Cryptanalysis of An Efficient Secure Group Signature Scheme *

Li-Hua Li‡ Chi-Yu Liu§ Min-Shiang Hwang†

Department of Management Information System†
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Email: mshwang@nchu.edu.tw
Fax: 886-4-23742337

Department of Information Management‡
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan, R.O.C.

Graduate Institute of Networking and Communication Engineering§
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan, R.O.C.

May 8, 2004

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC91-2218-E-324-003.

†Responsible for correspondence: Prof. Min-Shiang Hwang

Cryptanalysis of An Efficient Secure Group Signature Scheme

Abstract

Group signature has been proposed for many years, those schemes are still not efficient. In 2002, Shi proposed a group signature scheme based on the discrete logarithm problem. In Shi's scheme, he claims that his scheme is efficient compared to previous proposed schemes. Although his scheme is better than others, the scheme is not secure. In this article, we will show that Shi's scheme will be subjected forgery attack.

Index Terms: Cryptanalysis, discrete logarithm, group signature, security

1 Introduction

A group signature allows individual members to create signature in the name of a group. For example, there is an employee to process a business transaction, and he/she must sign the digital signature on behalf of a company. The digital signature is the company's representative during processing the business deal. There are three requirements in a group signature scheme as following:

1. Only the legitimate group member could create signature of a document on behalf of the group.

2. A receiver could verify the group signature, but he/she could not acquire the identification of a signer from the group signature.

3. In a case of a dispute, the group authority could verify the identification of the signer, and other group members could verify the valid identity of

signer.

In 1991, Chaum, and Heyst [1] brought up a concept of the group signature, and proposed four algorithms of group signature. But the proposed schemes are not secure and optimal. In 1995, Chen and Pedersen [2] proposed the requirements of a group signature. In 2002, Shi [4] proposed an efficient group signature scheme which is better than previous schemes [1, 2, 3], but it could not withstand a forgery attack. In this article, we will show that the security weakness, and proof Shi's scheme is not secure.

In the second section, we will describe Shi's scheme including four phases. Next, we will propose an attack for Shi's scheme. Finally, we will give a conclusion for this article.

2 Shi's Scheme

In this section, we review Shi's scheme. There are three phases in the scheme: initiation, signing and verification, and identification phases. The following is the brief description of each phase.

Initiation Phase:

In this phase, some of system parameters must be defined. p, and q are two large primes such that $q|(p-1)$, and g is a generator with order q in $GF(p)$. T is a group authority which has a secret key x_T and public key $y_T = g^{x_T} \bmod p$. Then, each group member u_i chooses his/her secret key x_i, and computes his/her public key $y = g^{x_i} \bmod p$. After, the group authority executes the following equations to obtain its signature $\{r_i, s_i\}$.

1. Randomly chooses a number k_i such that $gcd(k_i, q) = 1$.

2. Computes r_i ($r_i = g^{-k_i} \cdot y_i^{k_i} \bmod p$) and s_i ($s_i = k_i - r_i \cdot x_T \bmod q$). Next, the authority T sends $\{r_i, s_i\}$ to the member u_i with secure channel.

3. After receiving the above information, u_i could verify the signature as follows: $g^{s_i} \cdot y_T^{r_i} \cdot r_i \bmod p = (g^{s_i} \cdot y_T^{r_i})^{x_i} \bmod p$.

If all of the above equations hold, u_i will use the $\{r_i, s_i\}$ to sign a message.

Signing and Verification Phase:

In this phase, if u_i wants to sign a message, he/she must to compute the following steps.

1. Randomly chooses three random number a, b, and t.

2. Computes $\{A, B, C, D, E\}$ where $A = r_i^a \bmod p$, $B = r_i \cdot a \bmod p$, $C = (s_i - b) \bmod p$, $D = g^{a \cdot b} \bmod p$, $E = g^a \bmod p$, $\alpha_i = E^C \cdot y_T^B \cdot D \bmod p$, and $R = \alpha_i^t \bmod p$. u_i solves $h(m) = (R \cdot x_i + t \cdot s) \bmod p$ to get s. Next, u_i sends those information with message m to the verifier.

When the verifier receives the above signature, he/she will do the following steps.

1. Computes $\alpha_i = E^C \cdot y_T^B \cdot D \bmod p$ and $H_i = \alpha_i \cdot A \bmod p$.

2. Verifies $\alpha_i^{h(m)} = H_i^R \cdot R^s \bmod p$. If the equation is hold, the signature is a valid group signature for message m.

