A Key-Policy Attribute-based Signcryption Scheme for Enterprise Cloud Storage

Jia Luo[a], Qiuyue Zhu[b] and Jiangheng Kou[c]

School of Computer and Software Engineering, Xihua University, Chengdu 610039, China

[a]Sunshine524_luo@126.com, [b]qiuyue1316@163.com,[c]405192802@qq.com

Abstract

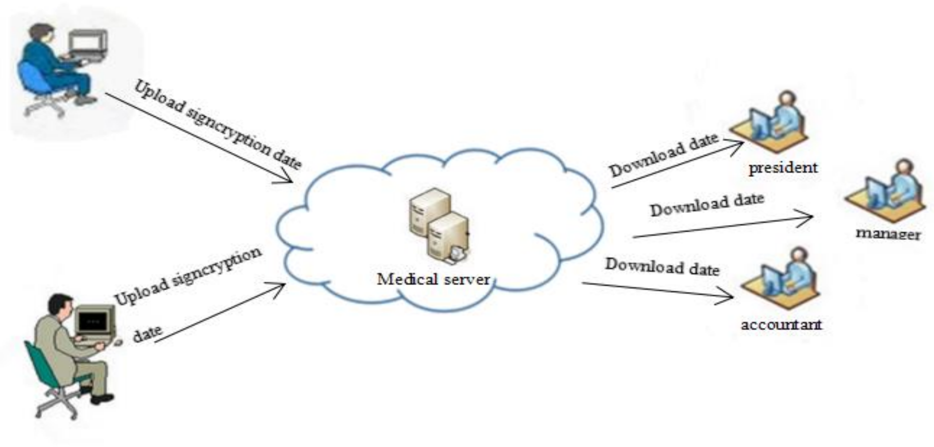
Enterprise Cloud Computing (ECC) has been widely used in our life, security has been regarded as one of the greatest problems in the development of ECC.In order to address this security loophole ,we propose a new key-policy attribute based signcryption (KP-ABSC) scheme and its application in ECC.The proposed KP-ABSC scheme is proven to be indistinguishable against adaptive chosen plaintext attacks under the DBDH assumption and existentially unforgeable against adaptive chosen message and identity attacks under the CDH assumption. The proposed scheme achieves public verifiability of the ciphertext,enabling any party to verify the integrity and validity of the ciphertext.

Keywords

Key-Policy Attribute based Signcryption, Public Verifiability, Confidentiality, Unforgeability.

1. Introduction

As economic globalization paces up, Cloud Computing is widely applied in our lives. For instance, Enterprise Cloud Computing is a cloud system specifically applied within commercial domain. It designs internal computer systems for commercial corporations, including customer relationship management software, human resource software and database software, etc. By utilizing the massive computing and storage capacity of internet background center database, it is able to provide corporations with services such as data aggregation and distribution, data storage and backup, and data management. The value of the Enterprise Cloud Computing can be listed as follows. First, it enhances the utilization efficiency of the system. Second, it automatically distributes, supplies and manages data. Third, the flexibility of IT is strengthened. Fourth, it has strong maneuverability. Fifth, scalability is featured.



