第 35 卷 第 3 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.3 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)03—0166—03 文献标识码：A 中图分类号：TP309

一个群签名方案的密码学分析与改进

王永峰，张建中
(陕西师范大学数学与信息科学学院，西安 710062)

摘 要：通过对一个基于中国剩余定理的群签名方案进行密码学分析，发现其安全缺陷。针对该缺陷提出一种改进的群签名方案，在不改变群成员密钥的前提下，有效实现群成员的加入与撤销。分析结果表明，该方案安全可靠，具有较高实用性。
关键词：群签名；中国剩余定理；群成员撤销；伪造攻击

Cryptanalysis and Improvement of Group Signature Scheme

WANG Yong-feng, ZHANG Jian-zhong
(College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062)

【Abstract】Cryptanalysis of a group signature scheme based on Chinese remainder theorem shows that it exists security flaws. Aiming at these flaws, this paper puts forward an improved group signature scheme. It realizes effective participation and revocation of group members under the condition that keep the group member secret key unaltered. Analysis results show that this scheme is secure and practicable.
【Key words】group signature; Chinese remainder theorem; revocation of group member; forgery attack

群签名概念由文献[1]提出，其后，随着实际应用的深入，文献[2]提出具有群成员撤销功能的群签名。基于 ACJT 群签名方案，文献[3]提出“2 个成员删除”方案，该方案的签名长度与被撤销成员个数成线性关系。如何安全有效地废除群成员是群签名研究的重要方向之一[4]。近年来，众多学者开始研究动态群签名，文献[5]提出一个基于中国剩余定理的群签名方案，该方案在实现群成员加入或撤销时，能在更新群公钥的情况下，不更新其他群成员的密钥。文献[6]对文献[5]方案进行了安全性分析和改进。本文在文献[7-8]的基础上对文献[6]方案进行密码学分析，发现它存在如下安全缺陷：(1)群中心伪造签名；(2)在群管理员和群成员合谋的情况下，可以陷害已签过名的任意群成员；(3)在群管理员和被撤销成员合谋的情况下，被撤销成员可以继续生成有效的群签名。

1 基于中国剩余定理的群签名方案[6]

文献[6]方案包括 3 个参与实体：群中心，群管理员，群成员。群中心用于建立整个系统并为每个群成员和群管理员分配密钥。必要时，群管理员可以打开一个合法签名，以确定签名者身份。

1.1 系统初始化

群中心秘密选择 2 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 $ed\equiv 1\bmod\phi(n)$，其中，$\phi(\cdot)$ 是欧拉函数；e,d 分别作为群中心的公钥和私钥。随机选择 x_i,y_i 使 $x_iy_i\equiv 1\bmod\phi(n)$，选择素数 p_i 大于 y_i，并使得当 $i\neq j$ 时，$\gcd(p_i,p_j)=1$。将 $(x_i,p_i,p_i^d \bmod n)$ 秘密送给群成员 U_i，并将 (ID_i,y_i) 传送给群管理员。群成员 U_i 验证 $p_i\equiv(p_i^d \bmod n)^e(\bmod n)$ 是否成立，若成立，则相信 $(x_i,p_i,p_i^d \bmod n)$ 是群中心送来的，并将其作为签名密钥保存。

设系统现有 k 个群成员，群中心利用中国剩余定理计算同余式组 $c\equiv y_i(\bmod p_i),i=1,2,\cdots,k$ 的解 $c\equiv y_1P_1P_1'+y_2P_2P_2'+\cdots+y_kP_kP_k'(\bmod P)$，其中，$P=p_1p_2\cdots p_k$；$P_i=P/p_i$；$P_iP_i'\equiv 1(\bmod p_i)$。群公钥为 (n,e)。

1.2 成员加入

假设 Bob 想成为群成员，它向群中心提出申请并提供身份证明，群中心随机选择 $x_{k+1}\in Z_n$，由 $x_{k+1}y_{k+1}\equiv 1(\bmod\phi(n))$ 求出 y_{k+1}，选择大于 y_{k+1} 的素数 p_{k+1}，使 $\gcd(p_{k+1},p_i)=1,i=1,2,\cdots,k$，重新计算新的 c，即

$$c\equiv y_1P_1P_1'+y_2P_2P_2'+\cdots+y_kP_kP_k'+y_{k+1}P_{k+1}P_{k+1}'(\bmod P)$$

