt the text.

We use logical expression to describe short text access control structure, n attributes as n elements. Each element is connected by "AND", "OR", and the threshold value etc.

The access control structure of CP-ABE is integrated into the time, category, theme, receiver and sender et al. So that we achieve the fine-grained control for short message and meet the encrypted

sharing needs of short message in the multi-user environment.

3. Encryption scheme of short message

According to the access control structure described in Section II, execute the improved CP-ABE scheme which reduces the number of bilinear operations to a fixed range in the decryption operation and improves the decryption efficiency.

1) Performing initialization algorithm on Server: Generating cyclic group G_1、G_2 of order p, g is a generator of G_1, bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$. System attribute set $P = \{p_1, p_2, \dots, p_u\}$, $1, \dots, u$ represent attribute label, β represents random chose, $\delta \in Z_p$, $\gamma_1, \dots, \gamma_u \in G_1$. Run initialization algorithm, output the public key $PK = \{g, g^\beta, e(g,g)^\delta, \gamma_1, \dots, \gamma_u\}$. The master sercet key MSK=g^δ,send MSK to users who encrypt short message, open PK to all users.

2) Data owner encrypts short message m.

a) According to the section II, construct the access control structure of short message.

$$\Gamma = (T_a)\mathrm{AND}(S_e)\mathrm{AND}(Z_1, Z_2, \dots, Z_b, p)\mathrm{AND}(K_1, \dots, K_c, q)$$
$$\mathrm{AND}(R_1\ \mathrm{OR}\ R_2, \dots., \mathrm{OR}\ R_d)\mathrm{AND}(C_1, C_2, \dots, C_g, o). \quad (3)$$

d' is the number of receivers encryption required，c' is the number of words in the short message M, q is the keywords threshold, p is the theme threshold , and o is the category threshold.

b) Data owner gets the master public key MPK from server, and encrypt short message based on access control structure.

According to the access control structure, data owner executes Monotone Span Programs [9] and generates linear secret sharing matrix M and mapping function ρ [10]. M is a $\ell \times$ n matrix, M_i is the I throw of the matrix, ρ is injective function. h represents the different attributes of M,and $\rho: \{1, \dots, \ell\} -> \{h|\rho(i) = h, i \in [1, \ell]\}$. According to the linear secret sharing scheme, we select random vector $V = (s, t_2, t_3, \dots, t_n) \in Z_p^n$, s is secret shared key, $t_2, t_3, \dots, t_n$ are random value, λ_i is the secret sharing key shadow, $\lambda_i = VM_i$, M_i is the I th row vector of M, and run encryption algorithm, output as follows:

$$CT = \{C=m*e(g,g)^{\delta s}, C'=g^s, C_i=g^{-\beta\lambda_i}\gamma^s_{\rho(i)},\ h\epsilon\Gamma/\rho(i),\ D_{I,h}=\gamma_h^s\}. \quad (4)$$

3) Get the decryption key of short message

a) According to the short message content that data user wants to visit, data user constructs short message attribute set $B.B = \{T_i, Z_1, \dots, Z_x, K_1, \dots, K_y, R_f, S_k, C_1, \dots, C_j\}$. B contains creation time of short message $T_{i'}$, sender information of short message $S_{k'}$, key words of short message $K_1,\dots,K_{y'}$, theme of short message $Z_1,\dots,Z_{x'}$, category of short message $C_1, \dots, C_j$,and receivers information of short cipher message. And data user submits attribute set to the server to get the decryption key.

b) According to the attribute set B submitted by data user and the master secret key MSK, cloud server selects random parameters $t \in Z_p$ and generates a secret key SK to decrypt the short message.

$$SK=\{k=g^\delta g^{-\beta t}, L=g^t, p \in B, K_p=\gamma_p^t\},\ p \text{ is user attribute.} \quad (5)$$

4) Data user decrypts the short cipher message CT. After the user receives the ciphertext CT, then carries on the following operation:

a) Data user decides whether their own attribute set to meet the access control structure made by data owner.

