对一种群签名方案的伪造攻击

李艳俊[①]　武玉华[①]　李梦东[①]　杨　刚[②]
[①](北京电子科技学院电子信息工程系　北京　100070)
[②](北京理工大学理学院　北京　100081)

摘　要：王晓明等人提出一种群签名方案(2003)，并称可以抵抗各种伪造攻击，而且可以进行群成员的注销，但是经过认真分析，该方案存在安全隐患:首先，无法进行有效注销群成员。其次，攻击者可以伪造签名通过验证而使群权威无法识别。本文提出一种有效的攻击方案，并给出安全群签名方案的应具备的两个要素。

关键词：离散对数；群签名；伪造攻击
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2007)07-1772-03

Forgery Attack to a Group Signature Scheme

Li Yan-jun[①]　Wu Yu-hua[①]　Li Meng-dong[①]　Yang Gang[②]
[①](*Department of Electronic Information Engineering, Beijing Electronic Science and Technology Institute,Beijing* 100070, *China*)
[②](*School of Science, Beijing Institute of Technology, Beijing* 100081, *China*)

Abstract: Wang XM proposed a group signature scheme and claimed that it can resist all kinds of forgery attacks(2003). However，it was carefully analyzed, and there were defects in it: First, It cannot revoke group member effectively. Second，It cannot resist forgery attack.. In this paper, an effective attack scheme is proposed, and two factors that a secure group signature scheme should possess was given.

Key words: Discrete algorithmic; Group signature; Forgery attack

1　引言

1998 年Lee和Chang提出一个有效的基于离散对数问题的群签名方案[1]；一年后，即 1999 年，Tseng和Jan指出了该方案的安全隐患：一旦某个成员的一个签名被打开，他以前的所有签名都能被验证者识别，这不满足签名的匿名性，因此提出了两种改进的方案[2]；然而，时隔不到一年，Tseng和Jan的两个方案就受到了Li等人的伪造攻击[3]，利用伪造攻击便可以伪造出有效的群签名。而一个安全的群签名方案应该具有以下 4 个基本要求：

(1)有效性　生成的群签名可以通过验证；

(2)匿名性　除群权威之外，任何人从签名无法识别签名者的身份和其他信息；

(3)可追踪性　发生纠纷时，群权威可以打开签名，指出签名者；

(4)不可伪造性　包括群权威在内的所有人都不能伪造他人的有效群签名而不被发现。

2001 年以来，许多群签名方案又增加了可撤销成员功能[4–6]，即不仅要满足以上 4 个基本要求，还应该满足：安全有效地做到群组成员的不断更新，包括群成员的加入和群成员的撤销，其中有效实现群成员的撤销较为困难(简称可撤销性或可注销性)。在撤销成员时，这些方案可分为两种情况：一种是通过重新分配或更改所有成员的签名证书并同时更改群公钥来撤销成员；另一种是设置撤销成员列表。第一种情况安全性较高，但效率较低，尤其是当成员撤销频率较大时，证书和公钥更换频繁，计算量极大。所以提倡使用第二种方法。

2003 年王晓明等人针对Li等人的伪造攻击提出一种可撤销成员的群签名方案[7]，该方案称可以有效防止各种伪造攻击，但是存在两个安全隐患：(1)成员的可注销性不成立；(2)攻击者可以伪造签名通过验证而不被群权威识别。本文对该方案的性能进行了详细分析，并提出了一个有效的伪造攻击方案，指出伪造群签名可以通过原方案验证，但是群权威却无法识别。最后，本文还分析了原方案被攻击的原因，指出设计有效群签名应该注意的两个关键要素。

2　王晓明等人的方案

2.1　安全参数

(1)p，q 为两个大素数，且 $q \mid (p-1)$，　g 是 GF(p)中阶为 q 的生成员。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 $y_i = g^{x_i} \bmod p$ 作为公钥，群权威 T 选择随机数 $x_T \in Z_q^*$ 作为私钥，计算 $y_T = g^{x_i} \bmod p$ 作为公钥。

2005-12-14 收到，2006-06-20 改回
国家自然科学基金(70431002)，北京市自然科学基金(4063040)和北京电子科技学院信息安全与保密重点实验室基金(YZDJ0507)资助课题

