On the Security of Two Group Signature Schemes with Forward Security

Kitae Kim
Department of Mathematics, and
ISRL, Graduate School of IT&T, Inha University, Republic of Korea
ktkim@inha.ac.kr

Ikkwon Yie
Department of Mathematics, Inha University, Republic of Korea
ikyie@inha.ac.kr

Daehun Nyang
ISRL, Graduate School of IT&T, Inha University, Republic of Korea
nyang@inha.ac.kr

Keywords: digital signature, group signature, forward security, cryptanalysis

Received: September 22, 2008

A group signature scheme allows a group member of a group to sign messages on behalf of the group anonymously. In case of dispute, a special entity of the group, group manager, can reveal the signer of a valid group signature. In 2005, Zhang et al. proposed a new group signature with forward security based on their earlier scheme in ICICS 2003. Recently, Zhou et al. proposed a dynamic group signature scheme with forward security at GCC 2007, In the year of 2008, Zhang and Geung pointed out the scheme is insecure and suggested an improvement. In this paper, we analyze a security analysis of Zhang et al.'s group signature scheme and Zhou et al.'s group signature scheme. We also discuss why the improved Zhou et al.'s scheme by Zhang et al. is still insecure.

Povzetek: Analizirane so varnosti skupinskega podpisovanja dveh modelov: Zhou in Zhang.

1 Introduction

Following the first work by Chaum and van Heyst (10) in the year of 1991, many group signature schemes have been proposed and analyzed. In such a scheme, individual members of a group is allowed to sign messages on behalf of the group anonymously. Moreover, group signature schemes allow the group manager to reveal a signer's identity in case of dispute. Unforgeability, anonymity and traceability were noted as basic security requirements for group signature schemes by Chaum and van Heyst (10). Later, more security requirements such as unlinkability, collision-resistance, exculpability, and framing have been introduced. Informally, a secure group signature scheme must satisfy the following properties :

Unforgeability : Without knowledge of the secret key(s), no one can generate a valid group signatures. In other words, only the group members can sign messages on behalf of the group.

Anonymity : Anybody except the group manager has no information of the member's secret keys. Particularly, given a valid group signature, no one except the group manager can identify the signer.

Unlinkability : Even though seeing a list of signatures, anyone except the group manager can not relate two signatures together as being produced by the same member.

Traceability : It is not possible to produce signatures which can not be traced to one of the group that has produced the signature. That is, for given a group signature, the group manager is always able to determine who is the signer of the signature.

Exculpability : Neither member of the group nor the group manager can produce signatures on behalf of other group members. Sometimes, the requirement is used in a weaker form that group members except the group manager can not produce a valid signature that traced to other member of the group.

Coalition Resistance : Even though a set of group members collude together, it is not possible to generate signatures that cannot be traced to any of them. A weaker form that a set of members cannot produce a signature that is traced to other member than the set is sometimes called Framing.

In 2003, Zhang et al. (15) proposed a group signature scheme with forward security. However, G. Wang showed

that Zhang et al.'s scheme is insecure by presenting several attacks (14). After that, Zhang et al. suggested a new group signature scheme in (16) and claimed that their scheme satisfies all the above requirements, and, in addition to, forward security.

Recently, Zhou et al. (17) proposed a dynamic group signature scheme with forward security. But, Zhang and Geng showed that the Zhou et al.'s scheme is universally forgeable and suggested an improvement in (18). The authors claimed that their improvement can be proved to be secure without presenting the details of the proof.

In this paper, we analyze the Zhang et al.'s new group signature scheme in (16) and the improvement of Zhou et al's group signature scheme (as well as the original Zhou et al.'s scheme). More precisely, we point out the open algorithm of new Zhang et al.'s scheme does not properly operate, and show their scheme is not secure even if the algorithm can be improved. In addition, we show that the Zhou et al.'s scheme and its improvement are insecure.

2 Zhang et al.'s Group Signature Scheme

Before presenting Zhang et al.'s group signature scheme, we briefly review some notions used in the scheme.

For a positive integer n, the *Euler phi function* (or *Euler totient function*) $\phi(n)$ is defined to be the number of positive integers less then n which are relatively prime to n. If a positive integer n is a composite of two primes, say $n = pq$, then $\phi(n) = (p-1)(q-1)$.

