一种改进 TSENG-JAN 群签名的安全分析

张键红,王育民,张福泰
(西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 本文对一种改进的 Tseng-Jan 群签名进行安全性分析,指出了该方案具有广义伪造性和相关性,即任何人可以对任意消息签名,管理员却不能对签名者进行追踪;且能够区分两个不同的签名是否来自于同一个人.

关键词: 群签名; 广义伪造性; 相关性; 密码分析
中图分类号: TN918.2 **文献标识码**: A **文章编号**: 0372-2112 (2003) 04-0624-03

Security-Analysis of Modified Tseng-Jan Group Signature

ZHANG Jian-hong, WANG Yu-min, ZHANG Fu-tai
(National Key Lab of ISN, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: In this paper we analyze security of the Modified Tseng-Jan group signature which was presented. We show that the scheme is universally forgeable and linkable. That is, anyone can produce a valid group signature on any message without being traced by authority and makes it computationally hard to distinguish whether two different signatures are produced by the same group member or not.

Key words: group signature; universally forgeable; linkable; cryptanalysis

1 引言

随着电子商务的迅猛发展,传统的手写签名正在被数字签名所代替,由于数字签名的不可否认性和数据的完整性,数字签名正在进入现实生活. 自 1991 年 Chaum 和 Van Heyst[2]提出了群签名以来,群签名被广泛的研究并应用于不同的领域,如电子投票、电子拍卖、电子货币等. 当发生争议时,群管理员能够打开签名者的真实身份. 一个基本的群签名应具有匿名性即同一个群中的成员不能识别其他群成员的签名;不相关性即决定两个不同的签名是否来自于同一个人计算上是不可行的. 不可伪造性即任何多个群成员不能伪造其他成员的签名.

Tseng 和 Jan 给出了一种基于身份(ID)的群签名[5],文献[3,4]指出了该方案具有广义可伪造性,即任何人能够对任意消息 M 产生一个有效的签名. 并且群管理员不能追踪签名者;在文[3,4]中 Mare Joye 指出了 Tseng-Jan 的群签名不能抵制联合攻击即两个或两个以上的群成员能够勾结产生一个有效的且不能追踪的签名. 在文献[1]中 Constantin Popescu 基于 Tseng-Jan 的群签名提出了一种改进的群签名,并指出该方案的安全性是基于 e-次方根和离散对数问题的困难性. 本文针对文献[1]提出的群签名方案进行安全性分析,指出该方案实质上具有不可追踪可伪造性和相关性.

2 一种改进的 Tseng-Jan 的群签名方案

在本节对改进的 Tseng-Jan 群签名做一个简单的描述. 该签名方案包括四个实体:一个可信赖机构、一个群管理员、群成员和验证者. 可信赖机构充当协助者帮助系统建立系统参数,群管理员为群选择一对公/私钥对. 同时,与可信赖机构联合来发行新加入成员的资格证书;如果发生争执,群管理员可以打开签名来揭示签名者的真实身份. 群成员代表群匿名的签名;验证者通过群公钥来验证群签名的有效性.

2.1 密钥的产生

一个可信赖的机构选择两个大素数与文献[5]中素数选取要求一样,并且使得 $n = p_1 * p_2$. 同时,可信赖机构选择一个大整数 e(160bit),并使得 $\gcd(e, \phi(n)) = 1$. g 是一个大阶数的 Z_n^* 中元素即 $g \in Z_n^*$. Z_n 是一个整数环. 群管理员选择一个密钥 x,并计算相应的公钥 $y(y \equiv g^x \pmod n)$. 那么,群管理员的公钥就是 (n, e, g, y);私钥为 (p_1, p_2, x). $ID_i \in Z_n$ 是用户 U_i 的身份消息. $h(\cdot)$ 是一个无碰撞的哈希函数. 假设用户 U_i 要加入群(假设用户 U_i 和可信赖机构及群管理员的通信是安全的,秘密的),那么成员资格证书计算如下步骤. 可信赖机构首先要计算:

$$S_i = ID_i^{1/e} \pmod n$$

群管理员要计算:

$$x_i = (ID_i + eg)^x \pmod n$$

收稿日期:2002-09-20;修回日期:2002-11-29
基金项目:国家自然科学基金(No. 19931010)

那么用户 U_i 的成员资格证书就是二元组 (S_i, x_i).

2.2 消息签名

为了对一个消息 M 进行签名,一个拥有成员资格证书 (S_i, x_i) 的群成员 U_i. 首先,选择两个随机数 r_1 和 r_2,并且计算:

$$A \equiv y^{r_2 e} \pmod n$$
$$B \equiv x_i y^{S_i + r_1} \pmod n$$
$$C \equiv x_i y^{r_2} \pmod n$$
$$D \equiv S_i h(M \| A) + r_1 h(M \| A)$$

其中 $\|$ 表示两个二进制字符串的级连. 群成员 U_i 对消息 M 的签名就为 (A, B, C, D).