(3)安全的 Hash 函数 h，公开 h。

2.2 群成员的加入

当 u_i 加入群组时，先提交 y_i 给群权威 T，然后双方如下步骤执行：

(1) T 随即选取 $k_i \in Z_q^*$，并计算

$$r_i = g^{-k_i} y_i^{k_i} \bmod p_i, \quad s_i = k_i - r_i x_T \bmod q \tag{1}$$

秘密送 (s_i, r_i) 给 u_i，并存储 (s_i, r_i, k_i)。

(2) u_i 接到 (s_i, r_i) 后，验证

$$g^{s_i} y_T^{r_i} r_i = (g^{s_i} y_T^{r_i})^{x_i} \bmod p$$

若方程成立，则接收 (s_i, r_i)；反之，拒绝接收并停止。

2.3 群签名的产生过程

设待签名的消息为 m，u_i 随机选取 $a,b,d,t \in Z_q^*$ 并连同 (s_i, r_i)，计算 $C = r_i a - d \bmod q_i$，$A = y_i^b \bmod p$，$D = g^b \bmod p$，$E = r_i^a (1 + g^{-s_i a} y_T^{-r_i a})^{x_i} \bmod p$，$F = y_T^d \bmod p$，$B = s_i a - bh(A,C,E,F) + bh(E,D,F) \bmod q$，$a_i = [D^{h(E,D,F)} + g^B y_T^C F D^{h(A,C,D,E,F)}] \bmod p$，$R = a_i^t \bmod p$，$s = t^{-1}[h(m,R) - x_i R] \bmod q$。送 (s,R,A,B,C,D,E,m) 给签名验证者。

2.4 群签名的验证

群签名验证者计算 $a_i = D^{h(E,D,F)} + g^B y_T^C F D^{h(A,C,D,E,F)} \bmod p$，$\delta_i = A^{h(E,D,F)}[a_i D^{-h(E,D,F)} - 1] \cdot E \bmod p$，验证 $a_i^{h(m,R)} = \delta_i^R R^s \bmod p$。

2.5 群成员的识别

群权威 T 已存有每一个群成员的 (s_i, r_i, k_i) 可以预先计算

$$v_i = s_i^{-1} k_i \bmod q_i, \quad w_i = g^{v_i} \bmod p \tag{2}$$

并将 (v_i, w_i) 与 (s_i, r_i, k_i) 一起存储，如需要打开某一个群签名，T 可以查询已存的 (s_i, r_i, k_i) 和 (v_i, w_i)，判断哪个群成员对应的 (v_i, w_i) 满足：

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

于是 T 就能确定签名者的身份。

2.6 群成员的注销

注销某个群成员 (v_i, w_i) 时，群权威 T 先查询出对应的 (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

$$g^B y_T^C F D^{h(A,C,D,E,F)} = {w_i}^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \bmod p \tag{3}$$

如此式成立，则该群签名无效；否则，继续验证群签名的有效性，从而实现了群签名的注销。

3 对原群签名方案的分析

3.1 原方案可撤销性不成立

由原方案可知，每个成员都可以对签名进行验证，那么被撤销的成员 u_i 也可以查看到与自己签名相对应的 (v_i, w_i)，这时，u_i 可以利用 (s_i, r_i) 由式(2)计算得到 $k_i = s_i v_i \bmod q_i$，再由式(1)计算得到群权威的私钥 $x_T = r_i^{-1}(k_i - s_i) \bmod q$，那么成员 u_i 利用群权威的私钥便可以对任何人颁发有效的签名证书，由此一来，整个签名体系的安全性就会崩溃。所以原方案可撤销成员功能不成立。

3.2 对原方案的伪造攻击

即使不考虑可撤销性，该群签名方案也是不安全的，攻击者可以伪造群签名并通过验证，下面给出具体的伪造攻击方案。

3.2.1 系统初始化　参数选取

(1) p，q 为两个大素数，且 $q \mid (p-1)$，g 是 GF(p)中阶为 q 的生成员。公开 p，q，g。

(2)选择 SHA-1 做为 Hash 函数 h，公开 h。

公私钥对生成同原文。

3.2.2 群成员的加入同原文

3.2.3 伪造签名的生成　攻击者选取 4 个随机 a，b，c，t，对签名信息 m 计算：$A \equiv g^{ax_i} \bmod p$，$C \equiv c \bmod q$，$D \equiv g^a \bmod p$，$E \equiv g^{-b}(g^b + 1)^{x_i} \bmod p$，$F \equiv y_T^{-C} \bmod p$。由 $g^B D^{h(ACDEF)} \equiv g^b g^{ah(EDF)} \bmod p \Leftrightarrow B + ah(ACDEF) \equiv b + ah(EDF) \bmod q$，求出 B。