According to the linear secret sharing scheme, set the target vector V= (1,0,…,0). Match the attribute element set by data user and the attribute element mapping by matrix M, attribute set after matching is P={i: $\rho(i) \in B$, and $1 \le i \le l$},$P \subseteq \{1,2\ldots,l\}$. If you cannot find a set of vectors W multiple with the attribute vector M_i equal to the target vector V, the user's attribute set does not satisfy the access control structure made by data owner. Otherwise, visitors can make the following decryption operation.

b) The decryption operation is as follows:

Define the access control structure and the attribute set intersection of data user, $O = \{p: \text{exist } i \in P', p = \rho(i), p \in B \cap \Gamma\}$. The definition of the set is designed to prevent the redundant attributes in the decryption property to participate in the operation, and increase decryption operation cost.

User-defined function:

$$\beta(o)=\prod_{p \in O} \gamma(p). \tag{6}$$

$\gamma(p)$ represents attribute value γ_p of attribute p at group G_1, $\beta(o)$ represents attributes of short message multiply continuously. It provides convenience for the next calculation .

$$C_i^{'}=C_i * \prod_{p \in O/\rho(i)} D_{i,p} = g^{-\beta\lambda_i}\gamma_{\rho(i)}^{s} * \prod_{p \in O/\rho(i)} \gamma_p^{s} = g^{-\beta\lambda_i} * (\prod_{p \in O} \gamma(p))^{s} = g^{-\beta\lambda_i}\beta(o)^{s}. \tag{7}$$

C_i' represents the secret sharing key shadow λ_i in the distribution of the attributes short message. The secret sharing key shadow λ_i is matched through $\rho(i)$ in $x \in O/\rho(i)$.

$$K_O{}^{'} = \prod_{x \in O} K_x = \prod_{x \in O} \gamma_x^{t} = \prod_{x \in O} \gamma_x^{t} = \beta(o)^{t}. \tag{8}$$

Take the function $\beta(o)$ into C_i'、K_O', for later derivation.

The decryption formula is as follows:

$$e(g, g)^{\delta s} = \frac{e(K_O, C^{'}) e(\prod_{i \in P} (K_O^{'})^{w_i}, g^{s})}{e(\prod_{i \in P} (C_i^{'})^{w_i}, L)}. \tag{9}$$

$$m = \frac{CT}{e(g,g)^{\delta s}}. \tag{10}$$

According to decryption formula, we can obtain the short message content from the encrypted CT, apply CP-ABE into the encryption algorithm of short message effectively, realize quickly decrypt short ciphertext and access the short message for multiple users. The algorithm can meet the requirements of short message application.

4. Security proof

4.1 Security assumptions

The security of Waters scheme is based on the decision BDHE q-parallel assumption. This assumption is a strong difficult problem in mathematics, so it is not suitable for practical application. In this paper, the security assumptions were improved.

Definition 1：Modify the q-BDHE assumption, create an extension decisional-Bilinear Diffie Hellman Exponent assumption (Eq-BDHE). Choose bilinear group G_1, G_2[11] of order p, g is a generator of G_1, and choose randomly s, $\beta \in Z_p$ and $s = r + c\beta, \beta \neq r$、$\beta \neq s$.Select the security parameters c、r and c、r have no linear correlated with the victor $x = \{\beta^1, \ldots, \beta^q\}$. Give the vector as follows.

$y_2=(g,g^{\beta^1},\ldots,g^{\beta^q},g^{\beta^{q+2}},\ldots,g^{\beta^{2q}},g^s,c,r)$. (11)

There exists no probabilistic polynomial time algorithm F to distinguish $e(g,g)^{\beta^{q+1}s} \in G_2$ from y_2 and random value $R \in G_2$ with the negligible advantage ε . Proof is as follows.

$$T=e(g,g)^{\beta^{q+1}s}=e(g^{\beta^{q+1}},g^s)=e(g^{\beta^{q+1}},g^{r+c\beta})$$
$$=e(g,g)^{\beta^{q+1}r+\beta^{q+2}c}=e(g,g)^{\beta^{q+1}r}\,e(g,g)^{\beta^{q+2}c}. \quad (12)$$

According to derivation of the formula: $e(g,g)^{\beta^{q+2}c}$ can be calculated. Since r has no linear correlated with the victor $\mathbf{x}$, that is to say r cannot be expressed by vector $\mathbf{x}$, then given y_2, we cannot calculate $e(g,g)^{\sigma^{q+1}r}$. So the probability of identifying $T=e(g,g)^{\sigma^{q+1}r}$ can be negligible.

