对一种改进的群签名方案的密码学分析

鲁荣波[1],王常吉[2],何大可[3]
LU Rong-bo[1],WANG Chang-ji[2],HE Da-ke[3]

1.吉首大学 数学与计算机科学学院,湖南 吉首 416000
2.中山大学 计算机科学系,广州 510275
3.西南交通大学 信息安全与国家计算网格实验室,成都 610031
1.College of Math. and Computer Science,Jishou University,Jishou,Hunan 416000,China
2.Dept. of Computer Science,Sun Yat-Sen University,Guangzhou 510275,China
3.Laboratory of Information Security and National Computing Gird,Southwest Jiaotong University,Chengdu 610031,China
E-mail:lurongbo8563@163.com

LU Rong-bo,WANG Chang-ji,HE Da-ke.Cryptanalysis of improved group signature scheme.Computer Engineering and Applications,2007,43(33):22-23.

Abstract: An improved group signature scheme proposed by G.D.Si et al has been analyzed.We have showed that the scheme is insecure.The revocation center cannot open a valid group signature,so the group signature is not tracked.Meanwhile,the group manager can forge group signatures that could be verified by a verifier.And the scheme does not satisfy the properties of against coalition attack.Two group members can conspire to generate valid group signatures.
Key words: group signature;security analysis;forge attack;coalition attack

摘 要:对司光东等人提出的一种改进的群签名方案进行安全性分析,指出该方案是不安全的:群管理员不能够打开一个群签名,该群签名是不可跟踪的;群管理员可以伪造一个能通过验证的群签名;同时该方案并不能抵抗联合攻击,两个群成员合谋后可以伪造出有效的群签名。
关键词:群签名;安全性分析;伪造攻击;联合攻击
文章编号:1002-8331(2007)33-0022-02 **文献标识码:**A **中图分类号:**TP309

1 引言

群签名最早是 Chaum 和 Heyst 在 1991 年提出来的[1]。群成员允许任何群成员代表群进行匿名的签名,如发生争执,群管理员可以(或者借助一个第三方)揭示签名者的身份。由于群签名很好地为签名者(群成员)提供隐私保护,群签名在不同的领域越来越得到广泛的应用,如电子货币、电子选举、电子拍卖等,目前,人们已经提出了若干不同类型的群签名方案[2-4]2000 年,ATENIESE 等人提出了一个新的群签名方案(简称为 ACJT 方案)[5]。在安全性方面,ACJT 方案的成员加入协议关于新成员所选取的秘密值满足统计上的零知识,且已得到证明可以抵抗自适应的攻击者所发动的联合攻击。ACJT 方案是目前较为理想的方案。

一般而言, 一个安全有效的群签名需要满足以下安全性需求:

(1)可验证性:利用公开的信息,一个合法的群成员按照签名算法产生的群签名一定能够通过验证算法。

(2)不可伪造性:非群成员要产生一个通过验证算法的群签名在计算上是不可能的。

(3)匿名性:给定对任意消息的一个群签名,除了群管理员外,决定该签名是由哪个群成员产生在计算上是不可能的。

(4)不可否认性:群管理员总能确定合法签名者的身份。并且群管理员还能向其他实体(比如法官)证明: 给定的文档是由哪个成员签署的,同时不会泄露此成员以前或将来可能签署的消息的匿名性。

(5)可追踪性:一个正确的签名可以被群管理员揭开签字者的身份。

(6)抗联合勾结性:任何多个群成员勾结或与群管理员勾结都不能伪造其他群成员的签名。

(7)不可关联性:除群管理员外的任何人不能判定两个不同的签名是否由同一个成员所为。

(8)抗陷害攻击:群中没有任何子集(包含群管理员) 能代表群中其他成员签署消息。即群中任何子集都不能"陷害"不属于该子集的其他成员。

(9)防止滥用性:群成员不能使用群成员证书进行除合法的群签名外的任何活动,如果发生误用甚至滥用,安全有效的群签名必须具备追究群成员责任的能力。

文献[7]基于 RSA 签名给出了一种群签名方案(以下简称 Zhang-Wu-Zou-Wang 方案),并得出了签名和验证的计算量远

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60503005)。
作者简介:鲁荣波(1970-),男,副教授,博士,主要研究方向信息安全、电子支付;王常吉,博士,副教授,主要研究方向电子支付和密码学理论与应用;何大可,教授,博士生导师,主要研究方向网络安全、信息安全、电子支付、并行计算。

