第43卷 第2期 西 安 交 通 大 学 学 报 Vol. 43 №2
2009年2月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Feb. 2009

采用中国剩余定理的群签名方案的安全性分析与改进

李新社[1]，乐开端[2]，胡予濮[1]
(1. 西安电子科技大学计算机网络与信息安全教育部重点实验室，710071，西安；
2. 西安交通大学机械制造系统工程国家重点实验室，710049，西安)

摘要：运用RSA公钥密码体制共模攻击原理，分析了Chen方案的安全性，证明Chen方案在群成员的加入、删除、身份验证等环节中存在安全漏洞：只需在任一群成员帮助下，不需经过群中心，任何攻击者都可伪装成群成员，群成员之间也可以互相伪造签名. 针对Chen方案存在的安全缺陷，提出了一种新型的群签名方案，并对其安全性数学原理进行了分析和研究. 结果表明，该新方案可以抵抗共模攻击，具有可撤消、不可伪造、抗联合攻击、防陷害等性质.

关键词：群签名；成员删除；密码系统；共模攻击
中图分类号：TN918.1 **文献标志码**：A **文章编号**：0253-987X(2009)02-0077-04

Security Analysis and Improvement of a Group Signature Scheme Based on Chinese Remainder Theory

LI Xinshe[1], YUE Kaiduan[2], HU Yupu[1]
(1. Ministry of Education Key Laboratory of Computer Network & Information Security, Xidian University, Xi′an 710071, China;
2. State Key Laboratory of Mechanical System Engineering, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: The security of Chen scheme is analyzed with common modulus attack method of RSA public key cryptography, and some secure shortages in the process of adding, deleting and verifying a group member are detected. With the help of a legal group member in Chen scheme, any attacker who tries to bypass the group center can disguise himself as a group member, and group members can forge a signature each other. To get rid of the secure shortages in Chen scheme, a novel group signature scheme is proposed, and its security mathematics principle is analyzed to show that the new scheme is immune to common modulus attack with revocable property, unforgeability, coalition-resistance, security against framing attack, etc.

Keywords: group signature; member deletion; cryptography; common modulus attack

数字签名技术引起了学术界尤其是密码学界和计算机网络界的广泛关注，特别是随着电子商务的提出，数字签名技术获得了更加广泛的研究和应用. 群签名是新发展起来的一种数字签名技术，由Chaum和van Heyst于1991年提出[1]. 在群签名中，如果可以在不改变其他有效群成员密钥的情况下，安全地撤消群成员，我们称该群签名方案具有可撤消性. 在目前研制的授权群签名方案[2]、ACJT群签名方案[3]、基于Java的身份认证数字签名方案[4]、动态门限群签名方案[5]等中，虽然关注了可撤消性，但当增加或撤消一个成员时，都要改变更新密钥，而且其他群成员都要根据这个改变了的更新密钥去更新自己的密钥，并且在更新密钥时需要大量的指数运算，给其他成员带来繁重的额外开销. 文献

收稿日期：2008-04-12. 作者简介：李新社(1965—)，男，副教授. 基金项目：国家自然科学基金资助项目(50775172)；国家重点基础研究发展规划资助项目(2007CB311201).

[6]提出了一种基于中国剩余定理(CRT)的群签名方案,在不改变其他有效群成员密钥的情况下,认为可以安全地撤消群成员.本文运用RSA公钥密码体制共模攻击原理[7]对Chen方案进行了安全性分析,发现该方案是不安全的,并在此基础上,对Chen方案进行了改进,提出了一种新型方案,同时分析了该新方案的安全性和实用性.

1 Chen群签名方案简介

(1)系统建立.群中心秘密地选择两个大素数p、q和一个hash函数h,计算$n=pq$,选择$e\in Z_n$,并求d,使$ed\equiv1(\mathrm{mod}\phi(n))$,其中$\phi(n)$是欧拉函数.将$e$作为群中心的公钥,$d$作为群中心的私钥,随机选择$x_i,y_i\in Z_n$,使得$x_iy_i\equiv1(\mathrm{mod}\phi(n))$,并选择素数$p_i$大于$y_i$,将$(x_i,p_i,p_i^d)$秘密送给群成员.群成员验证公式$p_i\equiv(p_i^d)^e(\mathrm{mod}n)$是否成立,如果成立,相信$(x_i,p_i,p_i^d)$是群中心送来的,并将其作为签名密钥保存.群中心将$(\mathrm{ID}_i,y_i)$送给群管理员,其中$\mathrm{ID}_i$是用户$U_i$的身份.假设系统有$k$个成员,则应用中国剩余定理可求得同余方程组

$$c\equiv y_i(\mathrm{mod}p_i)\qquad i=1,\cdots,k$$
$$\gcd(p_i,p_j)=1\qquad i\neq j$$

