对一类群签名方案的伪造攻击

于宝证　　徐枞巍
(合肥工业大学管理学院　合肥　230009)

摘　要：该文对王晓明等(2003)和林松等(2006)最近依据 Tseng-Jan(1999)群签名方案各自提出的一种改进群签名设计了两种伪造攻击策略。利用该伪造攻击，攻击人不需要任何签名者的保密身份信息和秘密密钥信息，只是通过选取随机参数、改变原方案的部分设计步骤就能成功伪造出群成员证书，进而伪造出验证有效的群签名，从而威胁到群签名人的合法权益。该文的伪造攻击策略对 Lee-Chang(1998)群签名、Tseng-Jan 群签名及由其演化而来的所有群签名方案都具有效性，从而证明该类群签名方案全都是不安全的。

关键词：群签名；伪造攻击；安全性分析
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2009)01-0246-04

Forgery Attacks on a Series Group Signature Schemes

Yu Bao-zheng　　Xu Cong-wei
(*School of Management*, *Hefei University of Technology*, *Hefei* 230009, *China*)

Abstract: Two kinds of forgery attacks strategy on the group signature schemes proposed respectively by Wang *et al*.. (2003) and Lin *et al*.. (2006) based on the Tseng-Jan's(1999) group signature scheme is developed. Without using any secret identification or secret key, anyone can forgery a valid group member certificate and then generate a valid group signature using the forged certificate only through selecting some random parameters and changing the calculation procedures. Moreover, this kind of forgery attacks strategy can be used in Lee-Chang's (1998) group signature scheme, Tseng-Jan's group signature scheme and their varietals'. It means this series of group signature schemes is insecure.

Key words: Group signature; Forgery attack; Security analysis

1　引言

群签名允许群成员代表整个群体进行匿名签名，只有群管理员可在必要的情况下揭示某个群签名的具体签署者，因此在电子现金、电子投票等领域具有重要的应用。群签名的概念首先是由 Chaum-Heyst 在 1992 年提出的，鉴于群签名的发展趋势和重要性，在此之后，人们做了许多努力去构造各种群签名方案。1998 年 Lee-Chang 基于离散对数问题提出了一个高效的群签名方案[1]。Tseng-Jan 指出该方案不具备前向安全性，一旦一个群签名被打开，其以前或以后的签名就不具备匿名性，在此基础上他们给出了一个改进方案[2]。Sun 指出 Tseng-Jan 的改进群签名方案还是具有连接性；Joye-Lee-Hwang 指出 Lee-Chang 和 Tseng-Jan 方案有一个安全漏洞。之后 Tseng-Jan 又进行了改进以消除这种连接性和安全漏洞，但失去了原有方案的可证实性[3]。Tang 等提出了一个改进方案[4]，但由于大量使用知识证明，运算量大，效率不高，实用价值低。最近，王晓明等和林松等通过对 Tseng-Jan 改进方案的研究，分别提出了一种新的改进群签名方案(以下分别称 WF 群签名方案[5]和 LD 群签名方案[3])，并各自宣称改进方案能够有效避免伪造攻击。陈艳玲等指出 WF 群签名方案的一个安全缺陷[6]，曹正军认为该方案不具有可追踪性[7]。在详细研究 WF 群签名方案和 LD 群签名方案的设计结构后，我们发现该类方案存在重大设计缺陷，并给出了对该类群签名方案的两种通用伪造攻击构造策略。通过此伪造攻击，任何人都可伪造一个有效的群签名通过签名验证方程。该伪造攻击可适用于由 Lee-Chang 群签名方案演化而来的所有群签名方案。

2007-07-25 收到，2008-01-10 改回

2　WF 群签名方案和 LD 群签名方案简介

2.1 WF 群签名方案

WF 群签名方案由系统初始化、群成员加入、签名产生、签名验证、群成员识别和群成员注销 6 个部分组成。

2.1.1 系统初始化

(1) p， q 为两个大素数，满足 $q \mid p-1$， g 为 GF(p) 中阶为 q 的生成元。公开 p， q， g。

(2)群中的每一个成员 U_i 选择随机数 $x_i \in Z_q^*$ 作为私钥，计算 $y_i = g^{x_i} (\mathrm{mod}\, p)$ 作为公钥。群权威 T 选择随机数 $x_T \in Z_q^*$ 作为私钥，计算 $y_T = g^{x_T} (\mathrm{mod}\, p)$ 作为公钥。

