Security of A New Group Signature Scheme from IEEE TENCON'02

Fangguo Zhang and Kwangjo Kim

International Research center for Information Security (IRIS)
Information and Communications University(ICU),
58-4 Hwaam-dong Yusong-ku, Taejon, 305-732 KOREA
{zhfg, kkj}@icu.ac.kr

Abstract. Recently, R.H. Shi proposed a new group signature scheme at IEEE TENCON'02. However, in this paper, we will propose a universal forgery attack of this new group signature scheme against the known-message attack.

1 Introduction

Group signature is a relatively new concept introduced by Chaum and van Heijst [2] in 1991. A group signature scheme allows a group member to sign messages anonymously on behalf of the group. There are many group signature schemes have been proposed [1][3]. Recently, R. H. Shi proposed a new group signature scheme at IEEE TENCON'02 [4]. In this paper, we will show that Shi's group signature scheme is not secure, we propose a universal forgery attack of this group signature scheme against the known-message attack.

2 New Group Signature Scheme at IEEE TENCON'02

First of all, we review Shi's group signature scheme at IEEE TENCON'02 in brief using the same notation as [4].

[**Initiation phase**]
Let p and q be two large primes such that $q|(p-1)$, g be a generator with order q in $GF(p)$. Each group member u_i has x_i and $y_i = g^{x_i} (\bmod\ p)$ as the secret key and public key. Let T be a group authority with secret key x_T and the public key $y_T = g^{x_T} (\bmod\ p)$.

For each group member u_i, T computes (r_i, s_i) as: $r_i \equiv g^{-k_i} \cdot y_i^{k_i} \bmod p$ and $s_i \equiv k_i - r_i \cdot x_T \bmod q$. Where k_i is a random number, $\gcd(k_i, q)$=1.

Then, authority T sends (r_i, s_i) to the group member u_i secretly. After receiving (r_i, s_i), u_i can verify the validity of (r_i, s_i) using

$$g^{s_i} \cdot y_T^{r_i} \cdot r_i (\bmod\ p) \equiv (g^{s_i} \cdot y_T^{r_i})^{x_i} (\bmod\ p).$$

[**Signing phase**]
To sign message m, the group member u_i first chooses three random integers a, b and t in Z_q^* and computes $\{A, B, C, D, E\}$ using (r_i, s_i) as follows:

$$A = r_i^a \bmod p$$

$$B = r_i \cdot a \bmod p \text{ (\textbf{should be} mod } q)$$

$$C = (s_i - b) \bmod p \text{ (\textbf{should be} mod } q)$$

$$D = g^{a \cdot b} \bmod p, \ E = g^a \bmod p$$

and computes

$$\alpha_i = E^C \cdot y_T^B \cdot D \bmod p = g^{a \cdot k_i} \bmod p$$

$$R = \alpha_i^t \bmod p$$

Then the group member u_i solves S from

$$h(m) = (R \cdot x_i + t \cdot S) \bmod p \text{ (\textbf{should be} mod } q)$$

The group signature on m is (R, S, A, B, C, D, E).

[**Verification phase**]
Upon the verifier receives the message-signature pair $\{m, (R, S, A, B, C, D, E)\}$, he computes

$$\alpha_i = E^C \cdot y_T^B \cdot D \bmod p$$

and

$$H_i = \alpha_i \cdot A \bmod p.$$

The verifier accepts the signature if and only if

$$\alpha_i^{h(m)} \equiv H_i^R \cdot R^S \bmod p.$$

About the correctness of the verification and the identification phase of this scheme, the readers can refer to [4] in detail.

3 The Attack

Now, we give a universal forgery attack on Shi's group signature scheme against the known-message attack. Assume that we have a valid signature (R, S, A, B, C, D, E) of a message m. For arbitrary message m', let $\lambda \equiv h(m') \cdot h(m)^{-1} \bmod q$, randomly select an integer $\delta \in_R Z_q^*$, compute

$$\alpha_i' \equiv (E^C \cdot y_T^B \cdot D)^\delta \bmod p \ (= \alpha_i^\delta).$$

$$A' \equiv ((E^C \cdot y_T^B \cdot D) \cdot A)^{\lambda \cdot \delta} \cdot \alpha_i'^{-1} \bmod p \ (= H_i^{\lambda \cdot \delta} \cdot \alpha_i'^{-1}).$$

$$B' \equiv B \cdot \delta \bmod q$$

$$C' \equiv C \cdot \delta \bmod q$$
$$D' = D^{\delta} \bmod p$$
$$E' = E$$
$$R' = R$$
$$S' \equiv \lambda \cdot \delta \cdot S \bmod q.$$

The group signature on m' is $(R', S', A', B', C', D', E')$.

The correctness of verification of the forgery signature can be easily seen as follows:

$$\begin{aligned} \alpha'_i &\equiv E'^{C'} \cdot y_T^{B'} \cdot D' \bmod p \\ &\equiv E^{C \cdot \delta} \cdot y_T^{B \cdot \delta} \cdot D^{\delta} \bmod p \\ &\equiv (E^C \cdot y_T^B \cdot D)^{\delta} \bmod p \\ &\equiv \alpha_i^{\delta} \bmod p \end{aligned}$$

$$H'_i \equiv \alpha'_i \cdot A' \bmod p \equiv \alpha'_i \cdot H_i^{\lambda \cdot \delta} \cdot \alpha_i'^{-1} \equiv H_i^{\lambda \cdot \delta}.$$

So,

$$\begin{aligned} &\alpha_i'^{h(m')} \\ &\equiv \alpha_i^{\delta \cdot \lambda \cdot h(m)} \\ &\equiv (H_i^R \cdot R^S)^{\delta \cdot \lambda} \\ &\equiv H_i^{\delta \cdot \lambda \cdot R} \cdot R^{\delta \cdot \lambda \cdot S} \\ &\equiv H_i'^R \cdot R^{S'} \bmod p \end{aligned}$$

4 Conclusion

In this paper, we have shown that Shi's group signature scheme is not secure, any one (not necessarily a group member) can forge a valid group signature on an arbitrary message.

References

1. J. Camenisch and M. Stadler, *Efficient group signature schemes for large groups*, Advances in Cryptology-CRYPTO 97, LNCS 1294, pp.410-424, Springer-Verlag, 1997.
2. D. Chaum and E. Heijst, *Group signatures*, Advances in Cryptology-Eurocrypt 91, LNCS 547, pp.257-265, Springer-Verlag, 1991.
3. L. Chen and T.P. Pedersen, *New group signature schemes*, Advances in Cryptology-Eurocrypt 94, LNCS 950, pp.171-181, 1994. Springer-Verlag, 1991.
4. Shi Rong-Hua, *An efficient secure group signature scheme*, Proceedings of IEEE TENCON'02 (2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering), Vol.1, pp.109-112, 2002.