一个基于中国剩余定理的群签名方案的攻击及其改进方案

王凤和[①②] 胡予濮[①] 王春晓[③]
[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 西安 710071)
[②](泰山学院数学系 泰安 271000)
[③](山东建筑工程学院数理系 济南 250014)

摘 要：该文给出了对一个已有的群签名方案的攻击，表明了已有的群签名不能防止群成员的联合攻击，在联合攻击下攻击者可以得到任何群成员的秘钥从而伪造任何人的签名。同时该方案也不能防止不诚实的管理员伪造群成员的签名。利用 Schnorr 签名方案给出了一种改进方案，新的改进方案具有以下特点：联合攻击下是安全的；可以防止不诚实的群中心伪造群成员的签名；可以简单高效地实现成员撤消。

关键词：联合攻击；撤销；群签名；最大共因子
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2007)01-0182-03

An Attack and Improve of a Group Signature Scheme Based on Chinese Remainder Theorem

Wang Feng-he[①②] Hu Yu-pu[①] Wang Chun-xiao[③]
[①](*Key Lab of Computer Networks and Information Security*, *Ministry of Education*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*Dept. of Mathematics*, *Taishan Collage.*, *Taian* 271000, *China*)
[③](*Dept. of Math and Phys. Shandong Institute of Architechture and Engineering*, *Jinan* 250014, *China*)

Abstract: An attack is mounted on a group signature scheme based on Chinese Remainder Theory(Chen-Scheme). It shows the Chen-Scheme is insecure: A colluding subset of group members can find the private key of other members and forge their signatures; The dishonest group center can produce a valid signature on behalf of group members. Using Schnorr signature scheme this paper proposes an improve scheme, which has good characteristics: A colluding subset of group members can not produce a valid signature that the group manager can not open; A dishonest group center can not sign messages on behalf of other members; The revocation of the membership is efficient .

Key words: Collaborate attack; Revocation; Group signature; Greatest common divisor

1 引言

群签名首先由 Chaum 和 Van Heyst 提出[1]，在一个群签名方案中允许任意群成员代表群体对消息匿名地进行签字。在必要时可由群管理员确定签名人的身份。防止联合攻击和成员撤销是群签名领域的两个重要问题[2]。近年来提出许多在联合攻击下安全的群签名方案[3,4]。然而在成员撤消问题上许多安全的群签名都没有很好地实现高效的成员撤消[2−4]。而现实应用中群组总是动态的。因此实现高效的成员撤消是群签名应用的一个关键问题。近年来人们对群签名中的成员撤消问题给予了广泛的关注。提出了许多实现群成员撤消的方法[5−8]。但是没有很好地提高撤消算法的效率。因此设计包含高效的成员撤消功能、可以有效地防止联合攻击的群签名方案仍然是群签名的热点。

2005-06-08 收到，2005-11-14 改回
国家自然科学基金(60473029)资助课题

2004 年陈泽文等提出了一个基于中国剩余定理的群签名方案[9]，该方案可以在不改变其他群成员的秘钥的情况下实现简单快速的成员的加入或撤销。本文对该方案的安全性进行了分析，指出该方案存在以下问题：(1)在联合攻击下可以伪造任何群成员的签名；(2)该方案不能防止陷害攻击，群管理员(群中心)可以假冒群成员生成合法签名。

基于以上攻击方法。我们利用成熟的 Schnorr 签名对原方案进行了改进，成功地抵御了这种联合攻击和陷害攻击。新的改进方案具有以下特点：

(1)能够有效地防止联合攻击，在安全性分析中，本文给出了防止联合攻击的安全性证明。

(2)群组可以实现简单高效地实现成员撤消，当有成员撤消时，群组不需要改变其他群成员的秘钥，仅需要做简单的乘法模运算。计算量小。

(3)群管理员(群中心)无法伪造其他群成员的签名。

2　基于中国剩余定理的群签名及其攻击

2.1　基于中国剩余定理的群签名方案

本节简要介绍基于中国剩余定理的群签名，细节请参看文献[9]。其中群中心负责为群管理员和群成员分配秘钥，群管理员则在必要的时候打开签名确定签名者的身份。

2.1.1 *秘钥生成*　群中心随机地生成两个大素数 p,q 并选择一个公开的 Hash 函数 $h(\cdot)$，计算 $n=pq$，选择 $e\in Z_n$，并求 d, 使得 $ed\equiv 1(\bmod \phi(n))$，其中的 $\phi(n)$ 是 Euler 函数。随机选择 $x_i,y_i\in Z_n$，使得 $x_iy_i\equiv 1(\bmod \phi(n))$，并选择素数 $p_i>y_i$，且 $i\neq j$ 时 $p_i\neq p_j$。将 (x_i,p_i,p_i^d) 秘密送给群成员 U_i 作为成员的签名秘钥，U_i 验证式子 $p_i\equiv (p_i{}^d)(\bmod n)$ 以确信消息是群中心送来的。群中心将 (ID_i,y_i) 送给群管理员，其中 ID_i 是群成员的身份。