的解为

$$c\equiv y_1P_1'P_1+y_2P_2'P_2+\cdots+y_kP_k'P_k(\mathrm{mod}P)$$

其中$P=p_1p_2\cdots p_k$,$P_ip_i=P$,$P_i'\ P_i=1(\mathrm{mod}p_i)$.

将(n,e,c)作为群公钥发布.

(2)成员加入.群中心为新成员Bob随机选择$x_{k+1},y_{k+1}\in Z_n$,使得$x_{k+1}y_{k+1}\equiv1(\mathrm{mod}\phi(n))$,选择素数$p_{k+1}>y_{k+1}$,且$\gcd(p_i,p_{k+1})=1,i=1,\cdots,k$,重新计算$c$,并将$(x_{k+1},p_{k+1},p_{k+1}^d)$发送给Bob,将$(\mathrm{ID}_{k+1},y_{k+1})$送给群管理员.

(3)成员撤消.与加入过程类似,为了撤消成员U_i,群中心将y_i改为另外的一个随机数y_i',并重新计算c.

(4)群签名生成.对任意消息m,计算$s_i\equiv h(m)^{x_i}(\mathrm{mod}n)$,则$(m,s_i,p_i^d)$为成员$U_i$对消息$m$的签名.

(5)群签名验证.若Alice要对签名(m,s_i,p_i^d)进行验证,首先由群中心的公钥e,计算$p_i\equiv(p_i^d)^e(\mathrm{mod}n)$以及$y_i\equiv c(\mathrm{mod}p_i)$,接着验证$h(m)\equiv s_i^{y_i}(\mathrm{mod}n)$是否成立,成立则签名正确,否则签名不正确.

(6)群签名打开.给出签名(m,s_i,p_i^d)后,群管理员计算$p_i\equiv(p_i^d)^e(\mathrm{mod}n)$以及$y_i\equiv c(\mathrm{mod}p_i)$,然后通过与$y_i$相应的$\mathrm{ID}_i$确定签名成员的身份.

2 Chen方案的安全性分析

2.1 Chen方案不具有不可伪造性

不可伪造性是指只有群成员才能代表群进行签名,其他任何人都不能进行这样的合法签名.由于Chen方案所有的成员共模,那么对于系统中的任意一个用户Alice,用A表示,她持有$(x_\mathrm{A},y_\mathrm{A},p_\mathrm{A},P_\mathrm{A}^d)$以及系统的公钥$(n,e,c)$,Alice可以计算群中心私钥$d$的等效密钥.

因为

$$x_\mathrm{A}y_\mathrm{A}\equiv1(\mathrm{mod}\phi(n));\text{即 }x_\mathrm{A}y_\mathrm{A}-1=k\phi(n)$$

由于

$$(e,\phi(n))=1\tag{1}$$

不妨设

$$(e,k\phi(n))=1\tag{2}$$

如果$(e,k\phi(n))=s>1$,则令$k'=k/s$,那么$(e,k'\phi(n))=1$,则可以由欧几里德算法求得d',使

$$d'e\equiv1(\mathrm{mod}k'\phi(n))\tag{3}$$

那么d'就是所求的群中心私钥d的等效密钥.

有了这个等效密钥,就可以伪造系统授权,让任何人成为群成员.假设Tom不是群成员,我们试图不经过群中心而使Tom成为一个“群成员”,下面是具体步骤.

(1)选择素数p_T,使$y_\mathrm{T}\equiv c(\mathrm{mod}p_\mathrm{T})$且$(y_\mathrm{T},k\phi(n))=1$,计算$p_\mathrm{T}^{d'}$.

(2)由欧几里德算法求出x_T,使得$x_\mathrm{T}y_\mathrm{T}\equiv1(\mathrm{mod}k\phi(n))$.

