Journal of Theoretical and Applied Information Technology
20th April 2013. Vol. 50 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DYNAMIC GROUP SIGNATURE SCHEME BASED ON NON-INTERACTIVE PROOF

[1]XIE YONG, [1]ZHANG YILAI, [1]LIU MING
[1]Jingdezhen Ceramic Institute Jingdezhen, China
E-mail: Xieyongdian@163.com

ABSTRACT

Combined with identity-based signature technology and non-interactive proof, a dynamic group signature scheme was built based on the standard group scheme model. This scheme overcame the shortcoming of static property of standard scheme and was of strong Non-frameability. New members could dynamically join in group without updating the group public key and group manager could not forge any member's signature. By the performance and safety analysis of the scheme, it could prove that, this scheme was higher performance than other similar group signature schemes, and the correctness, anti-CPA attack complete anonymity and full traceability of this scheme had satisfied the secure request of standard scheme. Therefore the scheme is of preferable applicability.

Keywords: *Group Signature, Full Anonymity, Traceability, Non-interactive Proof*

1. INTRODUCTION

Group signature is a very special class of digital signature, where each signer of the group can sign messages anonymously on behalf of the group. And the group is managed by a trusted group authority, which is responsible for group members' composite and updating, and verifies the identity of the signer according to certain pre-set protocol in the event of a dispute. In 1991, D.Chaum and Heyst.E.V [1] first proposed the concept of group signature. After that, the group signature has aroused extensive attention of scholars from various countries; many group signature schemes [2]-[9] were proposed and widely used in the field of electronic auction, key escrow, electronic money, electronic voting and other e-commences.

In 2003, Bellare Miccianeio and Warinschi firstly proposed a provable security scheme for dynamic group, with the generalized non-interactive zero-knowledge proof technology, which was inefficient. Considering practicality, group signature schemes under the standard model must be realized by composite number rank group. Bellare, Shi, Zang [10] proposed the standard model of dynamic group signature scheme (BSZ model), pointed out that a secure dynamic group signature scheme should be correct and satisfy three security requirements. Boyen proposed a group signature scheme by composite number rank group [11] with zero-knowledge proof technology. It encrypted the identity of the signer as part of the signature and the group public key of scheme was logarithmic relationship with the number of members, but the anonymity of the scheme barely resist plaintext attack. A year later, Boyen improved group signature scheme [12], which consisted of six numbers of composite number rank group, group public key and the message space into a linear relationship. This scheme further enhanced the anti-plaintext attack, but its efficiency was still undesirable.

Combined with identity-based signature technology and non-interactive proof [13], we proposed a new group signature scheme under standard model. This scheme overcame the shortcomings of application only on static groups with new member dynamically joined into group, and it also could prove the signature legitimacy without interaction and had a higher efficiency of the implementation.

In this paper, section 2 presents the related theory. In section 3, we propose a dynamic group signature scheme based on non-interactive proof, and present its construction method. Section 4 presents a comparative experiment among our scheme and other group signature schemes, result of which is shown our scheme has higher performance. In section 5 the result of security analysis shows our scheme has a strong security. Last section summarizes the work of this paper.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. RELATED THEORIES

2.1 Definition of group signature model

A group signature scheme, defined as GS = (Initial, Join, Sign, Verify, Open), composed by the following polynomial-time algorithms:

(1) Initial: A probabilistic algorithm, the group manager implemented the algorithm used to generate the initial public and group private key of group, and generate a corresponding system parameters.

(2) Join: A new user asked group manager for adding into group under interaction protocols. New members would complete legal identity register and obtain a secret key and a membership certificate when the end of the implementation of the protocols.

(3) Sign: sing is a probabilistic algorithm between users and group members, through which group members could sign on message M by a private key and membership certificate.

(4) Verify: it is a deterministic algorithm, which used to authenticate the message signature is a valid group signatures.

(5) Open: it is a deterministic algorithm, used to extract the membership certificate written by Sign function to reveal the true identity of the signer.

2.2 The security needs of group signature

A good group signature scheme should meet the following safety requirements:

(1) Correct: A group signature of legal group members generated by the function Sign would be able to pass verifier's verification.