设系统有 k 个成员，群中心利用中国剩余定理[10]，可求同余方程组：

$$c\equiv y_i(\bmod p_i),\quad i=1,2,\cdots,k \tag{1}$$

的解：

$$c\equiv\sum_{i=1}^{k}y_iP_iP_i'(\bmod P) \tag{2}$$

其中 $P=p_1p_2\cdots p_k$，$P_i=P/p_i$，$P_iP_i'\equiv 1(\bmod p_i)$。群中心将 (n,e,c) 作为公钥，(d,p,q) 为秘钥。

2.1.2 *成员的加入和撤销*　在有成员加入或撤销时，群中心只需利用式(1)改变 c 的值并公布出去，而不必改变其他群成员的秘钥。具体细节请参看文献[9]，本文不再详叙。

2.1.3 *签名*　群成员 U_i 要对消息 m 签名，U_i 首先计算 $h(m)$, 再计算 $s_i=(h(m))^{x_i}(\bmod n)$，则 (m,s_i,p_i^d) 即为 U_i 的签名。

2.1.4 *验证*　若 Alice 要对 U_i 的签名 (m,s_i,p_i^d) 进行验证，Alice 利用群公钥 e 计算：$p_i\equiv(p_i{}^d)^e(\bmod n), y_i\equiv c(\bmod p_i)$，得到 y_i，然后验证：$h(m)\equiv s_i^{y_i}(\bmod n)$ 是否成立。若成立，签名合法，否则不接受签名。

2.1.5 *打开*　群管理员通过计算 $p_i\equiv(p_i{}^d)^e(\bmod n),\quad y_i\equiv c(\bmod p_i)$ 得到 y_i，利用和 y_i 对应的 ID_i 确定签名者的身份。

2.2 签名的攻击

2.2.1 *群中心伪造群成员的签名*　显然该方案中群中心知道所有的群成员的签名秘钥，因此一个不诚实的群中心可以伪造其他群成员的合法签名而不被发现，因此原方案不能有效的防止陷害攻击。

2.2.2 *联合攻击*　几个群成员利用联合攻击很容易得到群中心的秘钥 $\phi(n)$。从而可以任意伪造其他成员的签名而不被发现。假设群成员 U_1,U_2 联合对方案攻击。此时 U_1,U_2 分别掌握着 $x_1y_1\equiv 1(\phi(n)), x_2y_2\equiv 1(\bmod \phi(n))$，可知 $\phi(n)$ 是 x_1y_1-1, x_2y_2-1 的公因子。不妨设：$x_1y_1-1=A\phi(n)$, $x_2y_2-1=B\phi(n)$,当 $\gcd(A,B)=1$ 时，则 U_1,U_2 可能利用辗转相除法通过计算 x_1y_1-1, x_2y_2-1 的最大公因子得到 $\phi(n)$。如果 U_1,U_2 联合更多的群成员，则他们得到 $\phi(n)$ 的概率会更大。事实上假定有 t 个群成员联合攻击时，则有

$$\begin{cases}x_1y_1-1=A_1\phi(n)\\ x_2y_2-1=A_2\phi(n)\\ \quad\vdots\\ x_ty_t-1=A_t\phi(n)\end{cases}$$

只要 $(A_1,A_2,\cdots,A_t)=1$，则 $(x_1y_1-1,x_2y_2-1,\cdots,x_ty_t-1)=\phi(n)$ 成立。而当 $A_1,\cdots,A_T$ 中既有奇数又有偶数时肯定互素。于是 $(A_1,A_2,\cdots,A_t)=1$ 的概率：

$$P>1-2^{-t}-2^{-t}$$

显然联合成员越多，得到 $\phi(n)$ 的概率越大。攻击者得到群私钥 $\phi(n)$ 后利用 $x_iy_i\equiv 1(\bmod \phi(n))$，可以得到任何一个群成员的秘钥，因此可以伪造任何成员的签名而不被发现。

事实上不只群成员可以利用这种方法攻击群签名。即使攻击者 Eve 不是群成员也可通过多次加入群体，得到多对 $x_iy_i\equiv 1(\bmod \phi(n))$ 实现对签名的攻击；若 Eve 曾是群成员原有的 (x_i,y_i) 对攻击依然有用。