(3)将$(x_\mathrm{T},p_\mathrm{T},p_\mathrm{T}^{d'})$和$(y_\mathrm{T},\mathrm{ID}_\mathrm{T})$假冒群中心分别送给Tom和群管理员.因为有$p_\mathrm{T}^{d'}$作为群中心对$p_\mathrm{T}$的签名,Tom可以通过群中心的公钥$e$验证该签名,所以Tom有理由相信这是群中心送来的,所以Tom会将其保存以待验证,而群中心对此毫不知情,所以仍然维持系统公钥(n,e,c)的使用.

(4)对任意消息m,Tom可以产生群签名$(m,h(m)^{x_\mathrm{T}},p_\mathrm{T}^{d'})$.

(5)通过$p_\mathrm{T}\equiv(p_\mathrm{T}^{d'})^e(\mathrm{mod}n)$,$y_\mathrm{T}\equiv c(\mathrm{mod}p_\mathrm{T})$,$(h(m)^{x_\mathrm{T}})^{y_\mathrm{T}}\equiv h(m)(\mathrm{mod}n)$,任何人可以验证上述签名,并且群管理员打开签名得到的是Tom的身份信息ID_T.

证明Tom是假群成员的惟一方法是核对群中心所有的(x,p,p^d),将它们与$p_\mathrm{T}^{d'}$对比,并计算c.由于无法预测什么时候会出现假成员,因此给Tom制造很多伪造机会.

2.2 Chen 方案不具有防陷害性

Alice 根据自己持有的(x_A, y_A, p_A, P_A^d)，以及系统的公钥(n,e,c)也可以求得任意现有群成员（不妨设为 Bob）的私钥 x_B 的等效私钥 x'_B，从而伪造任何成员 Bob 的签名.

因为 Alice 可以从群中心的公钥中求得 Bob 的公开密钥，即

$$(p_B^d)^e \equiv p_B(\mathrm{mod}n)$$

$$y_B \equiv c(\mathrm{mod}p_B);\ (y_B, \phi(n)) = 1$$

同样不妨设

$$(y_B, k\phi(n)) = 1 \tag{4}$$

则可以由欧几里德算法求得

$$x'_B y_B(\mathrm{mod}k\phi(n)) = 1 \tag{5}$$

于是 Alice 就可以伪造 Bob 对消息 m 的签名$(m, h(m)^{x'_B}, p_B^d)$. 任何人都可以通过群中心来验证这个伪造的签名，认为其是合法的，那么 Alice 就可以轻易地陷害 Bob.

此外，尽管不同群成员私钥不同，但之间共模，所以签名公钥 y_B 也不相同，即不同成员签名公钥不同，因此任何人都可以验证两个都使用 y_B 作为签名公钥的群签名是同一个群成员所为，也就是说，Chen 方案不满足不可关联性.

3 新型方案

(1)系统建立. 群中心秘密地选择两个大素数 p、q 和一个 hash 函数 h，计算 $n=pq$，选择 $e\in Z_n$，并求 d，使 $ed\equiv 1(\mathrm{mod}\phi(n))$，其中 $\phi(n)$是欧拉函数. 将 e 作为群中心的公钥，d 作为群中心的私钥.

群中心为每个群成员 U_i 秘密选择两个大素数 r_i、q_i，计算 $n_i=r_iq_i$，选择 $y_i\in Z_{n_i}$，并求 x_i，使 $x_iy_i\equiv 1(\mathrm{mod}\phi(n_i))$. 将 y_i 作为群成员 U_i 的公钥，x_i 作为群成员 U_i 的私钥.

选择素数 p_i 大于 y_i，将(x_i, p_i, p_i^d)秘密送给群成员. 群成员验证 $p_i\equiv(p_i^d)^e(\mathrm{mod}n)$是否成立，如果成立，相信$(x_i, p_i, p_i^d)$是群中心送来的，并将$(x_i, p_i, p_i^d)$作为签名密钥保存. 群中心将$(\mathrm{ID}_i, y_i)$送给群管理员，其中 ID_i 是用户 U_i 的身份.