其中，新的 P,P_i,P_i' 可以通过给出的 P,P_i,P_i' 求出，即

$$P=Pp_{k+1}$$
$$P_i=P_ip_{k+1}$$
$$P_i'=P_i'p_{k+1}(\bmod p_i),i=1,2,\cdots,k$$

其中，$p_{k+1}p_{k+1}'\equiv 1(\bmod p_i)$。

群中心将 $(x_{k+1},p_{k+1},p_{k+1}^d \bmod n)$ 发送给 Bob，将 (ID_{k+1},y_{k+1}) 发送给群管理员。

1.3 成员撤销

设系统现有 k 个群成员，现在要撤销群成员 U_j，群中心将 y_j 改为 y_j'，使 $x_jy_j'\neq 1(\bmod\phi(n))$，重新计算新的 c，即

$$c\equiv y_1P_1'P_1+y_2P_2'P_2+\cdots+y_j'P_j'P_j+\cdots+y_kP_k'P_k(\bmod P)$$

并保存新的 c。

基金项目：国家自然科学基金资助项目(10571113)；陕西省自然科学基金资助项目(2004A14)；陕西省教育厅科学研究计划自然科学基金资助项目(07JK375)
作者简介：王永峰(1979－)，男，硕士研究生，主研方向：密码学与信息安全；张建中，教授、博士
收稿日期：2008-10-23 **E-mail：**jzzhang@snnu.edu.cn

1.4 签名的生成

群成员 U_i 要对消息 m 生成签名，计算 $s_i = h(m)^{x_i} (\mathrm{mod}\, n)$，则 $(m, s_i, p_i^d \bmod n)$ 就是 U_i 对消息 m 的签名。将签名送给群中心，群中心对签名 $(m, s_i, p_i^d \bmod n)$ 进行验证，计算 $p_i = (p_i^d \bmod n)^e (\mathrm{mod}\, n)$ 和 $y_i = c(\mathrm{mod}\, p_i)$，验证 $s_i^{y_i} (\mathrm{mod}\, n) = h(m)$ 是否成立，若成立，则群中心对消息 m 进行签名，即 $s = h(m)^d (\mathrm{mod}\, n)$，$(m, s_i, s)$ 即成员 U_i 的最终签名。

1.5 签名的验证

验证者验证 $s^e (\mathrm{mod}\, n) = h(m)$ 是否成立，若成立，则签名正确，否则签名不正确。

1.6 签名的打开

群管理员计算 $p_i = (p_i^d \bmod n)^e (\mathrm{mod}\, n)$ 和 $y_i = c(\mathrm{mod}\, p_i)$，通过 (ID_i, y_i) 识别签名者的身份。

2 密码学分析

改进方案与原方案的共同点是使用 RSA 签名，利用中国剩余定理实现群成员的加入与撤销。它们的不同点在于，改进方案的签名生成阶段由群成员和群中心共同完成，y_i 不再作为公钥。每个群成员都拥有自己的私钥 x_i，并可以计算相应的 y_i，即所有群成员均掌握自己的密钥对 (x_i, y_i)，在 RSA 签名中，暴露私钥 d 与分解 n 是等价的。

2.1 群中心的伪造签名

2.1.1 群中心对签名的伪造

对任意消息 m，群中心取随机数 s_i，并计算 $s = (h(m))^d (\mathrm{mod}\, n)$，签名 (m, s_i, s) 可以通过验证，且群管理员不可以追踪签名者身份的有效签名，具体验证过程如下：

$$s^e = (h(m)^d)^e \bmod n = h(m)^{de} \bmod n = h(m)$$

2.1.2 群中心对群成员 U_r 的陷害

对任意消息 m，群中心计算 $s_r = (h(m))^{x_r} \bmod n$，$s = h(m)^d \bmod n$，签名 $(m, s_r, p_r^d \bmod n)$ 被发送给群管理员，签名 (m, s_r, s) 可以通过验证，且群管理员可以识别签名者的身份是 U_r，从而对群成员 U_r 构成陷害。具体验证过程如下：

$$s^e = (h(m)^d)^e \bmod n = h(m)^{de} \bmod n = h(m)$$

身份揭示过程如下：群管理员计算 $p_r = (p_r^d)^e \bmod n$，$y_r = c(\mathrm{mod}\, p_r)$，利用 $y_r, (ID_r, y_r)$ 识别签名者的具体身份是群成员 U_r，从而对群成员 U_r 构成陷害。