(2) Unforgeability: It is computationally impossible for non-group members to produce a signature by the group authentication algorithm. In other words, the only legal group members could produce a valid group signature.

(3) Anonymity: Any messages of group signature could not be calculated by anyone in addition to the group manager.

(4) Unllkability: It was hard to confirm two group signatures whether coming from the same group.

(5) Traceability: The true identity of the signer can be revealed by group manager with its correct signature.

(6)Coalition-resistance: Any number of group members' collusion or the group manager's collusion with others could not forge the signature of the other group members.

(7) Non-frameability: Any members of group or the group manager could not sign as the other group members, and group members would not be responsible for others' signature.

2.3 The formal definition of security attributes

Bellare proposed the formal definition of security attributes of group signature through summing up the above security nature [14]. It summarized the core security features of group signatures as Full-Anonymity and Full-Traceability, and pointed out that no correlation can be derived from completely anonymous, and to meet the Full-Traceability must have non-frameability, anti-incrimination and anti joint strike.

Definition 1: We denote the advantage of adversary A in breaking the full-anonymity of *GS* by

$$Adv_{GS,A}^{trace}(k,n) = \Pr\left[Exp_{GS,a}^{anon-1}(k,n)=1\right] - \Pr\left[Exp_{GS,a}^{anon-0}(k,n)=1\right] \quad (1)$$

We consider that a group signature scheme is *fully-anonymous* if for any polynomial-time adversary *A*, the two-argument function $\mathrm{A}dv_{gs,\mathrm{A}}^{anon-1}(\cdot,\cdot)$ is negligible in the sense of negligibility of two-argument functions defined at the beginning of this section.

Definition 2: We define the advantage of adversary *A* in defeating full-traceability of the group signature scheme *GS* by:

$$Adv_{GS,A}^{trace}(k,n) = \Pr\left[Exp_{GS,a}^{trace}(k,n)=1\right] \quad (2)$$

If the two-argument function $\mathrm{A}dv_{GS,\mathrm{A}}^{anon-1}(\cdot,\cdot)$ could be negligible for any polynomial-time adversary *A*, we consider *GS* is *fully-traceable.*

Let us now proceed to the formalization. To any group signature scheme *GS = (GKg, Gsig,GVf, Open)*, adversary A and bit b we associate the first experiment given in Figure 1and Figure 2. Here, *A* is an adversary that functions in two stages, a *choose* stage and a guess stage. In the choose stage *A* takes as input the group members secret keys, *gsk*, together with the group public key *gpk*. During this stage, it can also query the opening oracle Open (*gmsk,*) on group signatures of his choice, and it is required that at the end of the stage *A* outputs two valid identities $1 < i_0, i_1 < n$, and a message *m*. The adversary also outputs some state information to be used in the second stage of the attack. In the second stage, the adversary is given

Journal of Theoretical and Applied Information Technology
20th April 2013. Vol. 50 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the state information, and a signature on *m* produced using the secret key of one of the two users' i_0, *i1*, chosen at random. The goal is to guess which of the two secret keys was used. The adversary can still query the opening oracle, but not on the challenge signature.

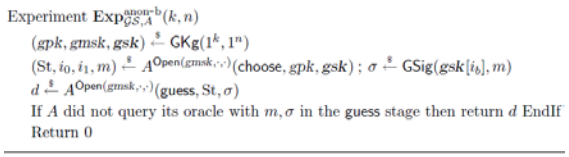

Fig. 1. Experiments of full-anonymity definition

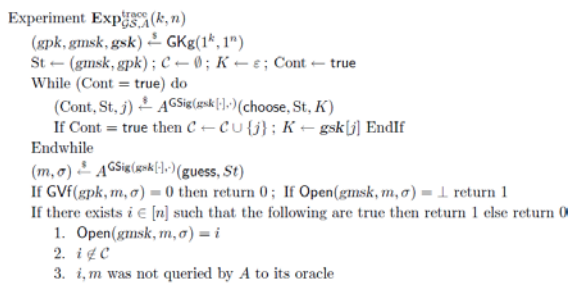

Fig. 2. Experiments of full-traceability definition

2.4 Complexity assumptions

The security of the group signature scheme is generally based on two types of passwords assumptions, which are computational Diffie-Hellman assumption and subgroup judgment assumption in the G_p.

