Untraceability of Two Group Signature Schemes

Zhengjun Cao[†]

[†]Institute of Systems Science, Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing, P.R. China. 100080 zjcamss@hotmail.com

Abstract A group signature scheme allows a group member of a given group to sign messages on behalf of the group in an anonymous fashion. In case of a dispute, however, a designated group manager can reveal the signer of a valid group signature. In the paper, we show the untraceability of two group signatures in [1, 5] by new and very simple attacks. Although those flaws, such as, forgeability, untraceability and linkability have been shown in [2, 7, 8, 9], we should point out that our attacks are more simple.

Keywords Group signature, Untraceability.

1 Introduction

The concept of group signature was introduced by Chaum and Heyst[3], which allow individual members to make signatures on behalf of the group. More formally, a secure group signature scheme must satisfy the following properties[4]:

- Unforgeability: Only group members are able to sign messages on behalf of the group.
- Anonymity: Given a valid signature of some message, identifying the actual signer is computationally hard for everyone but the group manager.
- Traceability: The group manager is always able to open a valid signature and identify the actual signer.
- Coalition-resistance: A colluding subset or group members (even if comprised of the entire group) cannot generate a valid signature that the group manager cannot link to one of the colluding group members.
- Unlinkability: Deciding whether two different valid signatures were produced by the same group member is computationally hard.
- Exculpability: Neither a group member nor the group manager can sign on behalf of other group member.

In the paper, we show the untraceability of two group signature schemes in [1, 5] by new and very simple attacks. Although those flaws, such as, forgeability, untraceability and linkability have been shown in [2, 7, 8, 9], we should point out our attacks are more simple.

2 Zhang-Wu-Wang group signature scheme

Zhang et al. proposed a novel efficient group signature scheme with forward security in [1]. Unfortunately, the scheme is linkable, untraceable and universally forgeable[2].

2.1 Review of Zhang-Wu-Wang group signature scheme

2.1.1 SETUP

The group manager (GM) randomly chooses two large primes p_1, p_2 of the same size such that $p_1 = 2p_1' + 1$ and $p_2 = 2p_2' + 1$, where both p_1', and p_2' are also primes. Let $n = p_1 p_2$, and $G =< g >$ be a cyclic subgroup of Z_n^*. GM chooses a random integer e which satisfies $gcd(e, \phi(n)) = 1$, and computes d such that $de = 1 \ mod \ \phi(n)$. Let $h(\cdot)$ be a coalition-resistant hash function. The expected system life-time is divided into T intervals. GM randomly choose an integer x as his secret key and computes the corresponding public key $y = g^x \pmod n$. $(c, s) = SPK\{\gamma : y = g^\gamma\}()$ denotes the signature of knowledge of $log_g y$ on the empty message. Finally, the group manager publishes the public key $(y, n, g, e, h(\cdot), ID_{GM}, T)$, where ID_{GM} is the identity of the group manager.

2.1.2 JOIN

If a user, say Bob, wants to join the group, he executes an interactive protocol with GM. Firstly, Bob chooses a random number $k \in Z_n^*$ as his secret key, and computes his identity $ID_B = g^k \ mod \ n$. Then Bob generates the signature of knowledge $(c, s) = SPK\{\gamma : ID_B = g^\gamma\}()$ to show that he knows a secret value k to meet $ID_B = g^k \ mod \ n$. Finally, Bob keeps k privately and sends $(ID_B, (c, s))$ to the group manager.

Upon receiving $(ID_B, (c, s))$, GM firstly verifies the signature of knowledge (c, s). If the verification holds, GM chooses a random number $\alpha \in Z_n^*$, and computes a triple (r_B, s_B, ω_{B_0}) from

$$r_B = g^\alpha \ mod \ n, \quad s_B = \alpha + r_B x, \quad \omega_{B_0} = (r_B ID_{GM} ID_B)^{-d^T} \ mod \ n.$$

Then GM sends Bob $(s_B, r_B, \omega_{B_0}$ via a private channel, and stores (s_B, r_B, ω_{B_0}) together with $(ID_B, (c, s)$ in his local database. After Bob receives (s_B, r_B, ω_{B_0}), he verifies the following relations:

$$g^{s_B} = r_B y^{r_B} \ mod \ n, \quad and \quad r_B ID_{GM} ID_B = \omega_{B_0}^{-e^T} \ mod \ n$$

If both the above equations hold, Bob store (s_B, r_B, ω_{B_0}) as his resulting initial membership certificate.