2.2 群管理员和群成员对其他签过名的群成员的合谋陷害

由方案的签名打开阶段可知，群管理员掌握所有参与签名的群成员公钥 y_i，若其中一位签过名的群成员 U_t 与群管理员合谋，则根据 x_t, y_t 可以求出模数 n 的分解式。利用群管理员所掌握签名成员的公钥 y_i，根据扩展欧几里得算法可以计算群成员 U_i 的私钥 x_i 和群中心私钥 d。利用 x_i，d 和群管理员掌握的群成员 U_i 的签名 $(m, s_i, p_i^d \bmod n)$ 可以陷害群成员 U_i。

2.3 群成员撤销后的群签名生成

假设群成员 U_k 被撤销，U_k 现在掌握 $(x_k, p_k, p_k{}^d \bmod n)$，由签名的打开阶段可知，群管理员掌握新的 c'，若两者合谋，则由 2.2 节可知，U_k 可以计算模数 n 的分解式，从而继续生成有效群签名。伪造过程如下：先计算 $y_k' = c' \bmod p_k$，然后计算分别满足 $x_k' y_k' = 1 \bmod \phi(n)$ 和 $ed = 1 \bmod \phi(n)$ 的 x_k' 和 d，最后计算 $s_k = h(m)^{x_k'} (\mathrm{mod}\, n), s = (h(m))^d (\mathrm{mod}\, n)$，则 (m, s_k, s) 是被撤销成员 U_k 在被撤销后生成的有效群签名。验证过程如下：

$$s^e = (h(m)^d)^e \bmod n = h(m)^{de} \bmod n = h(m)$$

3 改进方案

3.1 系统生成

群中心选择 2 个大素数 p, q，其中，q 是 $p-1$ 的一个素因子，g 是 Z_p^* 的一个元素，$g^q = 1 \bmod p$。选择一个公开的 Hash 函数 $h(\cdot)$，用户 U_i 向群中心提出申请并提供身份证明，群中心选择大素数 $p_i \in Z_p^*$，当 $i \neq j$ 时，$\gcd(p_i, p_j) = 1$ 且 $\gcd(p_i, g) = 1$。把 p_i 传送给 U_i，U_i 随机选择 x_i，计算 $y_i = g^{x_i} (\mathrm{mod}\, p_i)$，并把 y_i 发送给群中心。

群中心计算同余式组 $c \equiv y_i (\mathrm{mod}\, p_i), i = 1, 2, \cdots, k$，可得

$$c \equiv y_1 P_1 P_1' + y_2 P_2 P_2' + \cdots + y_k P_k P_k' (\mathrm{mod}\, P)$$

其中，$P = p_1 p_2 \cdots p_k$；$P_i = P / p_i$；$P_i P_i' \equiv 1 (\mathrm{mod}\, p_i)$。

群中心将 (ID_i, y_i) 传送给群管理员，群公钥为 (g, c)。

3.2 成员加入

设群中现有 k 个群成员，U_{k+1} 申请加入群，群中心选择大素数 p_{k+1}，且 $\gcd(p_{k+1}, p_i) = 1 (i \neq k+1)$。把 p_{k+1} 秘密传送给 U_{k+1}，U_{k+1} 随机选择 x_{k+1}，$y_{k+1} = g^{x_{k+1}} (\mathrm{mod}\, p_{k+1})$。把 y_{k+1} 传送给群中心，群中心重新计算新的 c，即

$$c \equiv y_1 P_1 P_1' + y_2 P_2 P_2' + \cdots + y_k P_k P_k' + y_{k+1} P_{k+1} P_{k+1}' (\mathrm{mod}\, P)$$