As RSA-like schemes, their group signature scheme is constructed on the group $\mathbb{Z}_n^\times$, where $\mathbb{Z}_n^\times = \{k : 0 < k < n \text{ and } \gcd(k,n) = 1\}$. Due to the security, n is usually chosen to be a product of two strong primes of the same size. A prime p is called *strong prime* if $(p-1)/2$ is also prime. To summarize, n is chosen to be $n = p_1p_2$ such that p_1 and p_2 are large strong primes of the same size.

Additionally, two cryptographic primitives, a hash function and a signature of knowledge, are used in Zhang et al.'s group signature scheme. More precisely, it employs a coalition resistant hash function $h(\cdot)$, and a signature of knowledge SPK on the discrete logarithm : Given g and $y = g^\gamma$ for some γ, $SPK\{\gamma : y = g^\gamma\}()$ is a (non-interactive) proof of knowledge of γ

2.1 The Scheme

We briefly describe Zhang et al.'s new group signature scheme (16).

Setup. The group manager (GM) randomly chooses two strong primes p_1, p_2. Let $n = p_1p_2$ and $G =< g >$ be a cyclic subgroup of $\mathbb{Z}_n^\times$. GM chooses an integer x as his secret key, and computes the public key $y = g^x \bmod n$. GM selects a random integer e such that $\gcd(e, \phi(n)) = 1$ and computes d such that $de = 1 \bmod \phi(n)$. The expected system life-time is divided into T intervals which are publicly known. Finally, GM publishes the public key $(y, n, g, e, h(\cdot), ID_{GM}, T)$, where $ID_{GM} \in \mathbb{Z}_n^\times$ is the identity of the group manager and $(c, s) = SPK\{\gamma : y = g^\gamma\}()$.

Join. If a user, say Bob, wants to join to the group, Bob executes an interactive protocol with GM as follows :

1. Bob chooses a random $k \in \mathbb{Z}_n^\times$ as his private key, and computes his identity $ID_B = g^k \bmod n$. Then he generates $(c, s) = SPK\{\gamma : ID_B = g^k\}()$. Finally, Bob keeps k privately and sends $(ID_B, (c, s))$ to the group manager.
2. Upon receiving $(ID_B, (c, s))$, GM verifies the signature of knowledge (c, s). If the verification holds, GM choose a random $\alpha \in \mathbb{Z}_n^\times$ and computes a triple (r_B, s_B, W_{B_0}) from

$$\begin{aligned} r_B &= g^\alpha \bmod n, \\ s_B &= \alpha + r_B x, \\ w_{B_0} &= (ID_{GM} r_B ID_B)^{-d^T} \bmod n. \end{aligned}$$

   Then GM sends Bob (s_B, r_B, w_{B_0}) via a private channel, and stores $(ID_B, (c, s))$ together with (r_B, s_B, w_{B_0}) in his local database.
3. After Bob receives (s_B, r_B, w_{B_0}), he verifies

$$g^{s_B} \stackrel{?}{\equiv} r_B y^{r_B} \bmod n \quad (1)$$

$$ID_{GM} ID_B r_B \stackrel{?}{\equiv} w_{B_0}^{-e^T} \bmod n \quad (2)$$

   If the equations (1) and (2) hold, Bob stores (s_B, r_B, w_{B_0}) as his initial membership certificate.

Evolve. Assume that Bob has the group membership certificate (s_B, r_B, w_{B_j}) at time period j. Then at time period $j+1$, he updates his group membership certificate as $(s_B, r_B, w_{B_{j+1}})$ by computing

$$w_{B_{j+1}} = \left(w_{B_j}\right)^e \bmod n,$$

where $w_{B_j} = (r_B ID_{GM} ID_B)^{-d^{T-j}} \bmod n$.

Sign. Suppose that Bob has the group membership certificate (s_B, r_B, w_{B_j}) at time period j. To sign a message m, Bob chooses random numbers $q_1, q_2, q_3 \in \mathbb{Z}_n^\times$, and computes

$$\begin{aligned} z_1 &= g^{q_1} y^{q_2} q_3^{e^{T-j}} \bmod n, \\ u &= h(z_1, m), \\ r_2 &= q_3 w_{B_j}^u \bmod n, \\ r_1 &= q_1 + (s_B + k)u, \\ r_3 &= q_2 - r_B u. \end{aligned}$$

The resulting group signature on m is $\sigma = (u, r_1, r_2, r_3, m, j)$.