For Enterprise Cloud Computing, confidentiality, integrity, authentication and non-repudiation must be guaranteed. On the other hand, its security requirement has also shifted, from both communicating parties are single users to at least one should be a multi-user. Attribute-Based Encryption(ABE)[1] introduced in 2006 can meet up with the new standards of cryptography. The encryption based on attribute is a public-key encryption mechanism. It describes identity via a set of attributes. Meanwhile, it introduces access control structure, relating the user’s private-key and cipher text to an attribute set and access structure. When and only when the private key matches the cipher text, can the information be cracked. In 2010, Gagné and other scholars [2] proposed the scheme of (n,n)-ABSC under standard model for the first time, and gave a formal edition of security definition, the combination of confidentiality of information and indistinguishability of cipher text. Nevertheless, the threshold of the signer and encipherer is fixed, and sign attribute is independent from both encrypt and decrypt attribute, so this theory was not flexible in practical application. Later in 2011, Emura and others [3] introduced CP-ABSC. It supported complex access structure and dynamic properties, but it needed the signer’s specific attribute. In 2012, Professors headed by Zhang Guoyin [4] put forward ABSC with dynamic threshold. This model has the features such as safeguarding the signer attribute’s privacy and safety, and enabling multi-receivers. In addition, it proved its security under random oracle model. In 2013, Dr. Hu Chunqiang [5] and his peers introduced FABSC within BANS application. Based on fuzzy attribute-based signcryption, this scheme used data encryption, access control and digital signature and applied them for patient’s medical information in BAN. In 2013, scholars including Dr. Guo Zhenzhou [6] came up with attribute-based ring signcryption scheme, which formed a ring signcryption consisting of the signer’s attribute and the decipherer’s attribute. However, such a scheme failed to fulfill the enforceability of cipher text because it did not require signer’s private-key. Also in 2013, Professor Wei [7] and his fellow scholars proposed a traceable attribute-based signcryption. In 2014, Liu and others [8] introduced CP-ABSC on the basis of a safe application environment that enabled people to share personal health record in cloud computing. This article introduces a scheme of KP-ABSC in enterprise cloud computing application environment. Compared to previous signcryption schemes, it is more efficient and has public verifiability. The security of this scheme is based on Computational Diffie–Hellman problem assumption and Decisional bilinear Diffie-Hellman problem Assumption. In addition, it is safe to choose attribute collection and message attack under random oracle model.

2. Preliminaries

2.1 Bilinear maps

Let G_1 and G_2 be two multiplicative cyclic groups of prime order p, Let g be a generator of G_1.and Discrete Logarithms Problem is difficult in G_1 and G_2, A bilinear map is a map $e: G_1 \times G_1 \rightarrow G_2$, satisfying the following properties:

Bilinearity:for all $u,v \in G_1$ and $a,b \in Z_p$, we have $e(u^a, v^b) = e(u,v)^{ab}$.

Non-degeneracy: There exists $u,v \in G_1$ such that $e(u,v) \neq 1$.

Computability:There is an efficient algorithm to compute $e(u,v)$ for all $u,v \in G_1$.

2.2 Complexity assumptions

Definition2.1(Computational Diffie–Hellman problem assumption)Given (g, g^a, g^b), where g is a generator of G and $a,b \in Z_p^*$, the computational Diffie-Hellman problem is to compute g^{ab}.

Definition2.2 (Decisional bilinear Diffie-Hellman problem Assumption) Given two groups G_1 and G_2 of the same prime order p, a bilinear map: $e: G_1 \times G_1 \rightarrow G_2$ and a generator g of G_1, the decisional bilinear Diffie-Hellman (DBDH) problem is, given (g, g^a, g^b, g^c, z) ,where $a,b,c \in Z_p^*$ and $z \in G_2$, to decide whether $z \overset{?}{=} e(g,g)^{abc}$ holds.

2.3 Monotone Span Program [9]

Let K be a field and $\{x_1, x_2, \ldots, x_n\}$ be a set of variables (will be labeled by attributes). A monotone span program over K is labeled matrix $\hat{M}(M,\rho)$ where M is a matrix of size $d \times l$ over K, and ρ is a labeling of the rows of M by an literal from $\{x_1,x_2,L\ ,x_n\}$ (every row is labeled by one literal).A monotone span program accepts or rejects an input by the following criterion. For every input set γ, define the submatrix M_γ of M consisting of those rows whose labels are in γ. The monotone span program $\vec{M}$ accepts γ if and only if $\vec{1}\in span(M_\gamma)$, The MSP $\vec{M}$ computes a Boolean function f_M if it accepts exactly those inputs γ where $f_M(\gamma)=\vec{1}$. The size of $\vec{M}$ is the number of rows in M.