(3)安全的 Hash 函数 h，公开 h。

2.1.2 群成员的加入　当 U_i 想成为群的一个成员，需作如下步骤：

(1)群权威 T 随机选择 $k_i \in Z_q^*$，并计算：

$$\begin{cases} r_i = g^{-k_i} y_i^{k_i} (\bmod p) \\ s_i = k_i - r_i x_T (\bmod q) \end{cases} \tag{1}$$

群权威将 (r_i, s_i) 秘密地发送给 U_i 并存储 (r_i, s_i, k_i)。

(2) U_i 接收到 (r_i, s_i) 后，验证：$r_i g^{s_i} y_T^{r_i} = (g^{s_i} y_T^{r_i})^{x_i} (\bmod p)$，如果上式成立，$U_i$ 接受 (r_i, s_i)。

2.1.3 群签名的产生　设待签名的消息为 m，U_i 随机选择 $a,b,d,t \in Z_q^*$，并计算：

$$\begin{cases} C = r_i a - d (\bmod q),\ A = y_i^b (\bmod p),\ D = g^b (\bmod p) \\ E = r_i^a (1 + g^{-s_i a} y_T^{-r_i a})^{x_i} (\bmod p),\ F = y_T^d (\bmod p) \\ B = s_i a - bh(A,C,D,E,F) + bh(E,D,F) (\bmod q) \\ a_i = [D^{h(E,D,F)} + g^B y_T^C F D^{h(A,C,D,E,F)}] (\bmod p) \\ R = a_i^t (\bmod p),\ s = t^{-1}[h(m,R) - x_i R] (\bmod q) \end{cases} \tag{2}$$

送 $\{s,R,A,B,C,D,E,m\}$ 给签名验证者。

2.1.4 群签名的验证　群签名验证者计算：

$$\left.\begin{aligned} a_i &= [D^{h(E,D,F)} + g^B y_T^C F D^{h(A,C,D,E,F)}] (\bmod p) \\ \delta_i &= A^{h(E,D,F)} [a_i D^{-h(E,D,F)} - 1] E (\bmod p) \end{aligned}\right\} \tag{3}$$

验证：

$$a_i^{h(m,R)} = \delta_i^R R^s (\bmod p) \tag{4}$$

2.1.5 群成员的识别　由于群权威有每个群成员的证书 (r_i, s_i, k_i)，T 可以预先计算：$v_i = s_i^{-1} k_i (\bmod p), w_i = g^{v_i} (\bmod p)$ 并将 (v_i, w_i) 与 (r_i, s_i, k_i) 一起存储。如需要打开某一个群签名，T 可以查询已存在的 (v_i, w_i) 和 (r_i, s_i, k_i)，判断哪个群成员对应的 (v_i, w_i) 满足：

$$g^B y_T^C F D^{h(A,C,D,E,F)} = w_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} (\bmod p) \tag{5}$$

于是群权威就能确定签名者的身份。

2.1.6 群成员的注销　如果要注销某个群成员，群权威 T 查询出要注销群成员对应的 (v_i, w_i)，并公布 (v_i, w_i) 为注销群成员。当签名验证者接到群签名时，首先从公布的注销群成员名单中取出 (v_i, w_i)，判断：

$$g^B y_T^C F D^{h(A,C,D,E,F)} = w_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} (\bmod p) \tag{6}$$