(1) The Computational Diffie-Hellman assumption (CDH) in G_p [15]: the number of elements as the aggregate number of n-order group G, n = pq, to set (g, g^a, g^b) ∈ G, wherein a, b ∈ Z_p, p is a prime number to calculate gab. No (t, qr, ε) adversary *A* questions q_r times within the time t, at least a probability ε to calculation gab, so adversary A has the advantage ε. If the probability Pr [A (g, g^a, g^b) =g^{ab}] ≥ ε. If G_p in CDH problem is difficult, then G in the CDH problem is also difficult.

(2) Subgroup judgment assumption [16]: Set group G and GT, the order of group G: n = pg, bilinear map e: G×G→GT, no polynomial-time algorithm A can ignore theSD-Adv_A solvable subgroup decision problem advantage, which the SD-Adv_A defined as:

$$\text{SD - Adv}_A = \left|\Pr[A(n, F, G_T, e, x) = 1] - \Pr[A(n, F, G_T, e, x^q) = 1]\right| \quad (3)$$

3. A DYNAMIC GROUP SIGNATURE SCHEME BASED ON NON-INTERACTIVE PROOF

In our group signature scheme, P is set as the participant of the group signer, GA is set of Manager. $H_u : \{0,1\}* \to \{0,1\}^{n_u}$ was non-collision Hash function used to generate identity and message with length of n_u. $H_m : \{0,1\}* \to \{0,1\}^{n_m}$ was non-collision Hash function used to generate identity and message with length of n_m. The whole signature specific process is as follows:

3.1 The initialization of system-initial ()

Group manager firstly select n = p*q, where p and q are two random prime numbers and their bit length is bigger than k. Let G be a bilinear group order of the composite number n. Let G_p and G_q be subgroup of G and their orders respectively are p and q. and then select number of generator g ∈ G and h ∈ G_q, randomly select from a secret value $\alpha \leftarrow_R Z_p$, and set $g_1 \leftarrow_R G$, calculate $A = e(g - g_1)^{\alpha}$. The next step randomly select group number $u', m' \leftarrow_R G$, select vector U= (u_i) and M= (m_i) of which length respectively are n_u and n_m. Finally, the group manager released the following group public key:

$$PK = (n, G, GT, e, g, h, g1, u', m', U, M, A = e(g, g1)^{\alpha}) \quad (4)$$

The master key MK and the tracer's key TK respectively are: MK=g_a, TK=q.

3.2 Members join- Join (PK, MP, ID)

Let bit string ID with length was n_u represented user identity. ID[i] represented the i-th bit of ID. Let U ⊂ {1, ⋯, nu} was collection about all subscripts of user ID.

At first, *user [ι]* would apply to become a member of the group, it would interact with GA to complete user authentication:

(1) *User [ι]* random selected $y_\iota, k \in RZ_P^*$, y_ι kept confidentiality of GA, and calculated $P_\iota = h^{y_\iota}$ and $Q_\iota = e(h, g)^k$ that sent to GA.

(2) GA select $c_\iota \in RZ_P^*$ for responding to User [ι].

(3) User [ι] calculated $s_\iota = k + c_\iota y_\iota$ and sent s_ι to GA.

(4) GA verified the equation $e(h, g)^{s_\iota} = Q_\iota \cdot e(p_\iota, g)^{c_\iota}$, if it was true, then

Journal of Theoretical and Applied Information Technology
20th April 2013. Vol. 50 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

GA sent a secret identifier $d_i \in Z_n$ and certification to user [ι], stored user identity and the corresponding secret identifier in the user list.

(5) User [ι]verified the equation as following after received certification(K_1,K_2).

$$e(K_1, g) = A \cdot e(g, h)^{y_\iota} \cdot e\left(u' \prod_{i \in u} u_\iota, K_2\right) \quad (5)$$

If the equation was true, it showed that the confirmed certification was valid. User [ι] would keep (K_1, K_2, y_ι) as signature key gsk[ι].