3. Security Definitions For Kp-Absc

Definition3.1(Confidentiality):A KP-ABSC is indistinguishable against adaptive chosen cipher text attack property under selective attribute model if there exists no polynomial-bounded adversary A having non-negligible advantage in the following games.

Init: The adversary A declares the set of attributes γ which will be used to signcryption the challenge cipher text, and sends γ to the challenger C.

Setup: The challenger C runs the $setup(\kappa)$ algorithm to generates the master secret key MK and outputs public parameters PK which with a security parameter κ. C gives PK to A , while keeps MK secret.

Phase 1: The adversary A can adaptively makes a polynomial number of the following queries oracles, but the challenge set γ does not satisfy $f_M(\gamma)=\vec{1}$.

- Key Extract oracle: The adversary A chooses a set of attributes ω and sends it to the challenger C .If $f_M(\omega)\neq\vec{1}$, then C runs $KeyExtract(MK,\hat{M},\omega)$ algorithm, and sends D_ω back to A . Otherwise, C rejects the request.
- Unsigncryption oracle The adversary A queries a cipher text CT and receiver's attribute set ω_B ,.If $f_M(\omega_B)=\vec{1}$ C rejects the request, Otherwise, C runs $KeyExtract(MK,\vec{M},\omega_B)$ algorithm to generates D_{ω_B} and runs $Unsigncryption(CT,\omega_B)$ algorithm, If CT is a valid signcryption cipher text ,then C returns m to adversary A , else C outputs"$\perp$".

Challenge: The adversary A decides when to end the**Phase1** after that submits two equal length messages $\{m_0,m_1\}$ and a receiver's attribute set γ ,then sends them to C.The challenger C chooses a random bit $\delta\in\{0,1\}$ and runs $Signcryption(PK,m_\delta,\gamma)$ algorithm to compute challenge ciphertext CT^* that related to m_δ ,then sends CT^* to the adversary A .

Phase 2: The adversary A can continue adaptively to make queries as in **Phase 1.**

Guess: The adversary A outputs a guess δ' of δ ,If $\delta'=\delta$,we say that A wins the game.

The success probability is defined to be $Succ_{\mathrm{A}}^{IND-ABSC-CCA2}(\kappa)=\left|\Pr[\delta'=\delta]\right|-\dfrac{1}{2}$.

Definition3.2 (Enforceability): A KP-ABSC is existentially unforgeable against adaptive chosen message attack property under selective attribute model if there exists no polynomial-bounded adversary A having non-negligible advantage in the following games.

Setup: Same as in the above game.

Training: A runs polynomial time number of queries as described in **Phase1** in **Definition 3.1**.Every time the query results must be valid and correct query.

Forgery: A outputs a new forged cipher text $CT'=(\sigma,V,\{E_i\}_{i\in\gamma},\{\sigma_j\}_{j\in\omega'_A})$,where γ and ω'_A are not queried in the **Training.** If Unsigncryption (CT',γ) is not outputs "$\perp$", then A wins the game.

4. Our Construction

The scheme is described as follows.

setup(κ) :The PKG selects a security parameter κ ,then PKG complete the following steps

1． let G_1 and G_2 be two multiplicative cyclic groups of prime order $p>2^{\kappa}$, and g be a generator of G_1. Let

$e: G_1 \times G_1 \to G_2$ be a bilinear map.

Define the universe of attributes U ,$|U| = l$. Now, for each attribute $i \in U$,choose a number t_i uniformly at random from Z_p ,let $T_i = g^{t_i} (i = 1, \cdots, l)$ .choose two number α, h uniformly at random from Z_p^* ,let $Y = e(g,g)^{\alpha}$ and

$H = g^h$.

2． Let $\{0,1\}^{l_m}$ be the message space, l_m is the length of each message sent. Choose a secure one-time symmetric-key cipher $\Sigma = (Enc, Dec)$ which takes a plaintext and cipher text of length $l_m + l_2$ with key space G_T .