Verify. Given $\sigma = (u, r_1, r_2, r_3, m, j)$, a verifier computes

$$z_1' = ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n,$$

and then checks $u' \stackrel{?}{=} h(z_1', m)$. If so, the verifier accepts the signature as a valid group signature from a legal group member.

Open. In case of a dispute, GM can open signature to reveal the actual identity of the signer. If $\sigma = (u, r_1, r_2, r_3, m, j)$ is a valid signature, GM operates as follows to find the signer's identity :

1. Computes $\eta = u^{-1} \bmod \phi(n)$.
2. Compute

$$z_1' = ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n.$$

3. Find w_B using (ID_B, r_B, w_{B_0}) in his local database satisfying

$$r_2 / w_B^{\eta} \stackrel{?}{\equiv} (z'/g^{r_1} y^{r_3})^{d^{T-j}} \bmod n.$$

Revoke. Suppose GM wants to revoke Bob's membership certificate at time period j. Then GM performs as follows :

1. Compute $R_j = w_B (r_B ID_B)^{d^{T-j}} \bmod n$.
2. Publish (R_j, j) in the certificate revocation list (CRL).

Given a valid signature $\sigma = (u, r_1, r_2, r_3, m, j)$, a verifier can identify whether σ is produce by a revoked member. For this sake, he performs as follows :

1. Compute

$$z_1' = ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n \quad (3)$$

2. Check

$$z_1' \left(r_2^{-1} R_j^u\right)^{e^{T-j}} \stackrel{?}{\equiv} g^{r_1} y^{r_3} \bmod n \quad (4)$$

If the signature satisfies the equation of (3) and (4) then the verifier concludes that the signature is revoked.

2.2 Security Analysis of Zhang et al.'s Scheme

In (16), Zhang et al. analyzed the security of their scheme, and concluded that their scheme satisfies the security requirements of group signature schemes. However, we find the open algorithm is incorrectly designed. Moreover, their scheme does not satisfy the unforgeability even if one can improve the open algorithm to work correctly.

2.2.1 Incorrectness of the open algorithm

Suppose that $\sigma = (u, r_1, r_2, r_3, m, j)$ is a valid group signature signed by Bob with valid certificate (s_B, r_B, w_{B_j}). Then since

$$\begin{aligned} z_1 &= g^{q_1} y^{q_2} q_3^{e^{T-j}} \bmod n \\ &= ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n, \end{aligned}$$

we have $\frac{z_1}{g^{r_1} y^{r_3}} \equiv ID_{GM}^u r_2^{e^{T-j}} \pmod n$, and so

$$\left(\frac{z_1}{g^{r_1} y^{r_3}}\right)^{d^{T-j}} \equiv ID_{GM}^{ud^{T-j}} r_2 \bmod n \quad (5)$$

$$= ID_{GM}^{ud^{T-j}} q_3 w_{B_j}^u \bmod n. \quad (6)$$

On the other hand,

$$\frac{r_2}{w_{B_j}^{\eta}} \equiv r_2 w_{B_j}^{-u^{-1}} \bmod n \quad (7)$$

$$\equiv q_3 w_{B_j}^u w_{B_j}^{-u^{-1}} \bmod n. \quad (8)$$

We can easily see the quantities (6) and (8) are not the same : If these are equal then $ID_{GM}^{ud^{T-j}} \equiv w_{B_j}^{-u^{-1}} \pmod n$. Powering ue^{T-j} on both sides we have $ID_{GM}^{u^2} \equiv ID_{GM} ID_B r_B \pmod n$, which leads to a contradiction.

Remark 2.1. Before the invention of the above scheme, Zhang et al. already proposed a group signature scheme (15) entitled with "A novel group signature scheme with forward security" in ICICS 2003. At the same time, Wang suggested several attacks against the scheme (14). Lately, Zhang et al. proposed a new group signature scheme described above. Considering Zhang et al.'s early scheme, the following modification is seemed to be natural :

Given a valid group signature $\sigma = (u, r_1, r_2, r_3, m, j)$, the group manager does the following :

1. Compute $\eta = u^{-1} \bmod \phi(n)$.
2. Compute $z_1' = ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n$.
3. Find $(s_B, r_B, w_{B_j}, ID_B)$ in his local database satisfying

$$\left(\frac{r_2^{\eta}}{w_{B_j}}\right)^{e^{T-j}} \stackrel{?}{\equiv} \left(\frac{z_1}{g^{r_1} y^{r_3}}\right)^{\eta} ID_B r_B \pmod n.$$

However, this modification is not a correct improvement. Indeed, for a valid signature $\sigma = (u, r_1, r_2, r_3, m, j)$, every (w_{B_j}, ID_B, r_B) (not necessarily membership certificate of actual signer) satisfies the equation of 3.