In conclusion, it requires restrictive condition. The restrictive condition are lacking parameter $g^{\sigma^{q+1}}$ and r has no linear correlated with $\mathbf{x}$. So identifying T has no relationship with c、r and it is proved that it is difficult to identify $e(g,g)^{\sigma^{q+1}r}$ $e(g,g)^{\sigma^{q+2}c}$.

4.2 Security analysis

According to indistinguishable chosen-plaintext game in the CP-ABE encryption scheme, we develop the definition based on CP-ABE to win the game.

Definition 2 :In the attribute encryption scheme, if the adversary can win chosen plaintext game in polynomial time, and the advantages ε can not be ignored, the scheme is secure.

Theorem 1: Assuming that decidability assumption Eq-BDHE is established, there is no adversary can choose to challenge the access structure $\Gamma(M_{l\times n},\rho)$ and break the encryption scheme in polynomial time in the attribute encryption scheme.

Proof: The security proof of the scheme is based on Theorem 1. Suppose that an adversary trys to challenge the access structure $\Gamma(M,\rho)$, he is able to break the security model with the undeniable advantages ε, so we can construct a simulator with the undeniable advantages $\frac{\varepsilon}{2}$ to solve the Eq-BDHE problem in Definition 2.

1) Init():The simulator loads the improved Eq-BDHE parameters y_2、T, the adversary announces to challenge access structure $\Gamma(M,\rho)$,$q \geq n+1$, n is the row of the matrix.

2) Setup():The simulator randomly selects $\delta=\delta'+\beta^{q+1},\delta \in Z_p$, making the system public key $e(g,g)^{\delta}=e(g,g)^{\delta'+\beta^{q+1}}=e(g,g)^{\beta^{q+1}}e(g,g)^{\delta'}$. For each element in system properties set U, select a random parameter Zx∈Zp,and perform the following operations.

If $x \in U$, $\gamma_x=g^{z_x}g^{\beta M_{I,1}}g^{\beta^2 M_{I,2}}\ldots g^{\beta^n M_{I,n}}$. (13)

Otherwise, $\gamma_x=g^{z_x}$. (14)

In addition to use γ_x as a factor in the calculation of g^{z_x}, so that all the attributes corresponding γ_x are random and independent of each other. Because of $q \geq n+1$ and the parametric conditions of Eq-BDHE assumptions, we are able to load each attribute x efficiently.

3) The adversary submits attribute set U' to the challenger to apply for the attribute private key. $U'=\{T_{i1},Z_1,\ldots,Z_{x1},K_1,\ldots,K_{y1},R_{f1},S_{k1},C_1,\ldots,C_{j1}\}$. If the attribute set meets the access structure submitted by the adversary, the challenger does not construct the attribute key. Otherwise, the following generation of private key operation is performed.

The private key is constructed as follows:

$L=g^t=g^{k+w_n\beta+\ldots\ldots+w_1\beta^q}$. (15)

After the calculation,

$$K=g^{\delta}*g^{-\beta t}=g^{\beta'+\beta^{q+1}}*g^{-\beta t}=g^{\delta'}*L^{\beta}=g^{\delta'}*g^{\beta k}\prod_{i=2,\ldots,n}(g^{-\beta^{q+2-i}})^{w_i}. \quad (16)$$

$$\text{When } x\in U_1',\ K_x=\gamma_x^t=L^{Z_X}(\prod_{j=1,\ldots,n}g^{\beta^j k}\prod_{\substack{m=1,\ldots,n\\ m\neq j}}(g^{\beta^{q+1+j-m}})^{w_m})^{M_{i,j}}. \quad (17)$$

$$\text{When } x\in U_2',\ K_x=\gamma_x^t=g^{z_x t}=L^{z_x}.\ U_1'=\{x:\ \rho(i)\in U'\cap U\},\ U_2'=\{x:\ \rho(i)\in U' \text{ 且 } \rho(i)\notin U\} \quad (18)$$

