TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 9, September 2014, pp. 7034 ~ 7040
DOI: 10.11591/telkomnika.v12i9.5051

A New ID-based Threshold Ring Signcryption without Random Oracles

Hua Sun*, Yanqiang Ge
School of Computer and Information Engineering, Anyang Normal University,
Anyang 455000, China
*Corresponding author, E-mail:sh1227@163.com

Abstract

Signcryption is a cryptographic primitive which could provide authentication and confidentiality simultaneously with a computational cost lower than signing and encryption respectively, while the ring signcryption has anonymity in addition to authentication and confidentiality. In order to design an identity-based threshold ring signcryption, this paper presented an efficient identity-based threshold ring signcryption scheme without random oracles by means of secret sharing and bilinear pairing technique, and gave security analysis of the scheme. In the last, we proved this scheme satisfied indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message and identity attacks in terms of the hardness of DBDH problem and CDH problem.

Keywords: *threshold ring signcryption, bilinear pairing, computational Diffie-Hellman problem, decisional bilinear Diffie-Hellman problem, identity based cryptography*

1. Introduction

In 1984, the concept of ID-based cryptography was proposed by Shamir [1], which was utilized to solve the complex certificate management in traditional public key infrastructure. In ID-based cryptosystem, the user's public key is used to identify his identity information, while his private key is generated by PKG. The first efficient and practical ID-based encryption scheme was put forward by Boneh [2], whose work opened a new era for the ID-based cryptography, then many ID-based cryptographic schemes using bilinear pairings were subsequently presented [3, 4].

Confidentiality and authentication are two important security targets. They sometimes need to be achieved simultaneously, however the realization of the traditional method is not only large amount of calculation and efficiency is low. Signcryption was firstly proposed by Zheng [5], which could obtain the two goals at the same time, and the costs of computation and communication is much more lower.

In 2004, the first ID-based threshold signcryption scheme was proposed by Duan [6], while it used the method of sharing the master key of PKG, so it was easy to mak PKG a bottleneck in realization. In 2005, another ID-based threshold signcryption scheme was put forward by Peng [7], which overcame the shortcoming of the previous one, however it could not provide forward security. In 2008, the first provably secure threshold signcryption scheme was proposed by Li [8], and given the security proof in random oracle. However, it was pointed out that the scheme was not existential unforgeable against attacks in the paper [9].

Anonymity is another target in the applications of cryptography. Ring signcryption can not only realize confidentiality and authentication, but the anonymity. The first ID-based ring signcryption scheme was proposed by Huang [10], while its efficiency is too low. In 2008, another ID-based ring signcryption scheme was proposed by Zhang [11], however it was not secure against adaptive chosen ciphertext attacks. In the same year, efficient ID-based ring signature and ring signcryption schemes were proposed by Zhun [12], but it was secure against adaptive chosen plaintext attacks. Later on, Zhu [13] gave another ID-based ring signcryption scheme, but it was also not secure against adaptive chosen ciphertext attacks. In 2009, Sharmila [14] pointed out that the several existing ID-based ring signcryption schemes were unsafe, and proposed a new corresponding scheme.

Received November 4, 2013; Revised May 27, 2014; Accepted June 18, 2014

In 2011, an ID-based threshold ring signcryption scheme was proposed by Luo [15], and then another ID-based reception threshold ring signcryption scheme was proposed by Deng [16], while the schemes were all designed in the random oracle. At present, most existing ring signcryption schemes are proved to be secure in the random oracle, however it is difficult to construct corresponding instance in practice due to the hypothesis that the hash function would be viewed as completely randomly. So it is more meaningful to construct efficient and provably secure threshold ring signcryption scheme in the standard model.

In this paper, we put forward a new ID-based threshold ring signcryption (IBTRSC) scheme and gave the formal security proof. The paper is organized as follows. Some mathematical preliminaries are given in Section 2. Our proposed scheme is presented in Section 3. Security analysis of the scheme is given in Section 4. Finally, we conclude the survey in Section 5.

2. Preliminaries

2.1. Pairings

Let G, G_T be cyclic groups of prime order p and g be a generator of G. A bilinear pairing is a map $e: G \times G \to G_T$ that satisfies the following properties:

1. Bilinear: $e\left(g^a, g^b\right) = e(g,g)^{ab}$ for all $a, b \in Z_p$.
2. Non-degeneracy $e\left(g, g\right) \neq 1$.
3. Computability It is efficient to compute $e\left(u, v\right)$ for all $u, v \in G$.