如上式成立，则此群签名无效，否则，继续验证群签名的有效性，即进行群签名的验证，从而实现群成员的注销。

2.2 LD 群签名方案

LD 群签名方案的系统初始化和群成员加入步骤与 WF 群签名方案类似，签名产生、签名验证、群成员识别部分简述如下。

2.2.1 群签名产生　如果 U_i 希望对消息 m 签名，则 U_i 可以随机选择 3 个数 $a,b,c \in [1, q-1]$，并计算：$A \equiv r_i^a (g + g^{s_i} y_T^{r_i})^a + g^{as_i} (\bmod p)$，$B \equiv as_i - b (\bmod q)$，$C \equiv ar_i - c (\bmod q)$，$D \equiv g^b (\bmod p)$，$E \equiv y_T^c (\bmod p)$。随后，群成员 U_i 随机选择 $t \in [1, q-1]$，并计算：$a_i \equiv g^B y_T^C DE (\bmod p)$，$r \equiv a_i^t \cdot (\bmod p)$。接着，群成员 U_i 求解同余方程：$h(m) \equiv rx_i + ts (\bmod q)$。其中 $h(\cdot)$ 为无碰撞的单向 HASH 函数，通过计算得到 s。则 $\{r,s,m,A,B,C,D,E\}$ 就是消息 m 的群签名结果。

2.2.2 群签名验证　签名者接收到签名后，先计算：$a_i \equiv g^B y_T^C DE (\bmod p)$，$DH_i \equiv A - Dg^B (\bmod p)$，并利用下式来验证签名：$a_i^{h(m)} \equiv DH_i^r r^s (\bmod p)$。

2.2.3 群签名识别　识别签名者时，验证方出示收到的签名 $\{r,s,m,A,B,C,D,E\}$。由于群权威有每个群成员的证书 (r_i, s_i, k_i)，所以可以计算出签名者。验证：$a_i \equiv (g^B D)^{s_i^{-1} k_i} \cdot (\bmod p)$。其中 s_i^{-1} 为 s_i 在 Z_q^* 上的乘法逆元。

如果上式成立，群权威就可以识别出上述签名是 U_i 签署的，则群权威就可以将自己的判断告诉验证者。证明如下：

因为：$(g^B D)^{s_i^{-1} k_i} \equiv (g^{as_i - b} g^b)^{s_i^{-1} k_i} \equiv (g^{as_i})^{s_i^{-1} k_i} \equiv g^{ak_i} \cdot (\bmod p)$，又因为 $a_i \equiv g^{ak_i} (\bmod p)$，所以 $a_i \equiv (g^B D)^{s_i^{-1} k_i} \cdot (\bmod p)$。该群签名的详细论证过程见文献[3]。

3　对 WF 群签名和 LD 群签名的伪造攻击

3.1 伪造攻击 1

以 WF 群签名为例，假设攻击者想伪造任意消息 m' 的一个有效签名，他可以按照如下步骤实现：

攻击者随机选择 $\delta \in Z_q^*$，计算 $r_i' = g^\delta y_T \bmod p$，$s_i' = \delta r_i' \bmod p$，$x_i' = 1 + r_i'^{-1} (\bmod q)$，$y_i' = g^{x_i'} (\bmod p)$，之后再随机选择 $a',b',d',t' \in Z_q^*$，并计算：

$$\begin{cases} C' = r_i' a' - d' (\bmod q),\ A' = g^{x_i' b'} (\bmod p),\ D' = g^{b'} (\bmod p) \\ E' = r_i'^{a'} (1 + g^{-s_i' a'} y_T^{-r_i' a'})^{x_i'} (\bmod p),\ F' = y_T^{d'} (\bmod p) \\ B' = s_i' a' - b' h(A',C',D',E',F') + b' h(E',D',F') (\bmod q) \\ a_i' = [D'^{h(E',D',F')} + g^{B'} y_T^{C'} F' D'^{h(A',C',D',E',F')}] (\bmod p) \\ R' = a_i'^{t'} (\bmod p),\ s' = t'^{-1}[h(m',R') - x_i' R'] (\bmod q) \end{cases} \tag{7}$$