4) Challenge the short plaintext: The adversary sends two equal length of plaintext to challenger. Challenger selects one of plaintext encrypt. The calculation as follows:

$$CT=\left\{C=m*e(g,g)^{\delta s},C'=g^{s},C_i=g^{-\beta\lambda_i}\gamma_{\rho(i)}^{s},\ D_{i,h}=\gamma_h^s\right\},\ h\in\Gamma/\rho(i). \quad (19)$$

Simulator loads Eq-BDHE parameters. According to the results of the load, the output ciphertext is divided into two categories.

a) If simulator loads parameters and output $T=e(g,g)^{\beta^{q+1}s}$, the output ciphertext as follows:

$$C=m_u e(g,g)^{\delta s}=m_u*e(g,g)^{(\delta'+\beta^{q+1})s}=m_u*e(g,g)^{\beta^{q+1}s}*e(g,g)^{\delta' s}.$$

$$C'=g^{s}. \quad (20)$$

Simulator choice a random vector $V=(s,s\beta+t_2',s\beta^2+t_3',\ldots,s\beta^{n-1}+t_n')\in z_p^n$, .The random value $t_2',\ t_3',\ldots,\ t_n'\in Z_p$. s is attributes shared secret key, and the shared secret key s is divided into the form of vector V, combined with the lambda $\lambda_i=VM_i$ in linear refactoring features to eliminate parameter $g^{\sigma_j s}$ inC_i that simulator can't simulate term. The calculation results are as follows:

$$C_i=\left(\prod_{j=1,\ldots,n}g^{\beta^{M_{i,j}t_j}}\right)(g^{s})^{-z_{\rho(i)}}.$$

$$D_{i,h}=\gamma_h^s=(g^{z_h}g^{\beta M_{i,1}}g^{\beta^2 M_{i,2}}\ldots g^{\beta^n M_{i,n}})^{s}. \quad (21)$$

Because $s=r+c\beta$.

$$D_{i,h}=\gamma_h^s=\left(g^{z_h}g^{\beta M_{i,1}}g^{\beta^2 M_{i,2}}\ldots g^{\beta^n M_{i,n}}\right)^{s}=(g^{z_h}g^{\beta M_{i,1}}g^{\beta^2 M_{i,2}}\ldots g^{\beta^n M_{i,n}})^{r+c\beta}$$

$$=(g^{z_h}\prod_{j=1,2\ldots,n}g^{\beta^j M_{i,j}})^{r+c\beta}=g^{z_h r}\prod_{j=1,2,\ldots n}(g^{\beta^j})^{M_{i,j}r}\cdot g^{z_h}\prod_{j=1,2,\ldots n}(g^{\beta^{(j+1)}})^{M_{i,j}c}. \quad (22)$$

Where in $h\in\Gamma/\rho(i)$, the short ciphertext is effective value at this time, the adversary can break security scheme with probability $\frac{1}{2}+\varepsilon$ to win the game.

b) If the simulator loads parameters and output $T=R$,the output ciphertext as follows:

$$C=m_u*e(g,g)^{\beta^{q+1}s}*e(g,g)^{\delta' s}=m_u*R*e(g,g)^{\delta' s}. \quad (23)$$

Because R is double linear group of random values, so C also becomes a random value. That completely hide the plaintext information from the adversary and the probability of adversary breaking the scheme is $\frac{1}{2}$. Thus the probability of the adversary breaking the scheme is related to the T value.

5) Repeat steps 3.

6) Guessing stage.