2.2. Intractability Assumption

Definition 1 Computational Diffie-Hellman (CDH) problem Given a group G of prime p and elements $g^a, g^b \in G$, where $a, b \in {}_R Z_p^*$, the CDH problem is to compute g^{ab}.

Definition 2 Decisional Bilinear Diffie-Hellman (DBDH) problem Given a group G of prime p and elements $g^a, g^b, g^c \in G$, $h \in G_T$, where $a, b, c \in {}_R Z_p^*$, the DBDH problem is to decide whether $h = e(g,g)^{abc}$.

3. The Proposed IBTRSC Scheme

In this section, we propose an efficient ID-based threshold ring signcryption scheme without random oracles, which consists of the following algorithms:

Setup: Let G, G_T be groups of the same order p, g be a generator of G, the bilinear pairing is given as $e: G \times G \to G_T$. Two collision-resistant hash functions $H_u: \{0,1\}^* \to \{0.1\}^{n_u}$ and $H_m: \{0,1\}^* \to \{0.1\}^{n_m}$ are used to produce the bit strings of length n_u and n_m. PKG firstly choose $\sim \in {}_R Z_p$, compute $g_1 = g^a$, then choose $u' \in {}_R Z_p, g_2, m' \in {}_R G$, vector $\hat{U} = \left(u_i\right)$ of length n_u and vector $\hat{M} = \left(m_i\right)$ of n_m, where $u_i \in {}_R Z_p$ and $m_i \in_R G$. PKG set $z_1 = e\left(g_1, g_2\right)$ and $z_2 = e\left(g, g_2\right)$, so the system parameters are:

$$params = \left(G, G_T, e, g, g_1, g_2, u', \hat{U}, m', \hat{M}, H_u, H_m, z_1, z_2\right)$$ and the master private key is $msk = \sim$.

Private-Key Extract Given an identity information ID to PKG, let $u = H_u\left(ID\right)$ be the bit string of length n_m representing the identity ID, set $\Phi_{ID} \subseteq \{1, 2, \cdots, n_u\}$ be the set of index i such

that $u[i]=1$, where $u[i]$ is the ith bit of u. PKG choose $r \in_R Z_p$, compute $d_{ID}=(d_1,d_2)=\left(g_2^{\sim+r\left(u'+\sum_{i\in\Phi_{ID}}u_i\right)}, z_2^r\right)$, then PKG return $d_{ID}=(d_1,d_2)$ to user as his private key.

Signcrypt: Let $L=\{ID_1,...,ID_n\}$ be the set of n user identities for threshold ring signcryption. Suppose the actual t identities of signcrypter to be $\{ID_1,...,ID_t\}$, m is the message to be signcrypted, the receiver identity is ID_R. The threshold ring signcryption can be produced as follows:

1. Each signcrypter ID_i chooses $s_i \in_R Z_p$ as its sub-secret and a polynomial $f_i(x)=a_{i,0}+a_{i,1}x+\cdots+a_{i,t-1}x^{t-1}$ of degree $t-1$, whose coefficients are randomly choosed in Z_p. Let $s_i=a_{i,0}$, ID_i compute $C_{i,d}=g^{a_{i,d}}\ (d=0,1,..,t-1)$ and send them to other signcrypters. Then he computes $s_{i,j}=f_i(j)$ and sends it to other signcrypter $ID_j\ (j=1,2,..,t;\ j\neq i)$, and saves $s_{i,i}=f_i(i)$.

2. After ID_j receive $s_{i,j}$ from ID_i, he verifies the equation $g^{s_{i,j}}=\prod_{d=0}^{t-1}\left(c_{i,d}\right)^{j^d}$, and accepts it if the equation hold.

3. Each ID_i computes his secret $x_i=\sum_{j=1}^{t}s_{j,i}$.

4. Let the private key of each ID_i to be (d_{i1},d_{i2}), for $i\in\{1,2,...,t\}$. He computes $M=H_m(L,m)$, let $\mathrm{M}\subseteq\{1,2,\cdots,n_m\}$ be the set of index k such that $M[k]=1$. He chooses $r_i\in_R Z_p$, computes $\pm_{i1}=e(g_1,g_2)^{r_i}=z_1^{r_i}$, $\pm_{i2}=g^{r_i}$, $\pm_{i3}=r_i\left(u'+\sum_{j\in\Phi_{ID_R}}u_j\right)$, $\pm_{i4}=d_{i1}\left(m'\prod_{i\in\mathrm{M}}m_i\right)^{x_i\mathrm{¦}_i}$, $\pm_{i5}=g^{x_i\mathrm{¦}_i}$ $\pm_{i6}=d_{i2}$, and sents $(\pm_{i1},\pm_{i2},\pm_{i3},\pm_{i4},\pm_{i5},\pm_{i6})$ to other signcrypters, where $\mathrm{¦}_i=\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}\bmod p$ is the Lagrange coefficient.