3． Select three cryptographic hash function: $H_1: \{0,1\}^{l_m} \times Z_p^* \to Z_p^*$, $H_2: \{0,1\}^* \to \{0,1\}^{l_2}$, $H_3: \{0,1\}^* \to G_1$.

The published public key: $PK = (G_1, G_2, e, g, \{T_i\}_{i=1}^{l}, Y, \Sigma, H, H_1, H_2, H_3)$

The master secret of the system: $MK = (\alpha, h, \{t_i\}_{i=1}^{l})$.

keyExtract(MK, ω): given ω that is a use's attribute set to PKG, then PKG Complete the following steps

Inputs an MSP $\widehat{M}(M, \rho)$,where M is a matrix of size $d \times l$ over K , and ρ is a labeling of the rows of M by an attribute from U (every row is labeled by one attribute).

Choose a random vector $\vec{u}$ from Z_p^l such that $\vec{1} \cdot \vec{u} = \alpha$, that is, $\vec{u} =$ （$u_1, u_2, \cdots, u_l$）such that $\sum_{i=1}^{l} u_i = \alpha$.

For each row vector $\overrightarrow{M_i}$ give the following secret value to the user: $D_{i,0} = g^{\frac{\overrightarrow{M_i} \cdot \vec{u}}{t_{\rho(i)}}}$, $D_{i,1} = g^{h \cdot t_{\rho(i)}}$.

The use's decryption key $D = (D_{i,0}, D_{i,1} : i \in \omega)$.

Signcryption(m, γ)**:** $A \xrightarrow{m} B$

Here, $\omega_A' \subset \omega_A$ is the subset of attributes of the sender A ready to signcryption, γ is the attribute of the receiver B .The sender A choose a random value $r \in Z_p^*$ as its own private values,then A complete the following steps

1. Complete $s = H_1(m, r)$, $key = Y^s = e(g,g)^{\alpha s}, C_1 = g^s, V_1 = g^{sr}$.

2. For each $i \in \gamma$ complete $E_i = T_i^s, C_2 = \prod_{i \in \gamma} E_i$.

3. Compute $\theta = H_2(M, key, C_1, C_2, \omega_A', \gamma)$ and encrypt the message $C = Enc_{key}(M \| \theta)$.

4. Compute $Q = H_3(C, C_1, V_1, \omega_A', \gamma)$ and for each $j \in \omega_A'$ calculated to generate signature $V_2 = \{\prod_{j \in \omega_A'} D_{j,1}\} Q^{sr}$.

Finally, the cipher text CT is $CT = (\omega_A', \gamma, V_1, V_2, C, C_1, C_2)$.

Unsigncryption(C, ω_B)**:** The receiver B obtains the ciphertext CT and choose $\gamma \subset \omega_B$.

If $f_M(\gamma) = \vec{1}$, the span program $\widehat{M}(M, \rho)$ accepts γ . Thus, there exist $y_i \in Z_p$ such that, $\sum_{\rho(i) \in \gamma} y_i \square \overrightarrow{M_i} = \vec{1}$ .After that the receiver B Complete the following steps

1. Compute $Q' = H_3(C, C_1, V_1, \omega_A', \gamma)$ and check the validity of the ciphertext CT as $e(V_2, g) \overset{?}{=} e(H, \prod_{j \in \omega_A'} T_j) \cdot e(Q', V_1)$ .if it is invalid, output"$\perp$"; otherwise, proceed as follows.

2. Restore the symmetric decryption key as $key' = \prod_{\rho(i)\in\gamma} e(D_{i,0}, E_{\rho(i)})^{y_i}$,then Work out the message $M'\|\theta' = Dec_{key'}(C)$.