则 $\{s',R',A',B',C',D',E',m'\}$ 就是消息 m' 的一个伪造的有效盲群签名。

因为：群签名验证者接收到伪造的签名 $\{s',R',A',B',C',D',E',m'\}$ 后，先计算：

$$a_i' = [D'^{h(E',D',F')} + g^{B'} y_T^{C'} F' D'^{h(A',C',D',E',F')}] (\bmod p)$$

$$\delta_i' = A'^{h(E',D',F')} [a_i' D'^{-h(E',D',F')} - 1] E (\bmod p)$$

很显然，伪造群签名能够通过验证等式 $a_i'^{h(m',R')} = \delta_i'^{R'} R'^{s'} \cdot (\bmod p)$，因为

$$\begin{aligned} g^{s_i'} y_T^{r_i'} r_i' &= g^{s_i'} y_T^{r_i'} g^\delta y_T = g^{\delta r_i' + \delta} y_T^{r_i' + 1} = g^{\delta r_i' (1 + r_i'^{-1})} y_T^{r_i' (1 + r_i'^{-1})} \\ &= (g^{s_i'} y_T^{r_i'})^{(1 + r_i'^{-1})} = (g^{s_i'} y_T^{r_i'})^{x_i'} (\bmod p) \end{aligned}$$

$$\begin{aligned} a_i'^{x_i'} &= [g^{b' h(E',D',F')} + g^{s_i' a'} g^{-b' h(A',C',D',E',F')} g^{b' h(E',D',F')} \\ &\quad \cdot g^{x_T r_i' a'} g^{-x_T d'} g^{x_T d'} g^{b' h(A',C',D',E',F')}]^{x_i'} (\bmod p) \\ &= [g^{x_i' b' h(E',D',F')} (1 + g^{s_i' a'} g^{x_T r_i' a'})^{x_i'}] (\bmod p) \end{aligned}$$

$$\begin{aligned}\delta_i' &= A'^{h(E',D',F')}[a_i'D'^{-h(E',D',F')}-1]E'(\bmod p)\\ &= A'^{h(E',D',F')}[D'^{-h(E',D',F')}g^{B'}y_T^{C'}\\ &\quad\cdot F'D'^{h(A',C',D',E',F')}]E'(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{-bh(E',D',F')}g^{s_i'a'-b'h(A',C',D',E',F')+b'h(E',D',F')}\\ &\quad\cdot g^{x_T(r_i'a'-d')}g^{x_Td'}g^{b'h(A',C',D',E',F')}E'(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{s_i'a'}g^{x_Tr_i'a'}E'(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{s_i'a'}g^{x_Tr_i'a'}r_i'^{a'}(1+g^{-s_i'a'}y_T^{-r_i'a'})^{x_i'}(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{s_i'a'}g^{x_Tr_i'a'}r_i'^{a'}\\ &\quad\cdot((g^{-s_i'a'}y_T^{-r_i'a'})^{x_i'}(1+g^{s_i'a'}y_T^{r_i'a'})^{x_i'}(\bmod p)\\ &= g^{x_i'bh(E',D',F')}(g^{s_i'a'}y_T^{r_i'a'})^{x_i'a'}(g^{-s_i'a'}y_T^{-r_i'a'})^{x_i'}\\ &\quad\cdot(1+g^{s_i'a'}y_T^{r_i'a'})^{x_i'}(\bmod p)\\ &= g^{x_i'bh(E',D',F')}(1+g^{s_i'a'}y_T^{r_i'a'})^{x_i'}\cdot(\bmod p)\\ &= a_i'^{x_i'}(\bmod p)\end{aligned}$$

$$\begin{aligned}\therefore a_i'^{h(m',R')} &= a_i'^{(s't'+x_i'R')} = a_i'^{s't'}a_i'^{x_i'R'}\\ &= a_i'^{x_i'R'}R'^{s'} = \delta_i'^{R'}R'^{s'}(\bmod p)\end{aligned}\tag{8}$$

即伪造的签名能够通过签名验证方程。

不难发现，该伪造攻击策略是通过伪造一个能够通过证书验证方程的合法成员证书来实现的。由于 LD 群签名方案对群成员证书的构造策略与 WF 群签名相同，因此该伪造攻击策略也适应于 LD 群签名方案，进而可以推广到 Lee-Chang 群签名方案及由其演化而来的所有群签名方案，因为这些方案的群成员证书的构造策略都是相同的。