5. Let $m\in G_T$ be the message to be signcrypted, each signcrypter choose $l_1,...,l_n\in_R Z_p$, compute $U_i=\left(u'+\sum_{j\in\Phi_{ID_i}}u_j\right)$ $i=1,...,n$ $R_1=\pm_{16}z_2^{l_1},...,R_t=\pm_{t6}z_2^{l_t},R_{t+1}=z_2^{l_{t+1}},...,R_n=z_2^{l_n}$. Let $\pm_1=\prod_{i=1}^{t}\pm_{i1}\cdot m$, $\pm_2=\prod_{i=1}^{t}\pm_{i2}$, $\pm_3=\sum_{i=1}^{t}\pm_{i3}$, $\pm_4=\prod_{i=1}^{t}\pm_{i4}\cdot g_2^{\sum_{i=1}^{n}l_i(U_i)}$, $\pm_5=\prod_{i=1}^{t}\pm_{i5}$, then the threshold ring signcryption will be $C=(\pm_1,...\pm_5,R_1,...R_n)$.

Unsigncrypt: Let (d_{R1},d_{R2}) be the private key of signcryption receiver ID_R, when receive the threshold ring signcryption C, he compute as follows:

1. ID_R first compute $m=\pm_1\cdot\left(d_{R2}\right)^{\pm_3}\cdot e\left(d_{R1},\pm_2\right)^{-1}$, then he computes $M=H_m(L,m)$, let M be the set of index k such that $M[k]=1$.

2. ID_R verify the equation $e(\pm_4, g) = e(g_1, g_2)^t \cdot e\left(m' \prod_{i \in M} m_i, \pm_5\right) \cdot \prod_{i=1}^{n} (R_i)^{U_i}$, accept it and output *True* if the equation holds; otherwise, output *False*.

4. Analysis of the Proposed IBTRSC Scheme

In this section, we will analyze our proposed scheme in detail.

4.1. Correctness

The verification of the signcryption is justified by the following equations:

(1) According to secret sharing technology, we have:

$$\sum_{i=1}^{t} x_i \lambda_i = \sum_{i=1}^{t} f_i(0) = \sum_{i=1}^{t} s_i$$

(2) After receive the threshold ring signcryption C, we have:

$$\pm_1 = \prod_{i=1}^{t} \pm_{i1} \cdot m = z_1^{\sum_{i=1}^{t} r_i} \cdot m,$$

$$\pm_2 = \prod_{i=1}^{t} \pm_{i2} = g^{\sum_{i=1}^{t} r_i},$$

$$\pm_3 = \sum_{i=1}^{t} \pm_{i3} = \sum_{i=1}^{t} r_i \cdot \left(u' + \sum_{j \in \Phi_{ID_R}} u_j\right),$$

$$\pm_4 = \prod_{i=1}^{t} \pm_{i4} \cdot g_2^{\sum_{i=1}^{n} l_i(U_i)} = g_2^{ta + \sum_{i=1}^{t} (r_{ID_i} + l_i) \cdot (U_i) + \sum_{i=t+1}^{n} l_i(U_i)} \cdot \left(m' \prod_{i \in M} m_i\right)^{\sum_{i=1}^{t} x_i \lambda_i},$$

$$\pm_5 = \prod_{i=1}^{t} \pm_{i5} = g^{\sum_{i=1}^{t} x_i \lambda_i}$$

So we can get:

$$\pm_1 \cdot (d_{R2})^{\pm_3} \cdot e(d_{R1}, \pm_2)^{-1} = e(g_1, g_2)^{\sum_{i=1}^{t} r_i} \cdot m \cdot \left(e(g, g_2)^{r_{ID_R}}\right)^{\sum_{i=1}^{t} r_i \cdot (U_{ID_R})} \cdot e\left(g_2^{a + r_{ID_R}(U_{ID_R})}, g^{\sum_{i=1}^{t} r_i}\right)^{-1} = m,$$