远少于 ACJT 方案、满足不可伪造性及抗联合攻击等结论。文献[8,9]分别指出了该方案在签名跟踪性及抗联合攻击等方面存在的安全漏洞;文献[10]指出了该方案在模运算下的错误,同时在原方案的基础上,把撤销中心的工作移交给群管理员,提出了一种改进方案(以下简称 Si-Li-Xiao 方案),并声称改进的方案弥补了原方案的安全缺陷。对 Si-Li-Xiao 方案进行了安全性分析,分析表明,该方案仍然存在安全缺陷:群签名是不可跟踪的;群管理员可以伪造能通过验证的群签名(Zhang-Wu-Zou-Wang 方案并不存在该安全漏洞);同时,该方案也不能抵抗联合攻击,两个群成员合谋后可以伪造出有效的群签名。

2 Si-Li-Xiao 方案介绍

2.1 参数的选择

群管理员选择五个大素数 p_1,p_2,f,p_1',p_2', 满足 $p_1=2fp_1'+1$, $p_2=2fp_2'+1$, 计算 $n=p_1p_2$, 生成乘法群 Z_n^*, $ID_G\in Z_n^*$ 为群管理员的身份。随机选择整数 e, 满足 $gcd(e,\varphi(n))=1$, 计算 d 满足 $ed=1 \bmod \varphi(n)$, $\varphi(n)$ 是欧拉函数;$g\in Z_{n_G}^*$ 的阶为 f。$h(\cdot)$ 为无碰撞的哈希函数。群管理员的私钥为 $x_G\in Z_n^*$, 公钥为 $y_G=g^{x_G} \bmod n_G$。公开 $(n,e,y_G,ID_G,h(\cdot))$, 其余保密。

2.2 群成员的加入

(1)Bob:选择 $x\in Z_n^*$, 并计算其身份 $ID_B=g^x \bmod n$ 以及知识签名 $\delta=SPK\{r:ID_B=g^r\}(")$ 并把 (ID_B,δ) 传给群管理员。

(2)群管理员:通过 (ID_B,δ) 验证知识签名的正确性。

(3)群管理员:随机选择 $\alpha\in Z_n^*$, 计算:

$r=g^\alpha \bmod n$

$s=\alpha+rx_Gh(ID_B) \bmod f$

$w=(ID_Gry_G^{rh(ID_B)}ID_B)^{-d} \bmod n$

在群成员数据库中存储 (r,s,w,ID_B) 并通过秘密信道发送 (r,s,w) 给 Bob。

(4)Bob 验证:$g^s=ry_G^{rh(ID_B)} \bmod n$, $w^{-e}=ID_Gry_G^{rh(ID_B)}ID_B \bmod n$。若成立,则群成员 Bob 的成员资格证书 (r,s,w)。

2.3 群签名的产生

Bob 随机选择 $q_1,q_2\in Z_n^*$, 计算:$z=q_2^eg^{q_1} \bmod n$, $u=h(z,m)$, $r_1=q_1+(s+x)u$, $r_2=q_2w^u \bmod n$, 得到群签名 (u,r_1,r_2,m)。

2.4 群签名的验证

验证者收到群签名 (u,r_1,r_2,m), 计算:$z'=ID_G^ug^{r_1}r_2^e \bmod n$, $u'=h(z',m)$。

验证:$u=u'$ 是否成立,如成立,群签名有效。

2.5 群签名的打开

群管理员保存有群成员的个人信息 (r,s,w,ID_B), 对一个群签名 (u,r_1,r_2,m), 群管理员通过以下计算来揭示签名者的真实身份:

(1)计算:$\eta=1/u \bmod \varphi(n)$, $\delta=ID_G^ug^{r_1} \bmod n$。

(2)检验 (g^s,ID_B) 是否满足等式:$ID_B=(g^{r_1}/\delta g^{us})^\eta/w^e \bmod n$, 如果满足,则 ID_B 就是真实签名者。

3 对 Si-Li-Xiao 方案的密码学分析

文献[10]声称该方案弥补了 Zhang-Wu-Zou-Wang 方案的安全漏洞。对文献[10]方案的分析表明,该方案仍然存在安全缺陷:群签名是不可跟踪的;群管理员可以伪造一个能通过验证的群签名(Zhang-Wu-Zou-Wang 方案并不存在该安全漏洞);该群签名也不能抵抗联合攻击。