During registration process, signature key is composed of two parts by certificate released by GA and the user's private key, which could prevent GA forgery legitimate signature of User [ι].

3.3 signature stage- Sign (PK,gsk[ι],M)

Let *M[j]* represent the j-th bit of message $M \in \{0,1\}^{n_m}$, let $M' \subset \{1, \cdots, n_m\}$ represent subset of M[j] =1 in M. To stamp signature on message M, User [ι] took its signature key gsk[ι] and a random $r \in Z_n$ to generate two hierarchical signature, as following:

$$S = (S_1, S_2, S_3) = \left(g_1^a h^r \left(u' \prod_{i \in u} u_\iota\right)^{d_\iota} \left(m' \prod_{i \in M} m_\iota\right)^r, g^{d_\iota}, g_r\right) \quad (6)$$

Then user [ι] selected random exponent t_1, t_2, t_3 $\in Z_n$, and blinded signature S, and calculate:

$$\pi = g^{t_1} \cdot g^{y_\iota} \cdot \left(u' \prod_{i \in u} u_j\right)^{-t_1} \left(m' \prod_{i \in M} m_j\right)^{-t_3} \quad (7)$$

The final signature of user [ι] was $\delta = (\delta_1, \delta_2, \delta_3, \pi)$.

3.4 verification stage- Verify (PK, M, ID, δ)

A group signature was verified by calculating the following:

$$T = A^{-1} \cdot e(\delta_1, g) \cdot e\left(\delta_2, u' \prod_{i \in u} u_j\right)^{-1} \cdot \left(\delta_3, m' \prod_{i \in M} m_j\right)^{-1} \quad (8)$$

If T was equal to $e(h, \pi)$, this group signature can be identified as a valid group signature.

3.5 Open stage-Open (δ, TK)

Assuming that a valid group signature has passed the validation stage, it is a valid group signature. The signature tracers firstly parse δ as $\delta = (\delta_1, \delta_2, \delta_3, \pi)$, then use track-key TK calculated δ_2^q, next, verify each identity $d_i (0 \le i < 2^k)$, stored in the user list, by testing $(\delta_2)^q$ equaling to $(g^{d_i})^q$. If the existence of such d_i to comply with the above formula, system outputs the corresponding identity ID.

4. SCHEME PERFORMANCE ANALYSIS

There are three main indicators in the evaluation of a group signature performance [17]: group signature length, bilinear computation and length of public parameters in validation stage. The signature length is measured by the number of composite number rank group elements; the open parameter length is measured by the number of groups' elements to compose the parameters. The results of performance of our scheme, the literature [11], the literature [12], is shown in Table I.

Table I Performance Comparison

scheme	group signature length	bilinear computation	length of public parameters
literature [11]	2k+3	2k+3	$G_q \times G^{k+n_m+4} \times G_T$
literature [12]	6	6	$G_q \times G^{n_m+4} \times G_T$
Our scheme	4	4	$G_q \times G^{n_u+n_m+4} \times G_T$

In table I, n_u is user identity; n_m is the bit length of messages. Assuming all scheme in table 1 had reached the level of security of the RSA-1024, as shown in table 1, our scheme was better than the other two on the signature length and the bilinear computation in verification stage. Our scheme consists of four group elements, and only spent 4 times bilinear computing in signature stage. Our signature length and bilinear computation spent only 67% of literature [11]. Though length of public parameters in our scheme is bigger than literature [11], but the public parameters is not different very largely because n_u is far less than n_m and n_m is far less than λ.

