两个群签名方案的安全性分析

汪精明,王平水
(安徽财经大学 网络中心,安徽 蚌埠 233041)

摘 要:群签名在电子现金、电子选举等领域有着广泛应用,因此基于不同的数学问题设计安全高效的群签名方案有着重要意义。对最近提出的一个基于中国剩余定理的群签名方案和一个基于RSA签名的群签名方案进行研究,发现这两个方案存在安全漏洞:第一个方案中,任何一个群成员均可以分解系统模数,从而可以计算出系统中所有人的私钥;第二个方案的群签名打开算法不正确,从而无法追踪到群签名的生成者。分析表明,这两个方案均是不安全的,需要进一步完善。

关键词:群签名;中国剩余定理;可追踪性
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2007)09-0149-04

Security Analysis of Two Group Signature Schemes

WANG Jing-ming, WANG Ping-shui
(Network Center, Anhui University of Finance and Economics, Bengbu 233041, China)

Abstract: Group signature schemes have many applications, such as electronic cash and electronic vote. Thus, it is significant to devise efficient and secure group signature schemes based on all kinds of mathematic problems. In this paper, a group signature scheme based on Chinese remainder theorem and a group signature scheme based on RSA signature scheme are studied. Two security flaws in these schemes are found: in the former, the modulus of the system can be decomposed by every member of the group, so the private keys of everyone in the group can be computed; in the latter, the opening algorithm of the group signature scheme is incorrect, so the signer of the group signature can not be traced correctly. The analysis shows that the two schemes are not secure and need to be implemented.

Key words: group signature; Chinese remainder theorem; traceability

0 引 言

群签名是D. Chaum和E. van Heyst于1991年提出的[1]。一个群签名方案就是允许一个群体中的任意一个成员代表群体进行签名,签名的正确性可以用群公钥来进行验证。

●一个群签名方案要满足以下一些安全特性:

·正确性: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。

·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。

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

·不可关联性:确定两个不同的群签名是否来自于同一个群成员在计算上困难的。

·可追踪性:群管理员在必要的时候可以揭开一个正确的群签名的签名者真实身份。

·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。

●一个群签名通常由下列算法组成:

·系统建立:群管理员或群中心选择秘密钥,公布系统参数。

·成员加入:一个新用户通过和群管理员或群中心的交互协议请求加入,这个协议向新成员提供秘密钥和一个成员资格,并注册其身份。

·签名:用群成员的私钥和成员资格证书对消息 m 进行签名。

·验证:利用验证算法验证消息 m 的签名是否是一个合格的群成员的签名。

·打开:群管理员输入消息、消息的签名和自己的私钥,运行打开算法来揭示签名者的真实身份。

群签名方案的设计可以分为两大类:一类是基于知识签名设计的,一类是特别设计的。文献[2~4]中的方案属于第一类,文献[5~7]中的方案属于第二类。一些第一类方案在随机预言模型下可证明其是安全

收稿日期:2006-11-30
基金项目:安徽省教育厅自然科学基金资助项目(2006KJ017C)
作者简介:汪精明(1957-),男,江苏江阴人,实验师,研究方向为计算机网络与信息安全。

的;而第二类方案的效率很高,但其安全性一般只进行了启发式分析而没有在安全模型下进行正式证明,事实上很多第二类方案后来都被发现存在着安全性缺陷。由于群签名有着广泛的应用,对其效率有着较高的要求,所以很多学者仍在致力于采用直接设计的方法构造高效安全的群签名方案。

最近,国内学者分别基于中国剩余定理和 RSA 签名构造了两个群签名方案[8,9],这两个群签名方案具有高效的优点,其中文献[8]的方案还可以高效地撤销群成员的功能。但是分析后发现,这两个群签名方案在安全性方面还存在着问题:文献[8]的方案中任何一个群成员均可以分解系统模数 n,从而可以计算出系统中所有人的私钥,包括群中心的私钥,因此系统的安全性得不到保障;文献[9]的方案打开算法不正确,任何一个群成员均有可能被误认为是某个群签名的签名者。

1 文献[8]的群签名方案

该方案中存在三个实体:群中心、群管理人、群成员。群中心负责建立整个系统参数,包括为群成员和群管理人分配密钥;群管理人可以在必要的时候打开一个合法的群签名,确定签名者的身份;群成员可以代表群体进行签名,生成合法的群签名。

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 $ed \equiv 1 \pmod{\varphi(n)}$。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 $x_i \cdot y_i \equiv 1 \pmod{\varphi(n)}$,选择素数 p_i 大于 y_i,满足当 $i \neq j$ 时,$\gcd(p_i, p_j) = 1$,将 $(x_i, p_i, {p_i}^d)$ 秘密送给群成员 U_i。U_i 验证式子 $p_i = ({p_i}^d)^e \pmod n$ 是否成立。如果成立,则将 $(x_i, p_i, {p_i}^d)$ 作为签名密钥保存。群中心将 (ID_i, y_i) 送给群管理人,其中 ID_i 是用户 U_i 的身份。设系统当前有 k 个成员,利用中国剩余定理,可以求出同余方程组 $c \equiv y_i \pmod{p_i}, i = 1, \cdots, k$ 的解为 $c \equiv y_1P_1'P_1 + y_2P_2'P_2 + \cdots + y_kP_k'P_k \pmod P$,其中 $P = p_1p_2\cdots p_k = p_1P_1 = p_2P_2 = \cdots = p_kP_k, P_i'P_i \equiv 1 \pmod{p_i}, i = 1, \cdots k$。将 (n, e, c) 作为群公钥发布。