其中，新的 P, P_i, P_i' 可以通过给出的 P, P_i, P_i' 求出，即

$$P = P p_{k+1}$$

$$P_i = P_i p_{k+1}$$

$$P_i' = P_i' p_{k+1} (\mathrm{mod}\, p_i), i = 1, 2, \cdots, k$$

其中，$p_{k+1} p_{k+1}' \equiv 1 (\mathrm{mod}\, p_i)$。

群中心把 (ID_{k+1}, y_{k+1}) 传送给群管理员。

3.3 成员撤销

设现有 k 个群成员，现在要撤销群成员 U_j，群中心选择 y_j'，且 $y_j' \neq y_j \bmod p_j, j_j' \neq y_i \bmod p_i$。

重新计算 $c' \equiv y_1 P_1 P_1' + y_2 P_2 P_2' + \cdots + y_j' P_j P_j' + \cdots + y_k P_k P_k' (\mathrm{mod}\, P)$，其中，$P = p_1 p_2 \cdots p_j' \cdots p_k$；$y_i$ 为其他群成员的公钥。公布新生成的 c'。

3.4 签名的生成

设群成员 U_i 要对消息 m 生成签名，U_i 取随机数 k，计算 $r = g^k (\mathrm{mod}\, p_i), e = h(r \| m), s = k - x_i e (\mathrm{mod}\, p_i - 1)$，则生成的群签名为 (m, s, e, p_i)。

3.5 签名的验证

验证者对签名 (m, s, e, p_i) 进行验证，计算 $y_i \equiv c (\mathrm{mod}\, p_i)$，验证等式 $e = h(g^s y_i^e \| m)$ 是否成立，若成立则签名有效。

3.6 签名的打开

群管理员计算 $y_i \equiv c (\mathrm{mod}\, p_i)$，利用 (ID_i, y_i) 识别签名者的身份。

4 安全性分析

4.1 可验证性

方案的可验证性说明如下：

$$g^s y_i^e = g^s (g^{x_i})^e = g^s g^{x_i e} = g^{s + x_i e} = g^k (\mathrm{mod}\, p_i)$$

$$h(g^s y_i^e \| m) = h(g^k \| m) = h(r \| m) = e$$

4.2 匿名性

在本方案中，只有群管理员和群中心拥有 (ID_i, y_i)，对于不拥有 (ID_i, y_i) 知识的群成员，不能根据有效群签名和计算的 y_i 识别签名者的身份。

4.3 可撤销性

由撤销算法可知，若群成员 U_j 被撤销，当群管理员公布新的 c' 后，U_j 就不能继续生成有效的群签名，因为此时群公钥已经由原来的 (g,c) 变为 (g,c')。

若群成员 U_j 继续利用原来的私钥 x_j 生成群签名 (m,s,e,p_j)，则由 $y_j' = c'(\bmod p_j) \ne y_j$ 可得

$$g^s (y_j')^e = g^{k-x_j e}(y_j')^e = g^k (y_j)^{-e}(y_j')^e \ne g^k (\bmod p_j)$$

$$h(g^s (y_j')^e \| m) \ne h(g^k \| m) = h(r \| m) = e$$

若群成员 U_j 利用 c' 和 p_j 计算 y_j'，得 $y_j' = c'(\bmod p_j)$，再利用 y_j'，p_j 和等式 $y_j' = g^{x_j'} (\bmod p_j)$ 计算 x_j'，就会面临解离散对数的难问题，因此，群成员 U_j 不能再生成有效群签名。

4.4 不可伪造性

因为新方案采用 Schnorr 签名，所以不可伪造。即使方案不满足不相关联性，由于签名选择的是随机数，而二次签名取随机数的概率可以忽略不计，因此不会暴露签名者的私钥。

5 结束语

本文方案可以有效避免文献[6]方案存在的缺陷，但不具有不相关性，此问题有待进一步研究并解决。

参考文献

[1] Chaum D, Heyst F. Group Signature[C]//Proceedings of the EUROCRYPT'91. [S. l.]: Springer-Verlag, 1992: 257- 265.

[2] Bresson E, Stern J. Efficient Revocation in Group Signatures[C]// Proceedings of the Conference on Public Key Cryptography. [S. l.]: Springer-Verlag, 2001: 190-206.