5. SECURITY ANALYSIS

5.1 Correctness analysis

When the certifier got a group signature, it would calculate:

$$T = A^{-1} \cdot e(\delta_1, g) . e\left(\delta_2, u' \prod_{i \in u} u_j\right)^{-1} \cdot e\left(\delta_3, m' \prod_{i \in M} m_j\right)^{-1}$$

$$= A^{-1} \cdot e(g_1, g)^a . e\left(h, g^{y_\iota}\right) \cdot e\left(u' \prod_{i \in u} u_j, g^{d_\iota}\right) \cdot e\left(m' \prod_{i \in M} m_j, g^r\right) \cdot e\left(h, g^{t_\iota}\right) \cdot$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$e\left(u'\prod_{i\in u}u_j, g^{d_t}\right)^{-1}\cdot e\left(u'\prod_{i\in u}u_j, h^{-t_2}\right)\cdot e\left(m'\prod_{i\in M}m_j, g^{d}\right)^{-1}\cdot e\left(m'\prod_{i\in M}m_j, h^{-t_3}\right)$$

$$= e(h,\pi)$$

Therefore, as long as the signature was valid, then it must pass verification of the certifier. In addition, because $h\in G_q$, $(\delta_2)^q=(g^{d_t}h^{t_2})^q=(g^{d_t})^q$, that was a valid signature can also be opened correctly. So our scheme met the requirement of correctness.

5.2 Full anonymous analysis

Completely anonymous analysis in anti-CPA attack, we defined two *games*: H_0 and H_1. H_0 was the anonymity *game* of actual group signature, the distinction between H_0 and H_1, is that the public key *h* is randomly selected from the group *G*, not the group G_q.

Let algorithm A_g execute subgroup judgment problem *game* by challenge (n, G, G_Γ, e, ω). A_g would set $h=\omega$ and generate the remaining part of group public key, then send a complete public key to the adversary A during time *t'*, and execute anonymity *game*. If ω was selected at random from G_q, then execution usually was usually anonymity game *H0*; Otherwise, ω was randomly select from *G*, execution was H_1.

If *A* gave two identities ID_0, ID_1 and message *M*, *Ag* would verify the signer identity by indistinguishable *challenge* on the *M*. If A was true, Ag outputted *b=1* to show $\omega\in G_p$, else b=0 to show $\omega\in G$. Supposed A_g runtime *t*= *t'* , because $\Pr[\omega\in G]=\Pr[\omega\cup G_p]=1/2$, and $Adv_\beta<\varepsilon$, with the same analysis method in the literature [18], we could get $Adv_A - Adv_{A,H_1} = 2Adv_\beta < 2\varepsilon$.

That is, both H_0 and H_1 game were indistinguishable, unless the subgroup judgment assumption was easy. Because of $\delta_1=S\cdot h^{t_1}$, $\delta_2=S\cdot h^{t_2}$, $\delta_3=S\cdot h^{t_3}$, and if *h* came from group *G*, $\delta_1,\delta_2,\delta_3$ were well blind, the signature δ is statistics for identity d_t independent from signer from the aspect of adversary. To sum up, we could get our signature scheme with full anti-CPA anonymous attack.

5.3 Full traceability analysis

The proof of Full traceability of our group signature scheme can be simplified by the unforgeability proof of existence with tow level signatures. Adversary *A* was assumed existing which had win superiority ε on the signer identity tracing game during time *t*. We construct a simulator SM for this adversary A. Set SM group order decomposition n=pq. Definition of G_p, G_q, U and M were the same with algorithm, then defined G_{Tp}, G_{Tq} respectively were order *p* of G_T and group order of *q*. If A could solve CDH problem, SM must be able to challenger of A. A could receive public parameter from its challenger as following:

$$\tilde{PK}=\left(\tilde{g},\tilde{g}_1=\tilde{g}^a,\tilde{u}',\tilde{U}=(u_i),\tilde{m}',\tilde{M}=(m_i),\tilde{A}=e(\tilde{g},\tilde{g}_1)^a\right) \quad (9)$$

Then the simulator randomly selected $(f,h,\xi',\xi_1,\cdots,\xi_{n_u},\eta',\eta_1,\eta_2,\cdots\eta_{n_m})\in G_q^{n_u+n_m+4}$ and random index, $\beta\in Z_q$, and published group public key:

$$PK=\left(g=\tilde{g}f, u'=\tilde{u}'\xi', U=(u_i,\xi_i), m'=\tilde{m}'\eta', M=(m_i,\eta_i)\right) \quad (10)$$