Identification Phase:

In case of a dispute, the group authority T could obtain a group member u_i with the equation $E^C \cdot y_T^B \cdot D = E^{k_i} \bmod p$. T could proclaim the identification of u_i according to the r_i, s_i, k_i. In order to prevail on the verifier to believe that u_i is indeed the signer, and T must compute the following steps.

1. Computes $a = B \cdot r_i^{-1} \bmod p$.

2. T randomly chooses an integer d, and executes $r_T = (g \cdot y_T)^d \bmod p$, $s_T = (d - r_T \cdot a \cdot k_i) \bmod p$.

3. T sends $\{r_T, s_T, y_i\}$ to verifier.

When the verifier receives $\{r_T, s_T, y_i\}$, verifier does the following steps.

1. Computes $\beta_i = g \cdot y_i \bmod p$ and $\gamma = \alpha_i \cdot H_i \bmod p$.

2. Checks $r_T = \beta_i^{s_T} \cdot \gamma_i^{r_T} \bmod p$. If the above equation holds, verifier could identify the signer.

According to the steps of every phase in this scheme, We will point out the scheme contains a weakness of a masquerade attack.

3 Attack on Shi's Scheme

In this section, we show that Shi's scheme cannot withstand a masquerade attack. In the scheme, an illegal user could forge the group signature without obtaining any secret information. We suppose that an attacker wants to forge a legal member of a group. He performs the following steps before goes into the verification phase, and he will cheat the verifier successfully into believe the counterfeit group signature.

In order to forge the valid identification of a group member, and the attack must to perform the following steps.

1. The attack could randomly choose $\{R', S', B', C', D', E'\}$ and a meaningful message m'.

2. The attack must compute an α_i with the following equation:

$$\alpha_i' = E'^{C'} \cdot y_T^{B'} \cdot D' \bmod p.$$

3. He will compute the value of A' with the following equation:

$$A' = [(\alpha_i'^{h(m')-R'}) \div (R')^{S'}]^{R'^{-1}} \bmod p.$$

4. He sends $\{R', S', A', B', C', D', E'\}$ with m' to a verifier.

We could show that the attacker could success to forge a valid signature as follows. When the verifier receives the forge information, he computes α_i' and H_i' as follows:

$$\begin{aligned}
\alpha_i' &= E'^{C'} \cdot y_T^{B'} \cdot D \bmod p \\
H_i' &= \alpha_i' \cdot A' \bmod p.
\end{aligned}$$

Next, the verifier verifies the following equation:

$$\begin{aligned}
\alpha_i'^{h(m')} &= H_i'^{R'} \cdot R'^{S'} \bmod p \\
&= \alpha_i'^{R'} \cdot A'^{R'} \cdot R'^{S'} \bmod p \\
&= \alpha_i'^{R} \cdot [(\alpha_i'^{h(m') \cdot R'}) \div R'^{S'}] \cdot R'^{S'} \bmod p \\
&= \alpha'_{h(m')}.
\end{aligned}$$

When the verifier obtains the signature of a message m', he/she will verify the signature with Shi's verified equations. Then, the attack will successfully cheat the verifier to believe the valid group signature.

4 Conclusion

In 2002, Shi proposed an efficient secure group signature. His scheme is more efficient than others, but the scheme is not secure. In this article, we show out Shi's scheme could not withstand masqueraded attack. When an attacker randomly chooses R', S', B', C', D', E', and a meaningful message m', he could successfully cheat receiver to believe the valid source of the message m'. The attacker could be easily forged a valid identification of a member of a group.

References

[1] D. Chaum and E. Heyst, "Group signatures," in *Advances in Cryptology, Eurocrypt'91*, pp. 257–265, Lecture Notes in Computer Science, 1991.

[2] L. Chen and T. P. Pedersen, “New group signature,” in *Advances in Cryptology, Eurocrypt’94*, pp. 171–181, Lecture Notes in Computer Science, 1994.

[3] W. B. Lee and C. C. Chang, “Efficient group signature scheme based on the discrete logarithm,” *IEE Proceedings - Computer Digital Technology*, vol. 145, no. 1, pp. 15–18, 1998.

[4] R. H. Shi, “An efficient group signature scheme,” in *Proceedings of 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering*, vol. 1, pp. 109–112, 2002.