$\alpha_i = D^{h(EDF)} + g^B y_T^C F D^{h(ACDEF)} \bmod p$，$R \equiv \alpha_i^t \bmod p$

$s \equiv t^{-1}[h(m,R) - x_i R] \bmod q$。签名为 (s,R,A,B,C,D,E,F,m)。

3.2.4 验证签名　验证者接收到签名 (s,R,A,B,C,D,E,F,m) 后，计算 $\alpha_i = D^{h(EDF)} + g^B y_T^C F D^{h(ACDEF)} \bmod p$，$\delta_i \equiv A^{h(EDF)}[\alpha_i D^{-h(EDF)} - 1]E \bmod p$。伪造的签名可以通过验证方程 $a_i^{h(m,R)} = \delta_i^R R^s \bmod p$，下面给出证明。

证明

(1)

$$\begin{aligned}\alpha_i &= D^{h(EDF)} + g^B y_T^C F D^{h(ACDEF)} \bmod p \\ &= g^{ah(EDF)} + g^{b+ah(EDF)-ah(ACDEF)} y_T^C y_T^{-C} g^{ah(ACDEF)} \\ &\quad \cdot \bmod p \\ &= g^{ah(EDF)} + g^{b+ah(EDF)} \bmod p\end{aligned}$$

(2)

$$\begin{aligned}\delta_i &\equiv A^{h(EDF)}[\alpha_i D^{-h(EDF)} - 1]E \bmod p \\ &\equiv g^{ax_i h(EDF)}[\alpha_i g^{-ah(EDF)} - 1]g^{-b}(g^b + 1)^{x_i} \bmod p \\ &\equiv g^{ax_i h(EDF)}[(g^{ah(EDF)} + g^{b+ah(EDF)})g^{-ah(EDF)} - 1]g^{-b} \\ &\quad \cdot (g^b + 1)^{x_i} \bmod p \\ &\equiv g^{ax_i h(EDF)}(g^b + 1)^{x_i} \bmod p \\ &\equiv (g^b g^{ah(EDF)} + g^{ah(EDF)})^{x_i} \bmod p = (\alpha_i)^{x_i} \bmod p\end{aligned}$$

(3) $\delta_i^R R^s \equiv (a_i^{x_i})^R (a_i^t)^s \equiv a_i^{h(m,R)} \bmod p$。

3.2.5 群签名的识别　由于攻击者伪造的签名没有用到群权威 T 颁发的合法证书“(s_i, r_i)”，所以 T 无法用 (v_i, w_i) 对群签名进行识别。即识别签名者的式(3)不成立。

证明

$$\begin{aligned}\text{式(3)的左边} &= g^B y_T^C F D^{h(A,C,D,E,F)} \\ &= g^{b+ah(E,D,F)-ah(A,C,D,E,F)} y_T^C y_T^{-C} \\ &\quad \cdot g^{ah(A,C,D,E,F)} \bmod p \\ &= g^{b+ah(E,D,F)} \bmod p\end{aligned}$$

$$
\begin{aligned}
\text{而右边} &= w_i^B D^{[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \bmod p \\
&= w_i^{b+ah(E,D,F)-ah(A,C,D,E,F)} \\
&\quad \cdot g^{a[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \bmod p \\
&= g^{v_i[b+ah(E,D,F)-ah(A,C,D,E,F)]} \\
&\quad \cdot g^{a[h(A,C,D,E,F)v_i - h(E,D,F)v_i + h(E,D,F)]} \bmod p \\
&= g^{v_i b + ah(E,D,F)} \bmod p
\end{aligned}
$$