SM would send key TK to the adversary *A*. When *A* quested the user about private key, at first *A* would quested his challenger about the ID concerned user identity in the first layer signature, and generated the requested private key as following:

$$K=\left(K_1=\tilde{d}_1\cdot\left(\xi'\prod_{i\in}\xi_i\right)^{r_t}\cdot f^{\beta}, K_2=\tilde{d}_2\cdot f^{r_t}\right) \quad (11)$$

Because of $\tilde{g}\in G_p$ and $h\in G_p$, so if $e(\tilde{g},h)=1$ in G_T, it would verify that this private key lined with of the algorithm specification. When SM received requisition of signature on message M from A, it would quest A about a signature and then received response signature S. If $S=(s1,s2,s3)\in G_p^3$, then it would take out lasting value and select a random value $r\in Z_q$ and generated non-blind signature as flowing:

$$S=\left(S_1\cdot\left(\xi'\prod_{i\in U}\xi_i\right)^{r_t}\cdot\left(\eta'\prod_{j\in U}\eta_j\right)^{r}\cdot f^{\beta}\right) \quad (12)$$

SM converted S into blind signature by the way of user's signature, and constructed NIZK proof [19], then sent final signature to *A*.

At last A sent a forge signature δ to simulator about message M^*. If δ was not meet validation equation, *SM* would announce A forged failed, or *SM* began to track the identity ID^*.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Each adversary A previous questioned identities of the private key ID_i, SM would verify that whether $(\delta_2)^q$ and γ_{ID_i} were equal. If they were equal, SM set $ID^*=ID_i$ as tracked identity. If ID_i private key or message M^* signature of ID^* had been questioned by A before, SM aborted, or SM successfully forged. Then SM would continue to deal with his forged. Let $\delta \in Z_n$ and $\delta \equiv 0(\text{mod } q)$, $\delta \equiv 0(\text{mod } p)$, we would obtain:

$$e(\delta_1, g)^{\delta} \cdot e\left(\delta_2, u' \prod_{i \in U} u_i\right)^{-\delta} \cdot e\left(\delta_3, m' \prod_{j \in U} m_j\right)^{-\delta} = \tilde{A}$$

In the order subgroup, at this point, there is always

$$e(\sigma_1^{\delta}, g) \cdot e\left(\sigma_2^{-\delta}, u' \prod_{i \in U} u_i\right) \cdot e\left(\sigma_3^{-\delta}, m' \prod_{j \in M} m_j\right) = \tilde{A}$$

It was said that $\sigma^* = (\sigma_1^{\delta}, \sigma_2^{\delta}, \sigma_3^{\delta})$ meet with signature verification equation of message M^* given by uncertain ID^*. This shows that no matter who is the adversary, the simulator *SM* can win the game between with *challenger*.

6. CONCLUSIONS

Group signature allows any member of the group to do anonymous signature on behalf of the group. Meanwhile, each members of group should be able to autonomously join in or leave the group. Anonymity and no-correlation of group signature are the significant difference from general signatures.

A dynamic group signature scheme based on non-interactive proof was proposed in this paper, combined with identity-based signature technology and non-interactive proof to overcome the static shortcomings of the group, allowing the group members to join dynamically without updating the group public key. In the scheme, even the group manager could not forge a valid signature of any group members; the group signature length is fixed, composed of four elements within composite number rank group; and it only required four times bilinear computing in the signature verification process. Compared with the same type of group signature schemes, our scheme takes on higher performance, and the correctness, anti-CPA attack completely anonymous and full traceability of this scheme had satisfied the secure request of BSZ model. Therefore the scheme is of preferable applicability. Our scheme has better execution efficiency than literature [12], but it is still not ideal. So our further work is to improve the execution efficiency of our scheme.

ACKNOWLEDGMENT

This work is completed under the support of the National Science & Technology Pillar Program (No. 2012BAH25F02).