3. Compute $\bar{\theta} = \mathrm{H}_2(M', key', C_1, C_2, \omega'_A, \gamma)$,if $\theta' = \bar{\theta}$,accept the message as $M = M'$; else, output"$\perp$".

5. Analysis of the Proposed Scheme

5.1 Correctness of our proposed scheme

1. public verifiability of the cipher text

$$e(V_2,g) = e(\{\prod_{j\in\omega'_A} D_{j,1}\}Q^{sr},g) = e(\prod_{j\in\omega'_A} D_{j,1},g)e(Q^{sr},g) = e(H,\prod_{j\in\omega'_A} T_j)\cdot e(Q',V_1)$$

Work out the message

$$key' = \prod_{\rho(i)\in\gamma} e(D_{i,0}, E_{\rho(i)})^{y_i} = \prod_{\rho(i)\in\gamma} e(g^{\frac{\vec{M_i}\cdot\vec{u}}{t_i}}, g^{s\cdot t_{\rho(i)}})^{y_i} = \prod_{\rho(i)\in\gamma} e(g,g)^{\vec{M_i}\cdot\vec{u}\,s\,y_i} = e(g,g)^{s\vec{u}\sum_{\rho(i)\in\gamma} y_i \cdot \vec{M_i}} = e(g,g)^{s(\vec{1}\cdot\vec{u})} = e(g,g)^{s\alpha} = key$$

$$M'\|\theta' = Dec_{key}(C)$$

$$\bar{\theta} = \mathrm{H}_2(M', key', C_1, C_2, \omega'_A, \gamma) = \theta'$$

$$\Rightarrow M = M'$$

5.2 Confidentiality

Theorem5.2: If an IND-ABSC-CCA2 adversary A can break our scheme in the random oracle model, then there exists an effective algorithm B that solves DBDH problem with a non-negligible advantage. That is the algorithm B can distinguish between the $(A = g^a, B = g^b, C = g^c, e(g,g)^{abc})$ and $(A = g^a, B = g^b, C = g^c, e(g,g)^z)$ with a non-negligible advantage.

Proof: Suppose there exists an IND-ABSC-CCA2 adversary A can break our scheme with a non-negligible advantage ε, then we can build an effective algorithm B that can solve the BDHE problem with an advantage of at least $\frac{\varepsilon}{2}$ .Algorithm B construction is as follows

Init: The adversary A declares the set of attributes γ which will be used to signcryption the challenge ciphertext, and sends γ to the challenger C.

Setup: The challenger C runs the $setup(\kappa)$ algorithm with a security parameter κ ,then the challenger C complete the following steps.

1. Let G_1 and G_2 be two multiplicative cyclic groups of prime order $\mathrm{p}>2^{\kappa}$, and g be a generator of G_1 . Let $e:\mathrm{G}_1\times\mathrm{G}_1\to\mathrm{G}_2$ Be a bilinear map. Define the universe of attributes U , $|\mathrm{U}| = l$. For each attribute $i\in\mathrm{U}$,choose a number t_i uniformly at random from Z_p ,let $T_i = g^{t_i} (i = 1,\cdots,l)$ .choose two number α, h uniformly at random from Z_p^* ,let $Y = e(g,g)^{\alpha}$ and $H = g^h$ ..Let $\{0,1\}^{l_m}$ be the message space, l_m is the length of each message sent. Choose a secure one-time symmetric-key cipher $\sum = (Enc, Dec)$ which takes a plaintext and cipher text of length $l_m + l_2$ with key space G_T .Select three cryptographic hash function: $H_1:\{0,1\}^{l_m}\times\mathrm{Z}_p^*\to\mathrm{Z}_p^*$, $H_2:\{0,1\}^*\to\{0,1\}^{l_2}$, $H_3:\{0,1\}^*\to\mathrm{G}_1$.