2.1.3 EVOLVE

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

$$\omega_{B_{j+1}} = (\omega_{B_j})^e \ mod \ n,$$

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

2.1.4 SIGN

To sign a message m, Bob randomly chooses two numbers $q_1, q_2 \in Z_n^*$, and computes z_1, μ, r_1, r_2, r_3 as follows:

$$z_1 = g^{q_1} y^{q_2} \mod n, \qquad \mu = h(z_1, m),$$
$$r_2 = \omega_{B_j}^{\mu} \mod n, \quad r_1 = q_1 + (s_B + k)\mu h(r_2), \quad r_3 = q_2 - r_B \mu h(r_2)$$

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

2.1.5 VERIFY

Given $\sigma = (\mu, r_1, r_2, r_3, m, j)$, a verifier accepts it as a valid group signature on m if and only if $\mu \equiv h(z_1', m)$, where z_1' is computed by

$$z_1' = ID_{GM}^{\mu h(r_2)} g^{r_1} r_2^{h(r_2) e^{T-j}} y^{r_3} \mod n.$$

2.1.6 OPEN

In case of a dispute, GM executes the following procedure:
1. Check the validity of signature σ via VERIFY procedure.
2. Compute $\eta = 1/(\mu h(r_2)) \mod \phi(n)$.
3. Compute $z_1' = ID_{GM}^{\mu h(r_2)} g^{r_1} r_2^{h(r_2) e^{T-j}} y^{r_3} \mod n$.
4. Search his database to find a pair (ID_B, r_B) that satisfies the following equality:

$$r_B ID_B = (g^{r_1} y^{r_3} / z_1')^{\eta} \mod n.$$

5. If there is duple (r_B, ID_B) satisfying the above equation, GM conclude that ID_B is the identity of the actual signer. Otherwise, output $\perp$.

2.1.7 REVOKE

Omitted (see [1]).

2.2 Untraceability

Though the authors claim that the scheme is secure, it is not true. It has been shown that the scheme is linkable, untraceable and universally forgeable in [2]. Now We present a simple and direct attack in the following. It shows the scheme is untraceable from a new point of view.

SIGN

To sign a message m, the group member Bob randomly chooses three numbers $q_1, q_2, t \in Z_n^*$, and computes z_1, μ, r_1, r_2, r_3 as follows:

$$\begin{aligned} z_1 &= g^{q_1} y^{q_2} \mod n, \\ \mu &= h(z_1, m), \\ r_2 &= \underline{y^{t\mu}} \omega_{B_j}^{\mu} \mod n, \\ r_1 &= q_1 + (s_B + k)\mu h(r_2), \\ r_3 &= q_2 - r_B \mu h(r_2) - \underline{t\mu h(r_2) e^{T-j}} \end{aligned}$$

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

VERIFY

Given $\sigma = (\mu, r_1, r_2, r_3, m, j)$, a verifier accepts it as a valid group signature on m if and only if $\mu \equiv h(z_1', m)$, where z_1' is computed by

$$z_1' = ID_{GM}^{\mu h(r_2)} g^{r_1} r_2^{h(r_2) e^{T-j}} y^{r_3} \mod n.$$

Correctness:

$$\begin{aligned} z_1' &= ID_{GM}^{\mu h(r_2)} g^{r_1} r_2^{h(r_2) e^{T-j}} y^{r_3} \\ &= ID_{GM}^{\mu h(r_2)} g^{r_1} \underline{(y^{t\mu})^{h(r_2) e^{T-j}}} \omega_{B_j}^{\mu h(r_2) e^{T-j}} y^{q_2 - r_B \mu h(r_2)} \underline{y^{-t\mu h(r_2) e^{T-j}}} \\ &= ID_{GM}^{\mu h(r_2)} g^{r_1} \omega_{B_j}^{\mu h(r_2) e^{T-j}} y^{q_2 - r_B \mu h(r_2)} \\ &= ID_{GM}^{\mu h(r_2)} g^{q_1} g^{s_B \mu h(r_2)} g^{k \mu h(r_2)} \left(r_B ID_{GM} ID_B\right)^{-\mu h(r_2)} y^{q_2} y^{-r_B \mu h(r_2)} \\ &= ID_{GM}^{\mu h(r_2)} g^{q_1} g^{s_B \mu h(r_2)} g^{k \mu h(r_2)} \left(g^{s_B} y^{-r_B} ID_{GM} ID_B\right)^{-\mu h(r_2)} y^{q_2} y^{-r_B \mu h(r_2)} \\ &= g^{q_1} y^{q_2} = z_1 \qquad (mod\ n) \end{aligned}$$

But we have

$$(g^{r_1} y^{r_3} / z_1')^{\eta} = g^{s_B + k} \underline{y^{-te^{T-j} - r_B}} \neq r_B ID_B \mod n.$$

Therefore, the scheme is untraceable.

Remark: Underlined parts show the differentia between the attack and original scheme.

3 Kim-Park-Won group signature scheme

At Asiacrypt'96, Kim.et.al. proposed a convertible group signature[5] based on the scheme of Park et.al.[6]. It is so called K-P-W group signature scheme. However, there exist many weaknesses. For example: Lim and Lee[8] pointed out that the group members can forge and conspire to make a valid signature. Actually, though user U_i cannot obtain GC's secret key d, he can get ID_G^{-d} and g^d, where ID_G and g are the identity and a public parameter of GC (group center), respectively. The author of [8] pointed out that GC can change a valid signature into another group member's valid signature in the same message. The authors of [9] have shown

that GC can produce a valid group signature for any message and then impose it on any group member. [2] has also presented a universal forgery attack.