2.2.2 Forgery attack

The above subsection illustrates that the open algorithm of Zhang et al.'s group signature scheme does not correctly work. Of course, there might be an improvement of the

open algorithm while we couldn't find such one. However, we can break the scheme even if the algorithm can be modified to operate correctly. We remark that the attack in subsection is much similar to Wang's attack (14). Now, we describe our attack which can be mounted by anyone, not necessarily a group member.

Suppose that a group member Bob with certificate (r_B, s_B, w_{B_j}) was revoked by GM at time period j. Then the CRL should contain (R_j, j) where $R_j = w_{B_j}(r_B ID_B)^{d^{T-j}}$. Now an attacker Oscar (not a group member, outsider) can sign on any message M chosen by himself as follows :

1. Choose $q_1, q_2, q_3, \alpha, \beta \in \mathbb{Z}_n^{\times}$.
2. Compute

$$\begin{aligned} z_1 &= g^{q_1} y^{q_2} q_3^{e^{T-j}} \bmod n, \\ u &= h(z_1, M), \\ r_2 &= R_j^u g^{-\alpha} y^{\beta} q_3 \bmod n \\ r_1 &= q_1 + \alpha e^{T-j} \bmod n, \\ r_3 &= q_2 - \beta e^{T-j} \bmod n. \end{aligned}$$

In order to show that the tuple (u, r_1, r_2, r_3, M, j) is a valid group signature, it is enough to show that $z_1' = z_1$, where

$$\begin{aligned} z_1 &= g^{q_1} y^{q_2} q_3^{e^{T-j}} \bmod n, \\ z_1' &= ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n. \end{aligned}$$

We first note that

$$\begin{aligned} R_j &= w_{B_j}(r_B ID_B)^{d^{T-j}} \bmod n \\ &= (r_B ID_B ID_{GM})^{-d^{T-j}} (r_B ID_B)^{d^{T-j}} \bmod n \\ &= ID_{GM}^{-d^{T-j}} \bmod n. \end{aligned}$$

Then

$$\begin{aligned} z_1' &= ID_{GM}^u g^{r_1} r_2^{e^{T-j}} y^{r_3} \bmod n \\ &= ID_{GM}^u g^{r_1} (R_j^u g^{-\alpha} y^{\beta} q_3)^{e^{T-j}} y^{r_3} \bmod n \\ &= ID_{GM}^u g^{q_1 + \alpha e^{T-j}} R_j^{u e^{T-j}} g^{-\alpha e^{T-j}} \\ &\quad \cdot y^{\beta e^{T-j}} q_3^{e^{T-j}} y^{q_2 - \beta e^{T-j}} \bmod n \\ &= ID_{GM}^u {ID_{GM}}^{-d^{T-j} u e^{T-j}} \\ &\quad \cdot g^{q_1} y^{q_2} q_3^{e^{T-j}} \bmod n \\ &= g^{q_1} y^{q_2} q_3^{e^{T-j}} \bmod n = z_1 \end{aligned}$$

Thus, once the GM releases a revocation token (R_j, j) for a group member at time period j, everyone can generate valid group signatures during the same time period on any message. Since $R_i = R_j^{e^{i-j}}$, one can compute R_i for all $i > j$ from the token R_j and then mount the above attack. Therefore, one can generate valid signatures for any time period i where $i \geq j$.

3 Zhou et al.'s Group Signature Scheme

At GCC 2007, Zhou et al. proposed a dynamic group signature with forward security (17). Later, Zhang and Geung (18) showed the scheme is insecure by presenting a universal forgery attack, and proposed an improvement. However, we find that the improvement as well as the original scheme is insecure.