$$e(\pm_4, g) = e\left(g_2^{ta + \sum_{i=1}^{t} (r_{ID_i} + l_i) \cdot (U_i) + \sum_{i=t+1}^{n} l_i(U_i)} \left(m' \prod_{i \in M} m_i\right)^{\sum_{i=1}^{t} x_i \lambda_i}, g\right) = e\left(g, g_2^{ta}\right) \cdot e\left(\left(m' \prod_{i \in M} m_i\right)^{\sum_{i=1}^{t} x_i \lambda_i}, g\right) \cdot \prod_{i=1}^{n} (R_i)^{U_i}$$

$$= e(g_1, g_2)^t \cdot e\left(m' \prod_{i \in M} m_i, \pm_5\right) \cdot \prod_{i=1}^{n} (R_i)^{U_i}$$

4.2. Security Proofs

Theorem 1. Our IBTRSC scheme is IND-IDTRSC-CCA2 secure against adversary A under the assumption that the DBDH problem is intractable.

Proof. Let A be adversary against the proposed scheme, there will exist an algorithm B that can use A to solve the DBDH problem. B is given a DBDH instance (g, g^a, g^b, g^c, h), its goal is to decide whether $h = e(g, g)^{abc}$. B simulate the Setup algorithm of the scheme as follows:

B set $l_u = 2(q_e + q_s)$, $l_m = 2q_s$, where q_e is the number of private key query of A, and q_s is the number of signcrypt query of A, $l_u(n_u + 1) < p$, $l_m(n_m + 1) < p$. B randomly choose k_u, k_m, where $0 \le k_u \le n_u$ and $0 \le k_m \le n_m$. B choose $x' \in_R Z_{l_u}$ and vector $X = (x_i)$ of length n_u, where $x_i \in_R Z_{l_u}$; choose $z' \in_R Z_{l_m}$ and vector $Z = (z_k)$ of length n_m, where $z_k \in_R Z_{l_m}$; choose

$w' \in_R Z_p$ and vector $W = (w_i)$ of length n_m, where $w_i \in_R Z_p$. Then define three functions for $u = H_u(ID)$ and $M = H_m(L,m)$ as follows: $F(ID) = x' + \sum_{i \in \Phi} x_i - l_u k_u$, $K(M) = z' + \sum_{i \in \mathrm{M}} z_i - l_m k_m$, $L(M) = w' + \sum_{i \in \mathrm{M}} w_i$. Let $g_1 = g^a$, $g_2 = g^b$, $u' = x' - l_u k_u$, $u_i = x_i$, $1 \le i \le n_u$, $m' = g_2^{-l_m k_m + z'} g^{w'}$, $m_i = g_2^{z_i} g^{w_i}$, $1 \le i \le n_m$, we have $g_2^a = g^{ab}$ $F(ID) = u' + \sum_{i \in \Phi} u_i$ $m' \prod_{i \in \mathrm{M}} m_k = g_2^{K(M)} g^{L(M)}$, the system public parameters are $params = (G, G_T, e, g, g_1, g_2, u', \hat{U}, m', \hat{M}, H_u, H_m, z_1, z_2)$ and the master key is $msk = a$. Finally, B sends $params$ to A.

Phase 1: When the adversary A issue a number of queries, B response as follows:

Private-Key queries: When A make a query on the private key of input ID, if $F(ID) \neq 0 \bmod p$, B choose $r \in {}_R Z_p$, compute $d_{ID} = (d_1, d_2) = \left(g_1^{-1} (g g_2)^{r\left(u' + \sum_{i \in \Phi_{ID}} u_i\right)}, e\left(g g_2, g^{r\left(u' + \sum_{i \in \Phi_{ID}} u_i\right)} g_1^{-1} \right) \right)$ as the private key of A; if $F(ID) = 0 \bmod p$, B output FALL and abort the simulation.

Signcrypt queries: When A query a threshold ring signcryption on a group of n members specified by identities in $L = \{ID_1, ..., ID_n\}$, threshold value $t\,(t < n)$, message m, the actual signcrypter $ID_i\,(i = 1, ...t)$ and the receiver identity ID_R, B first compute $M = H_m(L,m)$, and then produce the corresponding signcryption C as follows:

(1) B choose $s, a_0, a_1, ..., a_{t-1} \in {}_R Z_p$, a polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$ of degree $t-1$, where $s = a_0$.

(2) For each actual signcrypter $ID_i\,(i = 1, ...t)$, if $F(ID_i) \neq 0 \bmod p$, B can construct its private key by the same method in private-key query, then compute its secret $x_i = f(i)$, and finally produce the corresponding threshold ring signcryption C.