To us surprise, we find that the identifying verification equation in the scheme is identical, that is to say, it has no relation to the actual signer's secret key of a given valid group signature.

3.1 Review of Kim-Park-Won group signature scheme

We first briefly describe the scheme in [5] as follows:

Let $n = pq = (2fp' + 1)(2fq' + 1)$, where p, q, f, p', q' are distinct primes. g has an order of f (i.e. $g^f = 1 \ mod \ n$), γ and d are two integers, where $\gamma d = 1 \ mod \ \phi(n)$, $gcd(\gamma, \phi(n)) = 1$. Let h, ID_G denote a secure hash function and the identity information of group center (GC), respectively. GC publishes (n, r, g, f, h, ID_G) as the group public keys and keeps (d, p', q') secret.

A group member U_i with identity information ID_G randomly selects his secret key $s_i \in (0, f)$ and then sends $(ID_i g^{s_i} \ mon \ n)$ to GC. GC computes $x_i = (ID_G g^{s_i})^{-d} \ mod \ n$ and sends it to member U_i secretly. member U_i chooses two distinct random integer numbers r_1, r_2 in $[0, f)$ and computes $V = g^{r_1} r_2^{\gamma} \ mod \ n$. Inputting h with V and message m, he get $e = h(V, m)$. Subsequently, he computes $z_1 = r_1 + s_i e \ mod \ f, z_2 = r_2 x_i^e \ mod \ n$. Thus he generates the group signature (e, z_1, z_2) for message m.

Signature verification equation:

$$e = h(\hat{V}, m) \text{ where } \hat{V} = (ID_G)^e g^{z_1} z_2^{\gamma} \ mod \ n$$

Identifying verification equation:

$$g^{z_1} = (\hat{V} r_2^{-\gamma})(g^{s_i})^e \ mod \ n. \quad \text{where } r_2 = z_2 x_i^{-e} \ mod \ n$$

3.2 Untraceability

Now we show that the identifying verification equation is **identical**. In fact, for a **given** valid group signature (e, z_1, z_2) and an **arbitrary** group member's secret key (x_j, s_j), we have

$$\begin{aligned}
& \hat{V}(z_2 x_j^{-e})^{-\gamma}(g^{s_j})^e = \hat{V} z_2^{-\gamma} x_j^{e\gamma}(g^{s_j})^e \\
= \ & (ID_G)^e g^{z_1} \underline{z_2^{\gamma} z_2^{-\gamma}} x_j^{e\gamma}(g^{s_j})^e \quad \text{(have no relation to the inner structure of } z_2\text{)} \\
= \ & (ID_G)^e g^{z_1} x_j^{e\gamma} g^{s_j e} \\
= \ & (ID_G g^{s_j})^e g^{z_1} x_j^{e\gamma} \\
= \ & \underline{x_j^{-e\gamma}} g^{z_1} \underline{x_j^{e\gamma}} \quad (e \text{ is counteracted}) \\
= \ & g^{z_1} (mod \ n) \quad \text{(have no relation to the inner structure of } z_1\text{)}
\end{aligned}$$

Therefore, the identity of the actual signer is untraceable. It's a serious designing error.

4 Conclusion

In this paper, we show the untraceability of two group signature schemes. Our new attacks are different from those in [2, 7, 8, 9]. Obviously, our attacks are more simple and direct.

References

[1] Jianhong Zhang, Qianhong Wu and Yumin Wang. A novel efficient group signature with forward security. Information and Communications Security (ICICS'03), LNCS 2836, 292-300. Springer-Verlag, 2003.

[2] Guilin Wang. On the security of a Group Signature Scheme with Forward Security. http://eprint.iacr.org/2003/226.

[3] D. Chaum and E. van Heyst. Group signatures. In: Advances in Cryptology-EUROCRYPT'91, LNCS 950, 257-265. Springer-Verlag, 1992.

[4] G. Ateniese, J.Camenisch, M.Joye, and G.Tsudik. A practical and provably secure coalition-resistant group signature scheme. In: Advances in Cryptology-CRYPTO'2000, LNCS 1880, 255-270. Springer-Verlag, 2000.

[5] Kim.S.J., Park.S.J., and Won.D.H., Convertible group signatures, Advances in Cryptology - Asiacrypt'96, 1996, (Springer). Vol. 1163, pp. 311-321 (Lecture Notes in Computer Science)

[6] Park.S.J., Lee.I.S., and Won.D.H., A practical group signature, Proc. JW-ISC'95, Japan, 1995, pp. 127-133

[7] Lim.C.H., and Lee.P.J., Remarks on convertible group of Asiacrypt'96, Electron. Lett., 1997, 33.(5), pp. 383-384

[8] Wang, C.H., Hwang.T.L., and Lee.N.Y., Comments on two group signatures, Inf. Process. Lett., 1999, 69. pp. 95-97

[9] Zichen Li, Yongchuan Wang, Yi Xian Yang and Weilin Wu, Cryptanalysis of convertible group signature, Electron. Lett., 1999, Vol.35, No.13, pp. 1071-1072