3.1 Brief Review of Zhou et al.'s Scheme

We first briefly describe the Zhou et al.'s group signature scheme in (17) as follows:

Setup. Let F_q be a finite field, $E : y^2 = x^3 + ax + b$ be an elliptic curve over the field , where q is a prime of n bits and $4a^3 + 27b^2 \bmod q \neq 0$, and $P \in E(F_q)$ be a (base) point whose order is a large prime number l. Let $\#E(F_q)$ and ψ denote the order of the elliptic curve and a function which makes the conversion from a point $P = (x, y) \in E(F_q)$ to x, respectively. We use $(P)_x$ instead of $\psi(P)$. Now, the group manager GM chooses a random $k_{GM} \in \mathbb{Z}_l^{\times}$ and then computes $K_{GM} = k_{GM} P$ as its public key. The GM's secret key is k_{GM}, and the group public key is K_{GM}. We assume that each user B has its identity ID_B which is an element of $E(F_q)$.

Join. When a user B wants to join the group, GM and B perform the following protocol :

1. B chooses a random $k_B \in \mathbb{Z}_l^{\times}$ as private key, and computes $K_B = k_B P$ as private key. Then B sends (K_B, ID_B) to the group manager.
2. Upon receiving (K_B, ID_B), GM chooses a random $u_B \in \mathbb{Z}_l^{\times}$, and computes $ID_B' = h(u_B || (ID_B)_x) P$. Then he sends ID_B' to the GM.
3. GM selects a random $v \in \mathbb{Z}_l^{\times}$, and computes $V_B = vP$ and

$$s_B = k_{GM} h((ID_B')_x || (V_B)_x) + v \bmod l.$$

GM sends (V_B, s_B) to the user B, and stores (ID_B, ID_B', u_B) in his local data base.

Finally, B gets its membership certificate (K_B, ID_B', V_B, s_B) and becomes a member of the group.

Sign. To sign a message $m \in \mathbb{Z}_l^{\times}$, a member B chooses a random $r \in \mathbb{Z}_l^{\times}$, and computes

$$\begin{aligned} R &= rP, \\ s &= (k_B - m(R)_x) r^{-1} \bmod l, \\ I &= ID_B' + ID_B + k_B K_{GM}. \end{aligned}$$

Then $\sigma = (m, s, R, I, K_B)$ is a group signature on the message m.

Verify. A verifier accepts a signature $\sigma = (M, \sigma_1, \sigma_2, \sigma_3, \sigma_4)$ if the following equations are satisfied

$$\begin{aligned} s_B P &\stackrel{?}{=} h((ID'_B)_x || (V_B)_x) K_{GM} + V_B, \\ \sigma_4 &\stackrel{?}{=} \sigma_1 \sigma_2 + m(\sigma_2)_x P. \end{aligned}$$

Note that the verifier must be able to search (s_B, V_B) corresponding to $\sigma_4 = K_B$. That is, this algorithm assumes that tuples (s_B, V_B, K_B) of all group members are public.

Open. Omitted (see (17))

3.2 A Comment on Zhou et al.'s Scheme and on its improvement by Zhang et al.

Zhang et al. (18) pointed out that Zhou et al.'s scheme is forgeable, and presented an improvement by including another hash function $H(\cdot) : \{0,1\}^* \times E(F_q) \rightarrow \mathbb{Z}_l^\times$ and revising the Sign and Verify algorithms. In particular, the revised Sign procedure is as follows :

To sign message m, a member B randomly selects $r \in \mathbb{Z}_l^\times$ to compute

$$\begin{aligned} R &= rP, \\ s &= (k_B - H(m, R)(R)_x) r^{-1} \bmod l, \\ I &= ID'_B + ID_B + k_B K_{GM}. \end{aligned}$$

Then the group signature on m is $\sigma = (m, s, R, I, K_B)$.

Though Zhang et al. claimed that their improved scheme is proved to be secure without detailed proofs, this revision as well as the Zhou et al.'s scheme is obviously linkable since two same pieces of information I and K_B are included in all group signatures generated by the same group member.

To avoid the linkability property, the deterministic information depending on the actual signer should be randomized. In this case, however, the group manager cannot trace the actual signer because the information I is used by the group manager in opening process. In other words, the Open algorithm cannot properly operate. Even worse, since K_B is critical value for signatures generated by B to be verified, no one can verify the signatures if the information is randomized. As a result, we conclude that the Zhou et al.'s scheme as well as Zhang et al.'s improvement cannot be repaired.