3　改进的群签名方案及其安全性分析

3.1 改进的群签名方案

原群签名中群中心利用自己的秘钥 $\phi(n)$ 多次为群成员分配密钥，过多的泄漏了私钥信息，以致群成员可以利用联合攻击得到群秘钥，我们的改进方案利用 Schnorr 签名方案，将群签名方案的安全性基于解离散对数的困难性，成功地保护了群中心的秘密信息不泄漏。系统组成：群中心，群成员，群管理员。

3.1.1 *系统生成*　群中心首先秘密地生成两个大素数 p,q。其中 q 整除 p–1, q>160bit, p>512bit。以保证解离散对数的困难性并选择一个公开的 Hash 函数 h(.)。$N=pq$。g 是 Z_p^* 的元，$g^q=1(\bmod p)$，选择 $u,v\in Z_n, uv\equiv 1(\bmod \phi(n))$。假设 Alice 要求加入群体，在向群中心出示身份后群中心选择大素数 $p_i\in Z_p^*$，且 $i\neq j$ 时，$p_i\neq p_j$。将 $p_i\in Z_p^*$ 送给 Alice，Alice 随机地选择 $x_{k+1},y_{k+1}, y_{k+1}\equiv g^{x_{k+1i}}(\bmod p_{k+1})$，并将 y_i 送给群中心。群中心得到 y_i 后利用中国剩余定理解同余式组：

$$c\equiv y_i(\bmod p_i),\quad i=1,2,\cdots,k+1$$

其中 k 是原来群成员的个数，得解：

$$c\equiv\sum_{i=1}^{k+1}y_iP_iP_i'(\bmod P)$$

其中 $P=p_1p_2\cdots p_{k+1}$，$P_i=P/p_i$，$P_iP_i'\equiv 1(\bmod p_i)$。于是群中心的公开参数(n, u, g, c),秘密参数(p, q, v,)。群中心把 (ID_i,y_i) 送给群管理员。

3.1.2 *成员加入和撤销*　同原方案一样当有新成员加入时，群中心只需随机地选择一个新的素数 $p_{k+1}\in Z_p^*$，且 $p_{k+1}\neq p_i, i=1,2,\cdots,k$。运行上面的协议，并把 $(\mathrm{ID}_{k+1},y_{k+1})$ 送给群管理员。并利用式(2)重新计算 c 的值，并代替原来的值。其他成员的秘钥信息不变。当有成员撤销时群中心只需

在式(2)中把对应的 y_i 改为一个新的随机数并重新计算 c，发布新的 c。不改变其他值。与文献[9]一样这种成员加入和撤销的过程也是简单高效的。

3.1.3 签名　设群成员 U_i 要对消息 m 签名。U_i 随机地产生随机数 k，于是 (s,e,p_i) 作为签名，其中 $r \equiv g^k (\mathrm{mod}\, p_i)$，$e = h(r \,||\, m)$，$s \equiv k - x_i e (\mathrm{mod}\, p_i)$。

3.1.4 验证　Alice 要验证 U_i 的签名，它可以如下操作：

$$c \equiv y_i (\mathrm{mod}\, p_i),$$

$$r' \equiv g^s y_i^{\,e} \equiv g^{k - x_i e} g^{e x_i} (\mathrm{mod}\, p_i) \equiv g^k (\mathrm{mod}\, p_i)$$

于是 Alice 验证是否有 $e = h(r' \,||\, m)$。如果是说明签名合法，否则不接受签名。

3.1.5 打开　如果发生争议群管理员可以通过 $c \equiv y_i (\mathrm{mod}\, p_i)$，得到 y_i，利用和 y_i 对应的 ID_i 确定签名者的身份。

3.2 安全性分析

3.2.1 防陷害攻击　任何群成员要或者群管理员要以他人的名义生成合法签名就必须知道对方的秘钥 x_i，因此他必须解离散对数的困难问题。

3.2.2 防群成员的联合攻击

定理　改进方案可以有效地防止群成员的上述联合攻击。

证明　假设攻击者 eve 可以利用算法 φ 通过 k 组密钥对 $(x_i, y_i, p_i)(i = 1,2,\cdots,k)$ 和 $c \equiv \sum_{i=1}^{k+1} y_i P_i P_i' (\mathrm{mod}\, P)$ 得到另一组秘钥对 $(x_{k+1}, y_{k+1}, p_{k+1})$。则我们证明 eve 可以利用算法 φ 来解决离散对数问题。即已知 $p_{k+1}, y_{k+1}, y_{k+1} \equiv g^{x_{k+1 i}} (\mathrm{mod}\, p_{k+1})$ 求 x_{k+1}？则 eve 可以如下操作：