显然，左边 $\neq$ 右边，即证。

因此原方案不满足群签名的可识别性，它可以被伪造攻击。

4 被攻击原因

原方案被伪造攻击的原因主要在于以下两个原因。

4.1 验证群签名的过程与群权威秘密信息的无关性

虽然在 2.4 节中验证群签名时用到了群公钥 y_T，但是 y_T 在验证签名时没有起到解密的作用，而是在计算 α_i 和 δ_i 的过程中互相抵消了。此外，群权威授予群成员的秘密 (s_i, r_i)，虽然参与了签名的计算，但是验证签名时没有与之对应的公开值来检验，同公钥 y_T 一样，在计算过程中相互抵消了。

4.2 群成员的公钥与私钥无对应关系

由 3.2.4 节(2)式可知，δ_i 和 α_i 只要满足关系式 $\delta_i = (\alpha_i)^{x_i} \bmod p$，便可以通过验证方程 $a_i^{h(m,R)} = \delta_i^R R^s \bmod p$。这里 x_i 是 δ_i 以 α_i 为底的离散对数，与 x_i 相对应的公钥 y_i 并没有参加验证过程，所以攻击者可以选取随机数作为 x_i，只要满足 $\delta_i = (\alpha_i)^{x_i} \bmod p$，然后计算 $s \equiv t^{-1}[h(m,R) - x_i R] \bmod q$，那么就可以通过验证方程 $a_i^{h(m,R)} = \delta_i^R R^s \bmod p$。

综上所述，要设计有效的群签名方案，签名中必须含有群权威的秘密信息，而且与秘密信息相对应的群公钥 y_T 必须在验证方程中起到解密的作用；此外，签名成员的公钥必须包含在秘密信息中，使得群权威在检验签名时可以识别签名者。这样的群签名才能是有效的。

5 结束语

王晓明等人提出的群签名方案，称该方案具有成员可撤销性，而且可以有效防止各种伪造攻击。但经过本文的仔细分析，该方案在撤销某群成员后，会产生严重的安全隐患；而且任何攻击者可以伪造群签名并通过验证。一个有效的群签名方案必须满足前文提到的 4 个性质，但是实际中很多方案的设计总是顾此失彼。经归纳总结，目前公开发表的群签名方案普遍存在以下几方面不足：

(1)随着群组规模的扩大，完成签名和验证签名的工作量呈指数增长；

(2)群成员的签名方案无法兼顾匿名性和可识别性[8]；

(3)不能有效地执行群成员的撤销工作。

群签名的设计还有待进一步改进和完善，要设计出有效实用的方案，必须以严谨的态度学习科学理论知识，并且和实践相结合。

参 考 文 献

[1] Lee W and Chang C. Efficient group signature scheme based on discrete logarithm. *IEE Proc. Comput. Digital Techniques*, 1998, 145(1): 15–18.

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

[3] Li Z C and Hui L C K, *et al*.. Security of Tseng-Jan's group signature schemes. *Information Processing Letters*, 2000, 75(5): 187–189.

[4] 王尚平, 王育民, 王晓峰等. 群签名中成员撤销问题的更新算子解决方案. 软件学报, 2003, 14(11): 1911–1917.
Wang Shang-ping, Wang Yu-min, and Wang Xiao-feng, *et al*.. A new solution scheme for the member deletion problem in group signature by use of renew operator. *Journal of Software*, 2003, 14(11): 1911–1917.

[5] Lysyanskaya J. Dynamic accumulators and application to efficient revocation of anonymous credentials. Advances in Cryptology-CRYPTO 2002, LNCS, Springer-Verlag, 2002, 2442: 61–76.

[6] Kim H J, Lim J I, and Lee D H. Efficient and secure member deletion in group signature schemes. Information Security and Cryptology(ICISC 2000), LNCS, Springer-Verlag, 2001, 2015: 150–161.

[7] 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.

[8] 黄振杰, 郝艳华, 王育民. 授权群签名. 电子学报, 2004, 32(5): 774–777.
Huang Zhen-jie, Hao Yan-hua, and Wang Yu-min. Authorized group signature. *Acta Electronica Sinica*, 2004, 32(5): 774–777.

李艳俊： 女，1979 年生，讲师，硕士，主要从事密码学及协议等方面的研究工作.

武玉华： 男，1978 年生，讲师，硕士，主要从事信息系统、信息安全方面的研究工作.

李梦东： 男，1963 年生，教授，博士，主要从事密码学及算法等方面的研究工作.

杨 刚： 男，副教授，主要从事密码学方面的研究工作.