2. The challenger C chooses a random bit $\mu\in\{0,1\}$ and four random values $a,b,c,z\in\mathrm{Z}_p$ .If $\mu = 1$,then $(A,B,C,Z) = (g^a, g^b, g^c, e(g,g)^{abc})$, otherwise $(A,B,C,Z) = (g^a, g^b, g^c, e(g,g)^z)$ .The algorithm B goal is to output a value δ' for speculation δ .

3. Let $Y = e(A = g^a, B = g^b) = e(g,g)^{ab}$.

4. If $i \in \gamma$,then randomly chooses $t_i = r_i \in \mathrm{Z}_p$ let $T_i = g^{r_i}$ .otherwise ,randomly chooses $\beta_i \in \mathrm{Z}_p, t_i = b\beta_i$ let $T_i = g^{b\beta_i}$.

The challenger C sends public key $PK = (\mathrm{G}_1, \mathrm{G}_2, e, g, \{T_i\}_{i=1}^{l}, Y, \Sigma, H, H_1, H_2, H_3)$ to adversary A and reserves the master secret of the system $MK = (\alpha, h, \{t_i\}_{i=1}^{l})$.

Phase 1: The adversary A can adaptively makes a polynomial number of the following queries oracles, but the challenge set γ does not satisfy $f_M(\gamma) = \vec{1}$.

- Key Extract oracle The adversary A chooses a set of attributes ω and sends it to the challenger C .If $f_M(\omega) \neq \vec{1}$, then C runs $KeyExtract(MK, \widehat{M}, \omega)$ algorithm, and sends D_ω back to A . Otherwise, C rejects the request.
- Unsigncryption oracle The adversary A queries a cipher text CT and receiver's attribute set ω_B .If

$f_M(\omega_B) = \vec{1}$, C rejects the request, Otherwise, C runs

$KeyExtract(MK, \vec{M}, \omega_B)$ Algorithm to generates D_{ω_B} and runs $Unsigncryption(CT, \omega_B)$ algorithm, If CT is a valid signcryption ciphertext, then C returns m to adversary

A , else C outputs "$\perp$".

Challenge: The adversary A decides when to end the **Phase1** after that submits two equal length messages $\{m_0, m_1\}$ and a receiver's attribute set γ ,then sends them to C .The challenger C chooses a random bit $\delta \in \{0,1\}$ and runs $Signcryption(PK, m_\delta, \gamma)$ algorithm to compute challenge cipher text CT^* that related to m_δ .If $\mu = 0$,let $s = c$ and complete $C = Enc_{key}(M \| \theta) = Enc_{e(g,g)^{abc}}(M \| \theta)$ of the CT^* ,this indicates that the cipher text is valid. Otherwise, let $C = Enc_{key}(M \| \theta) = Enc_{e(g,g)^z}(M \| \theta)$ is a random value. Finally, the challenger C sends CT^* to the adversary A .

Phase 2: The adversary A can continue adaptively to make queries as in **Phase1.**

Guess: The adversary A outputs a guess δ' of δ , If $\delta' = \delta$, the algorithm B outputs $\mu' = 0$ .otherwise, the algorithm B outputs $\mu' = 1$.

The adversary A win the game with a non-negligible advantage $Succ_{\mathrm{A}}^{IND-ABSC-CCA2}(\kappa) = |\Pr[\delta' = \delta]| - \frac{1}{2} = \varepsilon$, after that we analyzes advantage which the algorithm B can distinguish between the $(A = g^a, B = g^b, C = g^c, e(g,g)^{abc})$

And $(A = g^a, B = g^b, C = g^c, e(g,g)^z)$.

If $\mu = 0$, we can get a valid cipher text CT^* , the probability of the adversary A can guess correctly $\delta' = \delta$ is

$\Pr[\delta' = \delta | \mu = 0] = \frac{1}{2} + \varepsilon$ .When $\delta' = \delta$, the algorithm B outputs

$\mu' = 0$, thus $\Pr[\mu' = \mu | \mu = 0] = \frac{1}{2} + \varepsilon$.