2.3 签名的验证

为了对群签名进行验证,一个验证者需要检验下列等式是否成立.

$$C^{eh(M\|A)} y^{eD} \equiv B^{eh(M\|A)} A^{h(M\|A)} \pmod n$$

如果等式成立说明群成员 U_i 对消息 M 的签名 (A, B, C, D) 是一个有效的签名.

2.4 签名的打开

在将来,如果发生争执,群管理员能够打开签名来恢复签名者的身份 (ID_i). 通过检验哪个身份 ID_i 满足下列等式来揭露签名者的身份.

$$(ID_i + eg)^{xe} \equiv C^e A^{-1} \pmod n$$

3 群签名的安全分析

在本节将对文[1]介绍的群签名方案进行安全性分析,并指出该群签名方案具有的缺陷广义伪造性和相关性.

在该群签名中 RSA 的选取是 $n = pq, p = 2p' + 1, q = 2q' + 1, p、q、p'、q'$ 为素数. 为了安全而言,应该使得运算限制在模 n 的二次剩余中即阶数为 p', q' 的循环子群 $QR(n)$. 在 Z_n^* 中的元素的阶数只能为 $\{1, 2, p', q', p'q', 2p', 2q'\}$,一般为了安全而言,我们选择 g 的阶数为 $p'q'$,由群论知识知道,与 n 不互素的元素为 kq 或 kp 且它们的阶数不是 $p'q'$,因而,有 $\gcd(g, n) = 1$. 下面讨论群签名的相关性和广义伪造性.

定理

当 $n = pq, p = 2p' + 1, q = 2q' + 1, p、q、p'、q'$ 为素数,那么对于 kp 或 kq 在 Z_n^* 中不能构成循环群.

证明　假如 kp(或 kq)在 Z_n^* 中能构成循环群且阶数为 α,那么,有 $(kp)^\alpha \equiv 1 \pmod n$ 因而有 $pq \mid (kp)^\alpha - 1$ 但是 p 不能整除 $(kp)^\alpha - 1$,因而必须 $\alpha = 0$. 所以,在 Z_n^* 不能构成循环群.

3.1 可区分性(相关性)

可区分性就是指群签名的相关性即两个不同的群签名可以区分是否来自于同一个签名者. 由于对拥有一个资格证书 (S_i, x_i) 的群成员 U_i 而言,S_i 和 x_i 对于群成员 U_i 是一个固定的常量. 由上文可知群签名 (A, B, C, D). 其中 $C \equiv x_i y^{r_2} \pmod n$, $A \equiv y^{r_2 e} \pmod n$. 由于 e, n 是公开的,所以可以计算 $C^e = x_i^e y^{er_2}$. 因此,有下列常数:

$$C^e / A = x_i^e y^{er_2} / y^{er_2} = x_i^e \pmod n$$

由于对于同一个签名者而言,x_i 是一个固定的数;并且 e 是一个公钥值也是一个固定的常数,因而得到 x_i^e 是一个常数. 对于同一个签名者而言,他的两个签名 (A_1, B_1, C_1, D_1) 和 (A_2, B_2, C_2, D_2) 具有关系 $C_1^e / A_1 = x_i^e = C_2^e / A_2$,所以他的两个签名是可以区分的. 与群签名的不可相关性相矛盾. 因而,对两个不同消息的签名,可以推知是否来自于同一个签名者. 这样签名具有了相关性.

3.2 广义伪造性

广义伪造性就是指任何人可以对任何消息进行伪造. 由上文介绍的的验证算法代入签名 (A, B, C, D),可以发现等式:

$$\begin{aligned} C^{eh(M\|A)} y^{eD} &\equiv B^{eh(M\|A)} A^{h(M\|A)} \bmod(n) \\ &\Leftrightarrow (x_i y^{r_2})^{eh(M\|A)} y^{eD} \equiv (x_i y^{S_i + r_i})^{eh(M\|A)} \\ &(y^{r_2 e})^{h(M\|A)} \pmod n \Leftrightarrow x_i^{eh(M\|A)} y^{r_2 eh(M\|A) + eD} \\ &\equiv x_i^{eh(M\|A)} y^{S_i eh(M\|A) + r_1 eh(M\|A) + r_2 eh(M\|A)} \pmod n \\ &\Leftrightarrow y^{eD} \equiv y^{S_i eh(M\|A) + r_1 eh(M\|A)} \pmod n \Leftrightarrow y^{eS_i h(M\|A)} \\ &\equiv y^{S_i eh(M\|A)} \pmod n \end{aligned} \quad (1)$$

在式(1)的两端是两个相等的数值. 所以,可以以任意的二元组 (S_i', x_i') 作为群成员的的资格证书. 那么对任意的消息签名步骤为:

(a) 首先,选择任意两个随机数 r_1' 和 r_2'.