[3] Ateniese G, Song D, Tsudik G. Quasi-efficient Revocation in Group Signatures[C]//Proc. of the Conference on Financial Cryptography. Berlin, Germany: Springer-Verlag, 2002: 183-197.

[4] 张福泰，张方国，王育民. 群签名及其应用[J]. 通信学报，2001, 22(1): 77-85.

[5] 陈泽文，张尤军，王育民，等. 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.

[6] 胡　斌，施荣华，娄　悦. 一种改进的基于中国剩余定理的群签名方案[J]. 计算机工程与应用, 2006, 42(24): 115-116.

[7] 李　俊，崔国华，刘志远. 一个群签名的密码学分析与改进[J]. 电子学报, 2007, 35(4): 778-781.

[8] 王凤和，胡予濮，王春晓. 一个基于中国剩余定理的群签名方案的攻击及改进方案[J]. 电子与信息学报, 2007, 29(1): 182-184.

~~~~~~

（上接第 165 页）

虽然 n 的取值可取 1~30 的任意整数，但由于当前数据的平均跳数是 15 跳，因此实验中 n 可取 2，能完整记录 15 跳的信息。考虑到存在不具有 StackPi 标记功能的传统路由器的存在，在本实验中 n 取 3，能记录 10 跳的信息。

分析 Kit #0304，该数据共有 192 244 个节点，609 066 个无向的连接，平均度数为 6.37，而最大度为 1 071。由图 1 可知，度数大于 100 的节点的个数约 400 个，而度数小于 10 的节点大于 150 000 个，因此，该数据服从幂律分布。可以只在数百个度数大于 100 的集散节点处设置 IP 源地址假冒过滤，即仅在 $\frac{400}{192\,244} = 0.002$ 的节点配置就可抑制 80%的 IP 源地址假冒。

5 结束语

本文提出的基于无尺度的 StackPi 过滤是一种基于 Internet 的无尺度特性的在途中过滤方法。但基于无尺度的 StackPi 过滤与原有的 StackPi 在目的端过滤一样，都存在着虚警和漏警。当路由发生变化时，会有大量虚警产生，当攻击者的源 IP 地址与所假冒的 IP 地址经过相同的路径时(如在同一子网)，则会产生漏警，这是下一步研究的方向。

参考文献

[1] Ferguson P. Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing[S]. RFC 2267, 1998.

[2] Bremler-Barr A, Levy H. Spoofing Prevention Method[C]//Proc. of IEEE INFOCOM'05. [S. l.]: IEEE Press, 2005-04.

[3] Park K, Lee H. On the Effectiveness of Route-based Packet Filtering for Distributed Dos Attack Prevention in Power-law Internets[C]// Proc. of ACM SIGCOMM'01. San Diego, CA, USA: [s. n.], 2001.

[4] Li Jun, Mirkovic J, Wang Mengqiu, et al. SAVE: Source Address Validity Enforcement Protocol[C]//Proc. of IEEE INFOCOM'01. Anchorage, Alaska, USA: [s. n.], 2001.

[5] Jin Cheng, Wang Haining, Shin K G. Hop-count Filtering: An Effective Defense Against Spoofed DDos Traffic[C]//Proc. of ACM Conf. on Computer and Communications Security. Washington D. C., USA: [s. n.], 2003.

[6] Yaar A, Perrig A, Song D. Pi: A Path Identification Mechanism to Defend Against DDos Attacks[C]//Proc. of IEEE Symposium on Security and Privacy. Berkeley, California, USA: [s. n.], 2003.

[7] Yaar A, Perrig A, Song D. StackPi: New Packet Marking and Filtering Mechanism for DDoS and IP Spoofing Defense[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(10): 1853-1863.

[8] Pastor-Satorras R, Vespignani A. Epidemic Spreading in Scalefree Networks[J]. Phys. Rev. Lett., 2001, 86(14): 3200-3203.

[9] 闫　巧，夏树涛，吴建平. 改进的压缩边分段采样算法[J]. 西安电子科技大学学报：自然科学版, 2006, 33(5): 824-828.

[10] CAIDA[Z]. (2005-06-05). http://www.caida.org/home.
~~~~~~