REFRENCES:

[1] T.S. Bhatti, R.C. Bansal, and D.P. Kothari, "Reactive Power Control of Isolated Hybrid Power Systems", *Proceedings of International Conference on Computer Application in Electrical Engineering Recent Advances (CERA)*, Indian Institute of Technology Roorkee (India), February 21-23, 2002, pp. 626-632.

[2] CHAUM D, HEYST E V. Group Signatures [A].*Advances in Eurocrypt'91, (LNCS 547)* [C]. Berlin: Springer-Verlag, 1991.257-265.

[3] PETERSEN H. How to convert any distal signature scheme into a group signature scheme [A]*Security Protocols Workshop*[C]. Berlin: Springer-Verlag, 1997.465-479.

[4] CAMENISH J, MICHELS M. Separability and eficiency for generic group signature schemes [A]. *Advances in Crypto, 99*[C]. Berlin: Springer-Verlag, 1999. 413-430.

[5] XIA S, YOU J. A group signature schemes with strong reparability [J].*Journal of Systems and Software*, 2002, 60(3):177-182.

[6] MA H.R, Wu YX.An ID-based short group signature scheme [J].*Journal of Qingdao university* (Chinese), 2012 25 (3):57-60.

[7] D.Boneh, H.Shacham.Group signatures with verifier-local revocation [A]. *ACM-CCS 2004*. ACM Press, 2004:168-177.

[8] ZHANG Yue-yu, LI Hui,WANG Yu-min. Secure electronic auction scheme based on the group signature[J]. *Journal of Xidian University* (in Chinese), 2010, 4: 37-42.

[9] Chen Hu, Zhu Changjie,Song Rushun. Efficient Certificateless Signature and Group Signature Schemes [J]. *Journal of Computer Research and Development* (Chinese), 2010, 27(9):1321-1327.

[10] LI Ji-guo,SUN Gang,ZHANG Yi-chen ,Provably Secure Group Signature Scheme with Verifier-Local Revocation in the Standard Model[J]. *Acta Electronica Sinica*, 2011 39(7):1317-1319.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[11] M. Bellare, H. Shi, Zang. Foundations of group signatures: The case of dynamic groups[C]. *Proc of the Cryptographers' Track at the RSA Conference*. Berlin: Springer-Verlag, 2005: 136-153.

[12] X.Boye, B. Waters. Compact group signatures without random oraele. *Eurocrypt 2006, LNCS4004*. Berlin: Springer-Verlag, 2006:427-444.

[13] X.Boyen, B. Waters.Full-domain subgroup hiding and constant-size group signatures. *PKC 2007, LNCS 4450*.Berlin: Springer-Verlag, 2007: l-15.

[14] S Wei-min. Enhanced Identity-based Deniable Authentication Protocol [J] *Journal of Beijing University of Technology*, 2011, 37 (3):477-483.

[15] M.Bellare,D. Mieeiancio. Foundations of group signatures: formal definitions, simplified requiremenis, and a construction based on general assumption. *EUROCRPYT 2003*. Berlin: Springer-Verlag, 2003:614-629.

[16] ROY A, DATTA A, MITCHELL J C. Formal proofs of cryptographic security of Diffie-Hellman-based protocols [A].T*rustworthy Global Computing*[C]. Barcelona, Spain, 2008:312-329.

[17] D. Boneh, E. Goh, K.Nissim. Evaluating 2-DNF formulas on ciphertexts [A].*TCC2005*, Berlin: Springer-Verlag, 2005:325-341.

[18] ZHOU Yan-zhou,ZHANG Huan-guo,LI Li-xin,et a. A short group signature DAA scheme based on l-modified one more strong Diffie-Hellman problem assumption［J］. *Journal of Beijing University of Technology*(in Chinese),2010,36(5) :601-604.

[19] HAO Liming,SUN Xun A. Method to Implement Full Anonymous Attestation for Trusted Computing Platform[J] *Wuhan University Journal of Natural Sciences*, 2007, 13(1):254-261.

[20] Zhou Fucai, Xu Jian,Li Hui. Group Signature Based on Non-interactive Zero-Knowledge Proofs [J]. *China Communications*, 2011: 34(2): 433-450.