(1)选择大素数 $p_i \in Z_p^*$，且 $i \neq j$ 时，$p_i \neq p_j \neq p_{k+1}$ $(i = 1,2,\cdots,k)$

(2)随机选择 $x_i, y_i, y_i \equiv g^{x_i} (\mathrm{mod}\, p_i)$ $(i = 1,2,\cdots,k)$

(3)利用中国剩余定理计算：

$$c \equiv \sum_{i=1}^{k+1} y_i P_i P_i' (\mathrm{mod}\, P)，（其中：$$

$P = p_1 p_2 \cdots p_k p_{k+1}$, $P_i = P / p_i, P_i P_i' \equiv 1 (\mathrm{mod}\, p_i)$)

(4)将 $y_i, p_i, c.(i = 1,2,\cdots,k+1)$和$x_j (j = 1,2,\cdots,k)$ 作为算法 φ 的输入于是得到一组新的秘钥对 $(x_{k+1}, y_{k+1}, p_{k+1})$。从而 eve 成功地解决了离散对数问题。所以定理得证。

注：本方案的一个缺点和不足是该方案同原方案[9]一样也不满足非关联性[9]。文献[11]说明有的场合要用到关联性。如何对方案进行改进使它具有非关联性有待继续研究。

4 结束语

本文对一个基于中国剩余定理的群签名方案的安全性进行分析，说明这种群签名方案易遭受群成员的联合攻击、不能防止陷害攻击。并给出了一种改进方案可以抵御这种联合攻击，防止陷害攻击。而在实现群成员加入和撤销时改进方案和原方案同样简单快捷。

参 考 文 献

[1] Chaum D and Van Heyst E. Group signatures[A]. Proc of EUROCRYPT'91[C]. Lecture Notes in Computer Science, Berlin: Springer-verlag , 1991: 257–265.

[2] Ateniese G and Tsudik G. Some open issues and new directions in group signature[A]. Financial Cryptography 1999, Berlin: Springer-Verlag, 1999: 196–211.

[3] Camenish J and Stadler M. Efficient group signatures for large groups[A]. Proc.of CRYPTO'97[C]. Lecture Notes in Computer Science, Berlin: Springer-verlag, 1997, 1296: 410–424.

[4] Ateniese G, Camenish J, Joye M, and Tsudik G. A Practical and provably secure coalition-resistant group signature scheme[A]. Crypt'2000[C], Berlin: Springer-Verlag, 2000, 1880: 255–270.

[5] Kim Hyun Jeong, Lim Jong In, and Lee Dong Hoon. Efficient and secure member deletion in group signature schemes[A]. Proc of the 3rd Int. Conf. on Information Security and Cryptology-ICISC 2000[C]. Lecture Notes in Computer Science, Berlin: Springer-verlag, 2000, 2015: 150–161.

[6] Camenish J and Michels M. A group signature scheme with improved efficiency[A]. Proc.of ASICACRYPT'98[C]. Lecture Notes in Computer Science, Berlin: Springer-verlag , 1998, 1541: 160–174.

[7] Ateniese G and Tsudik G. Quasi-efficient revocation of group signature. 2001. http://eprint.iacr.org/2001/101/.

[8] Bresson E and Stern J. Efficient revocation in group signature . In: Proc.of PKC'01. Berlin: Springer-verlag, 2001: 190–206.

[9] 陈泽文, 张龙军, 王育民, 黄继武, 黄达人. 一种基于中国剩余定理的群签名方案. 电子学报, 2004, 32(7): 1062–1065.
Chen Ze-wen, Zhang Long-jun, Wang Yu-min, Huang Ji-wu, and Huang Da-ren. A group signature scheme based on Chinese remainder theorem. *Acta Electronica Sinica*, 2004, 32(7): 1062–1065.

[10] 柯召, 孙琦. 数论讲义(上册)[M]. 北京: 高等教育出版社, 2000: 42–43.

[11] Nakanishi T, Fujiwara T, and Watanabe H. A linkable group signature and its application to a fair secret voting[A].Proc. of 4th International Symposium on Communication theory and Applications[C]. 1997: 159–164.

王凤和：　男，1979 年生，讲师, 研究方向为群签名及其应用.

胡予濮：　男，1955 年生，教授，博士生导师, 研究方向为信息安全和网络安全.

王春晓：　女，1979 年生，讲师, 研究方向为应用数学.