(3) If the condition $F(ID_i) \neq 0 \bmod p, i = 1, ...t$ is not satisfied, and we have $K(M) \neq 0 \bmod p$, then B choose $r, r_1, ..., r_n, r_m \in {}_R Z_p$, and compute as follows:

$$\pm_1 = e(g_1, g_2)^r \cdot m,$$

$$\pm_2 = g^r,$$

$$\pm_3 = r\left(u' + \sum_{j \in \Phi_{ID_R}} u_j \right),$$

$$\pm_4 = g_2^{\sum_{i=1}^n r_i(U_i)} g_1^{-tL(M)/K(M)} \left(m' \prod_{i \in \mathrm{M}} m_i \right)^{r_m} = g_2^{ta + \sum_{i=1}^n r_i(U_i)} \left(m' \prod_{i \in \mathrm{M}} m_i \right)^{\tilde{r}_m},$$

$$\pm_5 = g_1^{-t/K(M)} g^{r_m} = g^{\tilde{r}_m},$$

$$R_1 = z_2^{r_1}, ..., R_n = z_2^{r_n}, \text{ where } \tilde{r}_m = r_m - t\,a / K(M).$$

We can see that $C = (\pm_1, ...\pm_5, R_1, ...R_n)$ is a valid threshold ring signcryption. If $K(M) = 0 \bmod p$, B output FALL and abort the simulation.

Unsigncrypt queries: When A query an unsigncryption on identities L receiver identity ID_R and the ciphertext C, B first obtain the private key d_{ID_R} of ID_R, B then execute unsigncrypt algorithm to output message *m* and return.

Challenge Phase: A choose two distinct messages m_0 and m_1 of equal length, identities $L^* = \{ID_1^*, ..., ID_n^*\}$ and receiver identity ID_R^*, then send them to B. If A has queried the private key of ID_R^*, B output FALL and abort the simulation; otherwise, B randomly choose $b \in (0,1)$, if $K(M_b) = 0 \bmod p$, B output FALL and abort the simulation, if $F(ID_R^*) \neq 0 \bmod p$, B output FALL and abort the simulation. Otherwise, B choose $r_1, ..., r_n, r_m \in {}_R Z_P$, and compute as follows:

$$\pm_1^* = h \cdot m_b ,$$

$$\pm_2^* = g^c ,$$

$$\pm_3^* = c\left(u' + \sum_{j \in \Phi_{ID_R^*}} u_j\right) = cF(ID_R^*),$$

$$\pm_4^* = g_2^{\sum_{i=1}^n r_i(U_i)} g_1^{-tL(M_b)/K(M_b)} \left(m' \prod_{i \in M} m_i\right)^{r_m} = g_2^{ta + \sum_{i=1}^n r_i(U_i)} \left(m' \prod_{i \in M} m_i\right)^{\tilde{r}_m},$$

$$\pm_5^* = g_1^{-t/K(M_b)} g^{r_m} = g^{\tilde{r}_m} ,$$

$$R_1^* = z_2^{r_1}, ..., R_2^* = z_2^{r_n} , \text{ where } \tilde{r}_m = r_m - t\,a / K(M_b) .$$

If $h = e(g,g)^{abc}$, we can see that $C^* = (\pm_1^*, ..\pm_5^*, R_1^*, ...R_2^*)$ is a valid threshold ring signcryption.

Phase 2: A may issue a number of queries as in Phase 1, but he can't make query on the private key of ID_R^* and the unsigncryption on C^*.

Guess Phase: A output a guess b' for b. If $b = b'$, B output $h = e(g,g)^{abc}$ as the solution of DBDH problem; otherwise, B output FALL.

Theorem 2. Our IBTRSC scheme is EUF-IDTRSC-CMIA secure against adversary A under the assumption that the CDH problem is intractable.

Proof. Let A be adversary against the proposed scheme, there will exist an algorithm B that can use A to solve the CDH problem. B is given a CDH instance (g, g^a, g^b), its goal is to compute g^{ab}. B then construct the system parameters as in Theorem 1 and send *params* to A.

Query Phase: A can issue a number of queries as in Theorem 1, and B make the same responses.