不失一般性，设系统有 k 个成员，利用中国剩余定理，群中心可以求得同余方程组

$$c \equiv y_i(\mathrm{mod}p_i) \qquad i = 1,\cdots,k$$

$$\gcd(p_i, p_j) = 1 \quad i \neq j \tag{6}$$

的解为

$$c \equiv y_1P'_1P_1 + y_2P'_2P_2 + \cdots + y_kP'_kP_k(\mathrm{mod}P) \tag{7}$$

其中 $P=p_1p_2\cdots p_k$，$P_ip_i=P$，$P'_i\ P_i=1(\mathrm{mod}p_i)$.

将(n,e,c)作为群公钥发布，并将每位群成员的大合数 n_i 公布.

(2)成员加入. 群中心为新成员 Bob 秘密选择两个大素数 r_{k+1}、q_{k+1}，计算 $n_{k+1}=r_{k+1}q_{k+1}$，选择 $y_{k+1}\in Z_{n_{k+1}}$，并求 x_{k+1}，使 $x_{k+1}\ y_{k+1}\equiv 1(\mathrm{mod}\phi(n_{k+1}))$. 将 y_{k+1}作为 Bob 的公钥，x_{k+1}作为 Bob 的私钥. 选择素数 $p_{k+1}>y_{k+1}$，且 $\gcd(p_i, p_{k+1})=1, i=1,\cdots,k$，重新计算 c，并将$(x_{k+1}, p_{k+1}, p_{k+1}^d)$发送给 Bob，将$(\mathrm{ID}_{k+1}, y_{k+1})$送给群管理员.

(3)成员撤消. 与加入过程类似，为了撤消成员 U_i，群中心将 y_i 改为另外的一个随机数 y'_i，并重新计算

$$c \equiv y_1P'_1P_1 + \cdots + y'_iP'_iP_i + \cdots + y_kP'_kP_k(\mathrm{mod}P) \tag{8}$$

(4)群签名生成. 对任意消息 m，计算 $s_i\equiv h(m)^{x_i}(\mathrm{mod}n_i)$，则$(m, s_i, p_i^d)$就是成员 U_i 对消息 m 的签名.

(5)群签名验证. 若 Alice 要对签名(m, s_i, p_i^d)进行验证，首先由群中心的公钥 e 和用户 U_i 的 n_i，计算 $p_i\equiv(p_i^d)^e(\mathrm{mod}n)$，$y_i\equiv c(\mathrm{mod}p_i)$以及 $h(m)$，接着验证 $h(m)\equiv s_i^{y_i}(\mathrm{mod}n_i)$是否成立，成立则签名正确，否则签名不正确.

(6)群签名打开. 给出签名(m, s_i, p_i^d)后，群管理员计算 $p_i\equiv(p_i^d)^e(\mathrm{mod}n)$以及 $y_i\equiv c(\mathrm{mod}p_i)$，验证 $h(m)\equiv s_i^{y_i}(\mathrm{mod}n_i)$，通过与 y_i 和 n_i 相应的 ID_i 确定签名成员的身份.

(7)新方案与 Chen 方案关键区别之处. 与 Chen 方案相比，新方案在系统建立时，每个群成员的签名公钥和签名私钥在产生的过程中使用的模数是不相同的，从根本上解决了原方案的共模漏洞问题. 在之后的成员加入、成员撤消、群签名生成、群签名打开、群签名验证等环节中针对不同的群成员使用的计算模数 n_i 也是不相同的. 不同群成员使用的参数之间相互独立，互相没有关系，因此不存在信息互相利用问题.

4 安全性与计算复杂性分析

Chen 方案是基于 RSA 体制的安全性准则（即大数分解困难性）而构造的，在系统建立时对不同成员却采用了相同的模数，于是出现了如文中第 2 部分所分析的安全缺陷. 新方案中对不同群成员使用的计算模数 n_i 互不相同，使用的参数也相互独立，信息无法相互利用和借鉴，所以要伪造某个群成员

U_i 的签名，必须进行大整数 n_i 的因子分解. 然而，迄今为止，还没有一种有效的算法可以用来进行大整数因子分解，故新方案的安全原理是可靠的.

根据群签名安全性[8]要求，将新方案和 Chen 方案对比，新方案具有下列性质.

(1)新方案对 RSA 算法的使用是安全的. 与 Chen 方案相比，新方案避免了 RSA 共模带来的安全隐患问题，可以有效地抵御目前针对 RSA 算法的选择密文攻击、共模攻击、低指数攻击、加密及签名攻击等.