3.2 伪造攻击 2

以 WF 群签名为例，攻击者随机选择 $\delta\in Z_q^*$，计算 $r_i'=gy_T^{\delta}\bmod p$，$s_i'=\delta^{-1}r_i'\bmod p$，$x_i'=1+\delta r_i'^{-1}(\bmod q)$，$y_i'=g^{x_i'}(\bmod p)$，之后再随机选择 $a',b',d',t'\in Z_q^*$，并计算：

$$\begin{cases}C'=r_i'a'-d'(\bmod q),\ A'=g^{x_i'b'}(\bmod p),\ D'=g^{b'}(\bmod p)\\ E'=r_i'^{a'}(1+g^{-s_i'a'}y_T^{-r_i'a'})^{x_i'}(\bmod p),\ F'=y_T^{d'}(\bmod p)\\ B'=s_i'a'-b'h(A',C',D',E',F')+b'h(E',D',F')(\bmod q)\\ a_i'=[D'^{h(E',D',F')}+g^{B'}y_T^{C'}F'D'^{h(A',C',D',E',F')}](\bmod p)\\ R'=a_i'^{t'}(\bmod p),\ s'=t'^{-1}[h(m',R')-x_i'R'](\bmod q)\end{cases}\tag{9}$$

则 $\{s',R',A',B',C',D',E',m'\}$ 就是消息 m' 的一个伪造的有效盲群签名。

因为群签名验证者接收到伪造的签名 $\{s',R',A',B',C',D',E',m'\}$ 后，先计算：

$$\begin{aligned}a_i' &= [D'^{h(E',D',F')}+g^{B'}y_T^{C'}F'D'^{h(A',C',D',E',F')}](\bmod p)\\ \delta_i' &= A'^{h(E',D',F')}[a_i'D'^{-h(E',D',F')}-1]E(\bmod p)\end{aligned}$$

很显然，伪造群签名能够通过验证等式 $a_i'^{h(m',R')}=\delta_i'^{R'}R'^{s'}(\bmod p)$，因为

$$\begin{aligned}g^{s_i'}y_T^{r_i'}r_i' &= g^{s_i'}y_T^{r_i'}gy_T^{\delta} = g^{\delta^{-1}r_i'+1}y_T^{r_i'+\delta} = g^{\delta^{-1}r_i'(1+\delta r_i'^{-1})}y_T^{r_i'(1+\delta r_i'^{-1})}\\ &= (g^{s_i'}y_T^{r_i'})^{(1+\delta r_i'^{-1})} = (g^{s_i'}y_T^{r_i'})^{x_i'}(\bmod p)\\ a_i'^{x_i'} &= [g^{b'h(E',D',F')}+g^{s_i'a'}g^{-b'h(A',C',D',E',F')}g^{b'h(A',C',D',E',F')}\\ &\quad\cdot g^{x_Tr_i'a'}g^{-x_Td'}g^{x_Td'}g^{b'h(A',C',D',E',F')}]^{x_i'}(\bmod p)\\ &= [g^{x_i'b'h(E',D',F')}(1+g^{s_i'a'}g^{x_Tr_i'a'})^{x_i'}](\bmod p)\\ \delta_i' &= A'^{h(E',D',F')}[a_i'D'^{-h(E',D',F')}-1]E'(\bmod p)\\ &= A'^{h(E',D',F')}D'^{-h(E',D',F')}g^{B'}y_T^{C'}\\ &\quad\cdot F'D'^{h(A',C',D',E',F')}]E'(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{-bh(E',D',F')}g^{s_i'a'-b'h(A',C',D',E',F')+b'h(E',D',F')}\\ &\quad\cdot g^{x_T(r_i'a'-d')}g^{x_Td'}g^{b'h(A',C',D',E',F')}E'(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{s_i'a'}g^{x_Tr_i'a'}E'(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{s_i'a'}g^{x_Tr_i'a'}r_i'^{a'}(1+g^{-s_i'a'}y_T^{-r_i'a'})^{x_i'}(\bmod p)\\ &= g^{x_i'bh(E',D',F')}g^{s_i'a'}g^{x_Tr_i'a'}r_i'^{a'}\\ &\quad\cdot(g^{-s_i'a'}y_T^{-r_i'a'})^{x_i'}(1+g^{s_i'a'}y_T^{r_i'a'})^{x_i'}(\bmod p)\\ &= g^{x_i'bh(E',D',F')}(g^{s_i'a'}y_T^{r_i'a'})^{x_i'a'}(g^{-s_i'a'}y_T^{-r_i'a'})^{x_i'}\\ &\quad\cdot(1+g^{s_i'a'}y_T^{r_i'a'})^{x_i'}(\bmod p)\\ &= g^{x_i'bh(E',D',F')}(1+g^{s_i'a'}y_T^{r_i'a'})^{x_i'}\cdot(\bmod p)\\ &= a_i'^{x_i'}(\bmod p)\end{aligned}$$