Forgery Phase: Finally, A output the forgery threshold ring signcryption C^* on identities $L^* = \{ID_1^*, ..., ID_n^*\}$, threshold value t, message m^*, and the receiver identity ID_R^*. If B do not abort the simulation in the query phase, and the following two conditions:

1) $F(ID_i^*) = 0 \bmod p$, for all $i \in (1, ..., n)$,

2) $K(M^*) = 0 \bmod p$, where $M^* = H_m(L, m^*)$

Would be satisfied simultaneously, then B can compute:

$$\left(\frac{\pm_4^*}{\left(\pm_5^*\right)^{L\left(M^*\right)}}\right)^{1/t} = \left(\frac{g_2^{ta+\sum_{i=1}^{*} r_i(U_i)}\left(m'\prod_{i\in M} m_i\right)^{r_m^*}}{g^{r_m^* \cdot L\left(M^*\right)}}\right)^{1/t} = \left(g_2^{ta}\right)^{1/t} = g_2^{a} = g^{ab},$$

Which is the solution of the CDH problem.

5. Conclusion

In this paper, we present a new threshold ring signcrypiton scheme based on secret sharing. As far as we know, most existing ID-based ring signcryption schemes were proved to be secure in the random oracle, while we construct the corresponding ID-based threshold ring signcryption scheme without random oracle. Then we prove the proposed scheme to be secure against adaptive chosen-ciphertext attack and adaptive chosen message and identity attack under the DBDH and CDH difficult problem, so the proposed scheme is safe and reliable.

Acknowledgements

This work is supported by National Nature Science Foundation of China under Grant (No. 61170244, No. U1204402).

References

[1] Adi Shamir. *Identity-based cryptosystems and signature schemes*. Proceedings of Crypto 1984, volume 196 of LNCS, 47-53.
[2] Dan Boneh, Matt Franklin. *Identity-based encryption from the Weil pairing.* Proceedings of Crypto 2001, volume 2139 of LNCS, 213-229.
[3] Florian Hess. *Efficient identity based signature schemes based on pairings.* Proceedings of SAC 2002, volume 2595 of LNCS, 310-324.
[4] Kenneth G Paterson, Jacob CN Schuldt. *Efficient identity-based signatures secure in the standard model*. Proceedings of ACISP. 2006; 4058 of LNCS: 207-222.
[5] Zheng Yuliang. *Digital signcryption or how to achieve cost (signature & encryption) <<cost (signature) + cost (encryption).* Advances in Cryptology-Crypto. 1997; 1294 of LNCS, Springer-Verlag: 165-179.
[6] SS Duan, ZF Cao, RX Lu. *Robust id-based threshold signcryption scheme from pairings.* proceedings of the 3rd international conference on information security, ACM, 2004, pp.33-37.
[7] CG Peng, X Li. *An identity-based threshold signcryption scheme with semantic security*. Proceedings of CIS. 2005; 3802 of LNCS, Springer-Verlag: 173-179.
[8] FG Li, Y Yu. *An efficient and provably secure id-based threshold signcryption scheme*. Proceedings of ICCCAS 2008, IEEE Press. 2008: 488-492.
[9] ZC Zhu, YQ Zhang, FJ Wang. *The analysis of an efficient and provably secure id-based threshold signcryption scheme and its secure version*. Proceedings of the second international conference on provable security. 2008; 5324 of LNCS, Springer-Verlag: 210-225.
[10] Huang Xin-yi, Susilo W, Mu Yi et al. *Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world*. Proceedings of the 19th international conference on advanced information networking and application. 2005; 2: 649-654.
[11] MW Zhang, B Yang, S L Zhu, et al. *Efficient secret authenticatable anonymous signcryption scheme with identity privacy.* Proceedings of IEEE ISI 2008; 5075 of LNCS, Springer-Verlag: 126-137.
[12] L J Zhun, F T Zhang. *Efficient id-based ring signature and ring signcryption schemes*. Proceedings of CIS 2008, IEEE Press, 2008; 303-307.
[13] ZC Zhu, YQ Zhang, FJ Wang. An efficient and provable secure identity-based ring signcryption scheme. *Computer Standards & Interfaces*. 2009; 31: 1092-1097.
[14] Sharmila Deva Selvi S, Sree Vivek S, Pandu Rangan C. *On the security of identity based ring signcryption schemes.* Proceedings of the 12th international conference on information security. 2009; 5735 of LNCS, Springer-Verlag: 310-325.
[15] DW Luo, MX He, X Li. ID-based threshold ring signcryption scheme. *Computer Engineering and Applications*. 2011; 47(33): 65-67.
[16] LZ Deng, JW Zeng. Identity based reception threshold ring signcryption scheme*. Journal of Xiamen University (Natural Science)*. 2012; 51(4): 660-665.