If the adversary can successfully guess the challenger selection decrypted plaintext, it indicates the determination of the Eq-BDHE problem can be solved. There exists a polynomial function,

which can be calculated:

$$T=e(g , g)^{\beta^{q+1}s}. \tag{24}$$

$$Pr\left[F\left(y, T=e(g , g)^{\beta^{q+1}s}\right)=0\right]=\frac{1}{2}+\varepsilon. \tag{25}$$

If the adversary can't guess which one is the encrypted plaintext, the result of Eq-BDHE is $T = R$.

$$Pr[F(y, T=R)=0]=\frac{1}{2}. \tag{26}$$

The probability of simulator solving the decisional Eq-BDHE problem is:

$$\varepsilon'=\frac{1}{2} Pr\left[F\left(y, T=e(g , g)^{\beta^{q+1}s}\right)=0\right]+\frac{1}{2}Pr[F(y, T=R)=0]-\frac{1}{2}=\frac{1}{2}\varepsilon. \tag{27}$$

4.3 Efficiency analysis

In this paper, we encrypt short message with Waters scheme and the improved CP-ABE scheme. Based on the experimental results, the computation efficiency of the short message encryption scheme is analyzed.

Assume that U is expressed the number of attributes of the whole system, |B| is expressed the user' attribute set size, |P| is expressed attribute element set mapping by access matrix of the data user's attribute element, |Γ| is expressed the number of attributes in the access control structure, |O| is expressed attribute set in the access control structure and the number of attribute of the intersection of data user's attribute sets. Pair is a bilinear pairing computation, $|G_1|$、$|G_2|$ are expressed the computations of group G_1、G_2respectively. The computation consumption of the improved CP-ABE scheme and Waters scheme are shown as Table 1.

Table1. Table consumption

Scheme	Decryption Consumption	Cipher Consumption	Private Key Consumption	Safety Assumption
Waters	$(2\|P\|+1)\times$ Pair $+(\mathbf{2}\|\mathbf{P}\|+\mathbf{1})\|\mathbf{G_2}\|$	$\|\mathbf{G_2}\|+(\mathbf{4}\|\mathbf{\Gamma}\|+\mathbf{1})\|\mathbf{G_1}\|$	$3\|G_1\|+$ $\|\mathbf{B}\|\|\mathbf{G_1}\|$	q-paraller-BDHE
Improved	$\|O\|\|P\|\|G_1\|+$ $(\|\mathbf{O}\|+\|\mathbf{P}\|)\|\mathbf{G_1}\|+\mathbf{3Pair}$ $+\mathbf{2}\|\mathbf{G_2}\|$	$\|G_2\|+\|G_1\|(1+$ $\mathbf{2}\|\mathbf{\Gamma}\|+\|\mathbf{\Gamma}\|^2)$	$3\|G_1\|+$ $\|\mathbf{B}\|\|\mathbf{G_1}\|$	Eq-BDHE

As shown in Table1, compared with the Waters scheme, the improved CP-ABE scheme is much weaker in security assumption; but the improved CP-ABE scheme is more efficient in decryption consumption. That is because the number of bilinear operations in the decryption operation is limited to three. While the number of bilinear operations in Waters scheme increases linearly with the number of attributes. According to experimental results in the literature [12], the running time of bilinear operations is 8.22ms, while the multiplication operation consumes only 0.0034ms in group G_1、G_2. It can be seen that the consumption time of bilinear operation is the longest in the short message encryption scheme based on attribute encryption.

Based on analysis above, we perform decryption experiment using the Waters scheme and the improved CP-ABE scheme respectively. According to the experimental results, grab WeChat content as short message content through the Spiderman crawler, use the short message encryption algorithm in section three and analyze the operation efficiency of short message in encryption scheme. Specific experimental environment is Hewlett-Packard AMD Athlon (tm) X2 Dual-Core QL-60 1.90GHZ, 2GB of memory, the operating system windows7, kernel version 6.1.7600, security preferences

TYPEA, and Eclipse4.3. We adapt cryptographic library (PBCL), and use JPBCL to realize the decryption experiment of CP-ABE. Test results as shown in Fig.1, the unit is ms.