$$\begin{aligned}\therefore a_i'^{h(m',R')} &= a_i'^{(s't'+x_i'R')} = a_i'^{s't'}a_i'^{x_i'R'}\\ &= a_i'^{x_i'R'}R'^{s'} = \delta_i'^{R'}R'^{s'}(\bmod p)\end{aligned}\tag{10}$$

即伪造的签名能够通过签名验证方程。同理，该伪造攻击策略也适应于 LD 群签名方案、Lee-Chang 群签名方案及由其演化而来的所有群签名方案。

4 结束语

本文讨论了由王晓明等和林松等最近依据 Tseng-Jan 群签名方案各自提出的一种群签名方案的安全性。通过分析显示，该方案是不安全的，任何攻击者都可利用伪造群成员证书方式来伪造有效的群签名，并提出两种伪造攻击策略。而且该伪造攻击构造策略可推广到 Lee-Chang 群签名方案及由其演化而来的所有群签名方案，从而证明该类群签名方案是不安全的。可见，在实际应用环境中，要构造一个安全的数字签名方案并不是一件简单的工作。

参 考 文 献

[1] Lee W B and Chang C C. Efficient group signature schemes based on discrete logarithm. *IEE Proc-Conput Digit Tech*, 1998, 145(1): 15–18.

[2] Tseng Y M and Jan J K. Improved group signature scheme based on discrete logarithm. *Electronics Letters*, 1999, 35(1): 37–38.

[3] 林松, 斜伟雨. 一种抗伪造攻击的改进的群签名方案. 四川大学学报(工程科学版), 2006, 38(1): 119–123.
Lin Song and Dou Wei-yu. A group signature scheme for resisting forgery attack. *Journal of Sichuan University* (*Engineering Science Edition*), 2006, 38(1): 119–123.

[4] 唐春明, 刘卓军, 王明生. 改进 Tseng-Jan 的群签名方案. 广

州大学学报(自然科学版), 2005, 4(3): 205–208.
Tang Chun-ming, Liu Zhuo-jun, and Wang Mings-heng. Improved Tseng-Jan 's group signature schemes. *Journal of Guangzhou University*(*Natural Science Edition*), 2005, 4(3): 205–208.

[5] 王晓明, 符方伟. 一种安全的群签名方案. 电子与信息学报, 2003, 25(5): 657–663.
Wang Xiao-ming and Fu Fang-wei. A secure group signature scheme. *Journal of Electronics & Information Technology*, 2003, 25(5): 657–663.

[6] 陈艳玲, 陈鲁生, 符方伟. 两种群签名方案的安全性分析. 电子与信息学报, 2005, 27(2): 235–238.
Chen Yan-ling, Chen Lus-heng, and Fu Fang-wei. Security cryptanalysis of two group signature schemes. *Journal of Electronics and Information Technology*, 2005, 27(2): 235–238.

[7] 曹正军. Wang-Fu 群签名方案的不可追踪性. 计算机工程与应用, 2006, 42(36): 142–143.
Cao Zheng-jun. Untraceability of Wang-Fugroup signature scheme. *Computer Engineering and Applications*, 2006, 42(36): 142–143.

于宝证：　男，1971 年生，博士生，副研究员，研究方向为电子商务和信息安全.

徐枞巍：　男，1956 年生，教授，研究方向为信息安全和高教管理.