If $\mu = 1$, the $key = e(g,g)^z$ is a random value, that is the cipher text CT^* is invalid. The probability of the adversary A can guess correctly $\delta' = \delta$ is $\Pr[\delta' = \delta | \mu = 1] = \frac{1}{2}$,in other words, $\Pr[\delta' \neq \delta | \mu = 1] = 1 - \frac{1}{2} = \frac{1}{2}$ .when $\delta' \neq \delta$,

The algorithm B outputs $\mu' = 1$, thus $\Pr[\mu' = \mu | \mu = 1] = \frac{1}{2}$.

Thus, the advantage of the algorithm B in solving DBDH problem is

$$\frac{1}{2}\Pr[\mu'=\mu|\mu=0]+\frac{1}{2}\Pr[\mu'=\mu|\mu=1]-\frac{1}{2}=\frac{1}{2}(\frac{1}{2}+\varepsilon)+\frac{1}{2}\frac{1}{2}-\frac{1}{2}=\frac{\varepsilon}{2}$$

5.3 Unforgeability

The enforceability of our scheme can be rely on the CDH problem. The detail process is similar to the proof of Maier's [10] construction which is omitted here.

6. Conclusion

In this paper, we proposed a novel key-policy attribute-based signcryption scheme (KP-ABSC) which can be applied on Enterprise Cloud Computing. The preliminaries, security definitions and a construction KP-ABSC are given, and proven to be indistinguishable against adaptive chosen plaintext attacks under the DBDH assumption and existentially unforgeable against adaptive chosen message and identity attacks under the CDH assumption. Our future research aims at designing more efficient attribute based signcryption schemes in standard model.

Acknowledgements

This paper is supported by Xihua University Graduate Innovation Fund (Research on attribute based ring signcryption scheme and its application, Fund number: ycjj2015073).

References

[1] Sahai A,Waters B.Fuzzy identity based encryption[A]. Advances in Cryptology(EUROCRYPT 2005)[C].Berlin, Springer-Verlag,2005.457-473

[2] Gagne M,Narayan S,Safavi-Naini R.Threshold attribute based signcryption[A].Proceedings of the 7th International Conference on Security and Cryptography for Networks, Amalfi, Italy, Sep. 13-15, 2010, LNCS 6280:154-171.

[3] Emura K,Miyaji A,Rahman M.Toward dynamic attribute based signcryption(Poster)[C]. Proceedings of the 16th Australasian Conference on Information Security and Privacy, Melbourne, Australia, July 11-13, 2011, LNCS 6812:439-443.

[4] Zhang G Y, Fu X J, Ma C G. A dynamic threshold attributes-based signcryption scheme[J]. Dianzi Yu Xinxi Xuebao(Journal of Electronics and Information Technology), 2012, 34(11): 2680-2686.

[5] Hu C,Zhang N,Li H,Cheng,X.,Liao,X.:Body Area Network Security: A Fuzzy Attribute-based Signcryption Scheme. IEEE Journal on Selected Areas in Communications 31(9), 37–46 (2013)

[6] Guo Z, Li M, Fan X. Attribute-based ring signcryption scheme[J]. Security and Communication Networks, 2013, 6(6): 790-796.

[7] Wei J, Hu X, Liu W. Traceable attribute-based signcrypt- ion[J]. Security and Communication Networks, 2014, 7(12): 2302-2317.

[8] Liu J, Huang X, Liu J K. Secure sharing of personal health records in cloud computing: ciphertext-policy attribute- based signcryption[J]. Future Generation Computer Systems, 2015, 52: 67-76.

[9] Goyal,V.,Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: CCS 2006: Proceedings of the 13thACM conference on Computer and communications security, pp. 89–98. ACM, New York (2006)

[10] Maji H K, Prabhakaran M, Rosutek M。Attribute-Based signatures LNCS 6558：Proc of Tocics in Cryptology CTRSA 2011． Berlin：Springer;2011:376-392