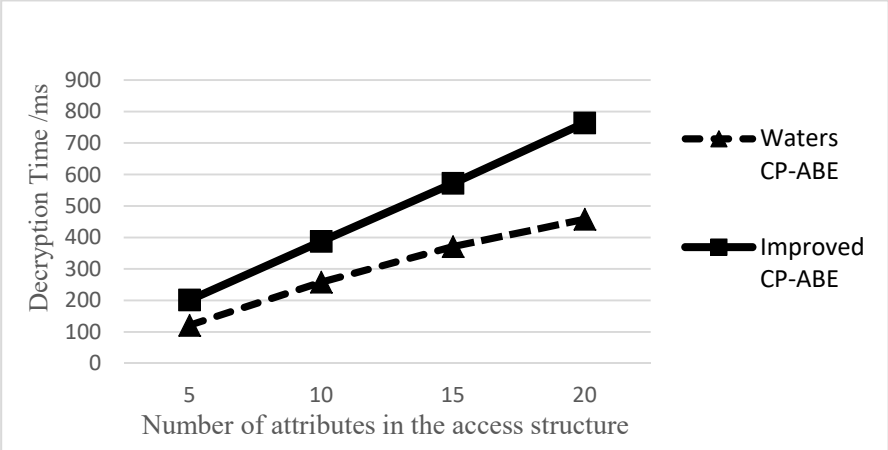

Fig. 1. Contrast of the schemes

Experimental results are shown by comparing with the CP-ABE program by Waters, the proposed scheme is less time-consuming when operating decryption. With the increase of the number of attributes in the access structure, the proposed program in the decryption stage is more efficient. This is mainly because that the amount of bilinear operations is limited to three in the CP-ABE, so the bilinear operation time is fixed in a range. Time's growth come mainly from the group of the mathematical operation on G_1, G_2, while the growth does not impact time of short message decryption. Therefore, this scheme based on CP-ABE provides greater efficiency in short message encryption.

5. Summary

In this paper, through the analysis of short ciphertext's access requirements, a short message encryption scheme based on CP-ABE is proposed. And Select the attribute elements of the short message extended model as the attribute elements of the access control structure. The scheme realizes the fine-grained access control of short message .Use the access control structure of short message, On the one hand, we can limit the user's access, on the other hand, and we can make different users access the same short message, to achieve the sharing needs of users' short message.

References

[1] Liu Hui and Wang Jing, "End-to-end security short message system based on public key encryption[EB/OL]," Beijing:Sciencepaper Online, 2007.

[2] Sun Yuze, Chi Jia, and Hu Liang, "Based on the DES encryption algorithm to encrypt communications between the server and the Android client," Journal of Northeast Normal University(Natural Science Edition) , 47(3), pp. 78-82, 2015.

[3] Kiah M L M and Al-Bakri S H, "A novel peer-to-peer SMS security solution using a hybrid technique of NTRU and AES-Rijndael," Scientific Research & Essays, 2(22), pp. 3455-3466, 2010.

[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," In EUROCRYPT 2005, LNCS 3494, Springer, pp. 457-473, 2005.

[5] Herranz J, Laguillaumie F, and Ràfols C, "Constant Size Ciphertexts in Threshold Attribute-Based Encryption," Public Key Cryptography – PKC 2010. Springer Berlin Heidelberg, pp.19-34, 2010

[6] Bethencourt, A.Sahai, and B.Waters, “Ciphertext-Policy Attribute-BasedEncryption,” In IEEE Symposium on Security and Privacy, IEEE ConputerSociety, Los Alamitos (2007), pp.321-334, 2007.

[7] Li M, Yu S, Zheng Y, Ren K, and Low W, “ Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” Parallel and Distributed Systems, IEEE Transactions on, 24(1), pp.131-143, 2013.

[8] Chen Yan li, Du Ying jie, and Yang Geng, “Efficient Attribute-based Authenticated Key Agreement Protocol,” 4(41), pp.150-154,177, 2014.

[9] Karchmer M and Wigderson A, “On span programs: Structure in complexity theory conference, ” San Diego, California:Proceedings of the Eighth Annual. IEEE, pp.102-111, 1993.

[10]Zhen Liu and Zhenfu Cao, “On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption,” Iacr Cryptology Eprint Archive +, 2010.

[11]Dan B and Franklin M, “ Identity based encryption from the Weil pairing: Advances in Cryptology — CRYPTO 2001,” Lecture Notes in Computer Science, 32(3), pp.213-229, 2003

[12]Chen Yanli,Du yingjie,Yang yu “ Efficient Attributebased Authenticated Key Agreement Protocol,” Computer Science, 4(41),pp.150-154, 2014