(b) 计算签名:$A' = y^{r_2' e} \pmod n$, $B' = x_i' y^{S_i' + r_1'} \pmod n$, $C' = x_i' y^{r_2'} \pmod n$, $D' = S_i' h(M \| A') + r_1' h(M \| A')$

最后,对消息 M 的签名就是 (A', B', C', D'). 当代入验证公式后,可以发现满足验证公式. 也可以通过验证公式逆向推导来得到一个签名.

之所以可以伪造签名主要因为验证公式中 x_i, S_i,实际上并没有起什么作用,在签名过程中签名者并没有证明他拥有资格证书 (x_i, S_i),他们之间的关系在验证公式中没有真正的体现. 同时,由式(1)可知,对于任意一个数 S 都满足 $y^{eSH(M\|A)} = y^{eSH(M\|A)}$,一步一步的后退验证公式,就可知 x_i, S_i 可以为任意数. 因而该群签名方案具有广义伪造性,由于任意的二元组可以作为群成员的资格证书,所以群管理员不能对签名者进行追踪.

4 结论

本文针对一种改进的 Tseng-Jan 群签名方案进行了安全分析,指出了该群签名方案具有广义伪造性,不可追踪性和相关性. 其安全性也并不基于文献[1]中所说的离散对数和 e-次方根的困难性.

参考文献:

[1] Constantin popescu. A modification of the tseng-Jan group signature scheme [J]. Studla Univ. Babes-Bolyai Informatica, Volume XLV, Number 2, 2000.

[2] David Chaum, Eugene van Heyst. Group signatures [A]. Advance in Cryptology EUROCRYP-T '91 Lecture Notes in Computer Science [C]. Springer-Verlag, Berlin, Vol, 547, 1991, pp 257 - 265.

[3] Marc Joye. On the difficulty of coalition-Resistance in group signature schemes (II) [R]. LCIS Tech. Report TR-99-6B, Tamkang University, June 1999.

[4] Mare Joye. On the difficulty of coalition-resistance in group signature scheme(I) [R]. Tech Report 98-17B, LCIS Tamkang, Tamsui, November 1998.

[5] Y Tseng, J Jan. A novel ID-based group signature [A]. In T L Hwang and A K Lenstra, editors, 1998 international Computer Symposium, Workshop on Cryptology and Information Security [C]. Tainan, 1998. 159 - 164.

作者简介:

张键红 男,1975/11/03 出生于河北省石家庄市,1998 年获河北师范大学数学系理学学士,2001 获计算机工学硕士,现在西安电子科技大学攻读博士学位,主要感兴趣方向电子商务安全数字签名和公平交换、网络安全和计算机软件. jhzh@nhe.net; jhzhs@hotmail.com

王育民 (见本期第 584 页)

中国人工智能学会 2003 全国学术大会(CAAI-10)

征 文 通 知

为了总结 2001 年中国人工智能学会全国学术年会以来的新进展,交流我国智能领域的自主创新成就,探讨人工智能未来的发展,中国人工智能学会决定 2003 年 11 月 19 至 21 日在广州召开第十届全国学术大会(CAAI-10),由广东工业大学承办. 欢迎从事人工智能领域研究、教学、应用的科技工作者、大专院校师生、以及一切有志于人工智能事业的朋友踊跃投稿.

大会将邀请著名科学家做前沿报告,同时将举行《中韩智能系统学术研讨会》. 凡被程序委员会录用的论文,将由北京邮电大学出版社正式出版专书《中国人工智能进展:2003》,并将从这些论文中评选授奖论文.

学术大会征文范围包括(但不限于):

理论创新:逻辑学,离散数学,模糊集-粗糙集,认知学,控制论,系统学,信息-知识-智能理论,可拓学,哲学,信息化与智能化

技术创新:机器学习,智能机器人,专家系统,知识工程与分布智能,智能控制与智能管理,神经网络与计算智能,自然语言理解,机器翻译,机器感知与虚拟现实,生物信息学与人工生命,计算机辅助教育,智能 CAD,智能制造,可拓工程,智能信息网络,智能系统工程,集对分析与联系数

应用发展:机器人足球,人工智能产品标准与产业发展,人工智能教育,人工智能普及,智能技术在各个领域的应用

征文截止日期:2003 年 7 月 31 日

详情请访问中国人工智能学会网站:http://caai.org.cn