(2)新方案具有可撤消性. 从新方案构造过程中可以看到，新方案可以在不改变其他群成员密钥的情况下，加入新成员或撤消已有成员，惟一改变的只是群公钥要素中的 c，不需要改变其他成员的签名密钥.

(3)新方案具有不可伪造性. 在不同模条件下，任何一个非法群成员基于大数分解的困难性得不到群中心的私钥或等效私钥，因而无法伪造群中心.

(4)新方案具有防陷害性. 同样基于大数分解的困难性，任何成员都无法计算出其他成员的签名密钥或等效密钥，也就无法生成能通过签名验证的伪造签名.

(5)新方案可抵抗联合攻击. 由于采用了不同的模数，群成员之间的公、私钥不存在关联性，无法合谋产生合法群成员的私钥或等效私钥，因而也就不存在关联攻击的可能.

这里需要说明的是，改进后的新方案和原方案[6]一样也不满足不可关联性，但这并不是特别重要，因为在很多场合需要用到关联性，如公平的电子投票系统[9]. 另外，改进方案和原方案[6]一样，在签名、验证、打开等过程中计算复杂度与群成员的个数无关，计算量小. 在系统的建立、群成员的加入和撤消过程中只需要乘法运算而不需要指数运算，效率比较高，计算量与群成员的个数相关，这就要求群中心要有较高的计算能力.

5 结束语

本文对 Chen 群签名方案进行了详细的分析，证明该方案是不安全的，并在此基础上提出了一种新型群签名方案. 该新方案可以抵抗共模攻击，具有可撤消性、不可伪造性、防陷害性、抗联合攻击等特点，具有重要的实用价值，特别适合于在服务端计算能力强而对客户端资源要求不高的情形，如移动通信网等. 至于新方案可能存在的其他潜问题，有待于下一步研究.

参考文献：

[1] CHAUM D, VAN HEYST E. Group signatures[C]// Advances in Cryptography EUROCRYPT'91. Berlin: Spriger-Verlag, 1991: 257-265.

[2] 黄振杰，郝艳华，王育民. 授权群签名[J]. 电子学报，2004，32(5)：774-777.
HUANG Zhenjie, HAO Yanhua, WANG Yumin. Authorized group signature [J]. Acta Electronic Sinica, 2004, 32(5): 774-777.

[3] 钟军，何大可. ACJT 群盲签名方案[J]. 计算机工程，2007，33(1)：19-21.
ZHONG Jun, HE Dake. ACJT group blind signature scheme [J]. Computer Engineering, 2007, 33(1): 19-21.

[4] 马春波，敖军，何大可. 基于双线性映射的多重签名与群签名[J]. 计算机学报，2005，28(9)：1158-1163.
MA Chunbo, AO Jun, HE Dake. Multi-signature and group signature based on bilinear pairing [J]. Chinese Journal of Computers, 2005, 28(9): 1558-1563.

[5] 王晓明，陈火炎，符方伟. 动态门限群签名方案[J]. 计算机学报，2004，27(9)：1182-1186.
WANG Xiaoming, CHEN Huoyan, FU Fangwei. Dynamic threshold group signature scheme [J]. Chinese Journal of Computers, 2004, 27(9): 1182-1186.

[6] 陈泽文，张龙军，王育民. 一种基于中国剩余定理的群签名方案[J]. 电子学报，2004，32 (7)：1062-1065.
CHEN Zewen, ZHANG Longjun, WANG Yumin. A group signature scheme based on Chinese remainder theorem [J]. Acta Electronic Sinica, 2004, 32 (7): 1062-1065.

[7] 冯登国. 密码分析学[M]. 北京：科学出版社，2000.

[8] 陈少真，李大兴. 有效取消的向前安全群签名体制[J]. 计算机学报，2006，29(6)：998-1003.
CHEN Shaozhen, LI Daxing. An efficient revocable group signature schemes with forward security [J]. Chinese Journal of Computers, 2006, 29 (6): 998-1003.

[9] NAKANISHI T, FUJIWARA T, WATANABE H. A linkable group signature and its application to a fair secret voting [J]. Trans IPS JAPAN, 1999, 40(7): 3085-3096.

(编辑 杜秀杰)