3.1 群签名是不可跟踪的

文中给出的群签名打开方程式是错误的,事实上,给定一个群签名 (u,r_1,r_2,m), 对任意一个群成员及其相应的 $(r_i,s_i,w_i,ID_{B,i},ID_G)$, 其中 (r_i,s_i,w_i) 为其群成员证书,$ID_{B,i}$ 为其身份,ID_G 为群管理员的身份。

因为:$g^{s_i}=r_iy_G^{r_ih(ID_{B,i})} \bmod n$

$$w_i=(ID_Gr_iy_G^{r_ih(ID_{B,i})}ID_{B,i})^{-d} \bmod n=(ID_Gg^{s_i}ID_{B,i})^{-d} \bmod n$$

所以:$$ID_{B,i}=\frac{1}{ID_Gg^{s_i}(ID_Gg^{s_i}ID_{B,i})^{-1}}=\frac{1}{ID_Gg^{s_i}((ID_Gg^{s_i}ID_{B,i})^{-d})^e)}=$$

$$\frac{1}{ID_Gg^{s_i}w_i^e}=(\frac{1}{ID_G^ug^{us_i}})^{\frac{1}{u}}/w_i^e=(g^{r_1}/ID_G^ug^{r_1}g^{us_i})^\eta/w_i^e=$$

$$\frac{(g^{r_1}/\delta g^{us_i})^\eta}{w_i^e} \bmod n$$

即给定一个群签名 (u,r_1,r_2,m), 对任意的 i 都有:$ID_{B,i}=(g^{r_1}/\delta g^{us_i})^\eta/w_i^e$, 从而该方程不能确认群成员的身份,因此该群签名是不可跟踪的。

3.2 群管理员的伪造攻击

Zhang-Wu-Zou-Wang 方案可以抵抗群管理员的伪造攻击,文献[9]声称继承了该安全特性。但事实上,Si-Li-Xiao 方案并不能抵抗群管理员的伪造攻击。具体的攻击过程如下:

群管理员随机选取 $r_1\in Z, z\in Z_n^*$, 令 $u=h(z,m)$, 计算:$r_2=(ID_G^{-u}g^{-r_1}z)^d \bmod n$。则 (u,r_1,r_2,m) 是一个能通过验证的群签名。

对以上由群管理员伪造的群签名 (u,r_1,r_2,m) 进行验证时,验证者按照通常的验证方程,首先计算:$z'=(ID_G^ug^{r_1}r_2^e)=ID_G^ug^{r_1}((ID_G^{-u}g^{-r_1}z)^d)^e=z \bmod n$。显然有 $u=h(z,m)=h(z',m)$ 成立,验证者接受 (u,r_1,r_2,m) 为一个有效的群签名。

3.3 对群签名的联合攻击

联合攻击是指部分合法群成员勾结起来产生一个能通过签名验证算法又不被群管理者跟踪的签名。下面就给出一个针对 Si-Li-Xiao 群签名方案的联合攻击。

(1)Alice 以身份 $ID_A=g^{x_A} \bmod n$ 加入群中,其中 $x_A\in Z_n^*$。得到一个群成员证书 (r_A,s_A,w_A), 则 $w_A^{-e}=ID_Gg^{s_A}ID_A \bmod n$。

(2)Charlie 以身份 $ID_C=g^{x_C} \bmod n$ 加入群中,其中 $x_C\in Z_n^*$。得到一个群成员证书 (r_C,s_C,w_C), 则 $w_C^{-e}=ID_Gg^{s_C}ID_C \bmod n$。

(3)Alice 和 Charlie 共同选择 $r\in Z$, 则有 $w_A^{-e}(g^{x_C-x_A+s_C-s_A})^r=ID_GID_Ag^{s_A}(w_Aw_c^{-1})^{re}$。即 $(w_c^rw_A^{1-r})^eg^{s_A+x_A+r(x_c-x_A+s_c-s_A)}=ID_G^{-1}$。

(4)Alice 和 Charlie 共同选择 $x_*\in Z_n^*$, 令 $ID_*=g^{x_*} \bmod n$, $w_*=w_c^rw_A^{1-r} \bmod n$, $s_*=s_A+x_A+r(x_C-x_A+s_C-s_A)-x_*$。显然有 $w_*^{-e}=ID_Gg^{s_*}ID_* \bmod n$。

(5)利用 (s_*,w_*,x_*,ID_*) 按照群签名产生算法产生对任意消息 m 的群签名,如下:

(下转 62 页)