4 Conclusion

Zhang et al.'s new group signature scheme described in section 2 is based on their earlier version in (15). The earlier scheme was analyzed by Wang (14) and Cao (9), but no attack against the later scheme was announced. In this paper, we firstly presented security analysis of Zhang et al.'s new group signature scheme. By our analysis, the open algorithm of their scheme is incorrectly designed. Moreover, the scheme is not secure even though the open algorithm can be improved. Finally, we analyze Zhou et al.'s group signature scheme (17) and an improved scheme (18). The Zhou et al.'s scheme and the improved scheme are always linkable because each signature in the schemes includes deterministic values corresponding to a group member.

Acknowledgement

The authors would like to thank anonymous reviewers for their valuable comments. This work was supported by the IT R&D program of MIC/IITA,[2008-F-036- 01,Development of Anonymity-based u-Knowledge Security Technology].

References

[1] G. Ateniese, J. Camenisch, M. Joye, G. Tsudik (2000), *A practical and provably secure coalition-resistant group signature scheme*, CRYPTO'00, LNCS 1880, Springer-Verlag, pp. 255-270.

[2] J.H. An, Y. Dodis, T. Rabin (2002), *On the security of joint signature and encryption*, EUROCRYPT'02, LNCS 2332, Springer-Verlag, pp. 83-107.

[3] G. Ateniese, B. de Medeiros (2003), *Efficient group signatures without trapdoors*, ASIACRYPT'03, LNCS 2894, Springer-Verlag, pp. 246-268.

[4] M. Bellare, D. Micciancio, B. Warinschi (2003), *Foundations of group signatures : Formal definitions, simplified requirements and a construction based on general assumptions*, EUROCRYPT'03, LNCS 2656, Springer-Verlag, pp. 614-629.

[5] D. Boneh, X. Boyen, H. Shacham (2004), *Short group signatures*, CRYPTO'04, LNCS 3152, Springer-Verlag, pp. 45-55.

[6] X. Boyen, B. Waters (2006), *Compact group signatures without random oracles*, EUROCRYPT'06, LNCS 4004, Springer-Verlag, pp. 427-444.

[7] J. Camenisch and A. Lysyanskaya (2002), *Dynamic accumulators and application to efficient revocation of anonymous credentials*, CRYPTO'02, LNCS 2442, Springer-Verlag, pp. 61-76.

[8] J. Camenisch and M. Stadler (1997), *Efficent group signature schemes for large groups*, CRYPTO'97, LNCS 1294, Springer-Verlag, pp. 410-424.

[9] Z. Cao (2005), *Untraceability of Two Group signature Schemes*, Cryptology ePrint archive, http://eprint.iacr.org/2005/055.

[10] D. Chaum, E.V. Heyst (1992), *Group signatures*, EUROCRYPT'91, LNCS 547, Springer-Verlag, pp. 257-265.

[11] H. Park, S. Lim, I. Yie, K. Kim, J. Song (2009), *Strong unforgeability in group signature schemes*, to apper in Elsevier.

[12] D.X. Song (2001), *Practical forward secure group signature schemes*, Proc. of the 8th ACM CCS 2001, ACM press, pp. 225-234.

[13] G. Tsudik and S. Xu (2003), *Accumulating composites and improved group signing*, ASIACRYPT 2003, LNCS 2894, Springer-Verlag, pp. 269-286.

[14] G. Wang (2003), *On the security of a Group Signature with Forward Security*, ICISC 2003, LNCS 2971, Springer-Verlag, pp. 27-39.

[15] J. Zhang, Q. Wu and Y. Wang (2003), *A Novel Efficient Group Signature With Forward Security*, ICICS 2003, LNCS 2836, Springer-Verlag, pp. 292-300.

[16] J. Zhang, Q. Wu and Y. Wang (2005), *A New Efficient Group Signature With Forward Security*, Informatica, Vol. 29, No. 3, Slovenian Society Informatika, pp. 321-325.

[17] X. Zhou, X. Yang, P. Wei and Y. Hu (2007), *Dynamic group signature with forward security and its application*, Proc. of the 6th International Conference on Grid and Cooperative Computing (GCC 2007), IEEE Compupter Society, pp. 473-480.

[18] J. Zhang and Q. Geng (2008), *On the Security of Group Signature Scheme and Designated Verifier Signature Scheme*, Proc. of International Conference on Networking, Architecture, and Storage, IEEE Computer Society, pp. 351-358.