成员加入:一个新的成员要加入到群中,群中心须要为其生成签名密钥,并更新群公钥。设该成员为第 $k+1$ 个,其签名密钥 $(x_{k+1}, p_{k+1}, {p_{k+1}}^d)$ 的生成与系统建立时相同。重新计算群公钥 $c \equiv y_1P_1'P_1 + y_2P_2'P_2 + \cdots + y_kP_k'P_k + y_{k+1}P_{k+1}'P_{k+1} \pmod P$,其中新的 P, P_i', P_i 可由原来的 P, P_i', P_i 给出,即 $P = Pp_{k+1}, P_i = P_ip_{k+1}, P_i' = (P_i'p_{k+1}') \pmod{p_i}, i = 1, \cdots, k$,其中 p_{k+1}' $p_{k+1} \equiv 1 \pmod{p_i}$。群中心发布新的 c,并将 (ID_{k+1}, y_{k+1}) 送给群管理人。

成员撤销:这个过程与加入的过程类似,为了撤销成员 U_j,群中心将 y_j 改为一个随机数 y_j',重新计算和发布新的 c。

签名:成员 U_i 用 $(x_i, {p_i}^d)$ 来对一个消息 m 进行签名,计算 $s_i = h(m)^{x_i} \pmod n$,则 $(m, s_i, {p_i}^d)$ 为 U_i 对 m 的群签名。

签名验证:任何人可用群公钥对 $(m, s_i, {p_i}^d)$ 进行验证。首先计算 $p_i = ({p_i}^d)^e \pmod n$ 以及 $y_i = c \pmod{p_i}$,然后验证式子 $h(m) = {s_i}^{y_i} \pmod n$ 是否成立。若成立则签名正确,否则签名不正确。

签名打开:给出签名 $(m, s_i, {p_i}^d)$,群管理人可以计算 $p_i = ({p_i}^d)^e \pmod n$ 以及 $y_i = c \pmod{p_i}$,然后查找与 y_i 对应的 ID_i,就可以给出签名成员的身份。

2 文献[8]方案的安全性分析

该群签名方案的构造使用了 RSA 签名和中国剩余定理。群中心和所有群成员共用同一个 RSA 模数 n,n 的分解只有群中心知道。群中心有一对 RSA 签名和验证密钥 (d, e),每个群成员有一对 RSA 签名和验证密钥 (x_i, y_i)。另外每个群成员还有一个群成员证书 $(p_i, {p_i}^d)$。从该方案的安全性分析部分可见该方案的安全性基于分解 RSA 模数 n 的困难性。但是因为每个群成员知道自己的密钥对 (x_i, y_i),可以应用下面的算法能以极大的概率分解 n,从而使该方案不再安全。

下面假设群成员密钥对是 (x, y),满足 $xy \equiv 1 \pmod{\varphi(n)}$,则下面的算法[10]能以至少 1/2 的概率分解 n,如果算法运行 m 次,那么 n 被分解的概率至少为 $1 - 1/2^m$。

算法:RSA - FACTOR(n, x, y)
记 $xy - 1 = 2^r s$,s 为奇数
随机选择 w 使得 $1 \leqslant w \leqslant n - 1$
$a \leftarrow \gcd(w, n)$
if $1 < a < n$ then return (a) ;a 是 n 的一个因子
$v \leftarrow w^s \bmod n$
if $v \equiv 1 \pmod n$ then return ("failure")
while $v \neq 1 \pmod n$ do
{
  $v_0 \leftarrow v$
  $v \leftarrow v^2 \pmod n$
}
if $v_0 \equiv -1 \pmod n$ return ("failure")
else {

$a \leftarrow \gcd(v_0+1, n)$

return (a)

}; a 是 n 的一个因子

算法分析:

① 如果 w 是 p 或 q 的倍数,则通过 $\gcd(w,n)$ 可直接分解 n。

② 如果 w 与 n 互素,那么通过连续平方计算 w^r, w^{2r}, w^{4r}, …,直到对于某个 t,有 $w^{2^t r} \equiv 1 \pmod n$。由于 $xy-1=2^s r \equiv 0 \pmod{\varphi(n)}$,所以 $w^{2^t r} \equiv 1 \pmod n$。因此 while 循环至多执行 s 次就会终止。While 循环结束后,值 v_0 满足 $v_0^2 \equiv 1 \pmod n$ 且 $v_0 \neq 1 \pmod n$。如果 $v_0 \equiv -1 \pmod n$,那么算法失败;否则,v_0 是 1 模 n 的一个非平凡平方根,则 $\gcd(v_0+1, n)$ 是 n 的一个因子。

该算法的成功概率至少为 1/2。有两种情况使得算法分解 n 失败:①$w^r \equiv 1 \pmod n$;②$w^{2^t r} \equiv -1 \pmod n$,对于某个 t,$0 \leqslant t \leqslant s-1$。如果 w 是这 $s+1$ 个同余方程中至少一个的解,那么它是一个"坏"选择,算法失败。文献[10]详细讨论了这 $s+1$ 个同余方程的解,结果表明至多有 $(n-1)/2$ 个 w 的选择是"坏"的,容易知道至少有 $(n-1)/2$ 个选择是"好"的,因此算法成功的概率至少为 1/2。所以平均运行该算法 $1/(1-1/2)=2$ 就可以分解 n,如果运行 m 次,则 n 被分解的概率至少为 $1-1/2^m$。

一旦某个群成员分解了 n,则可以通过群公钥 e 计算出群中心的私钥 d;也可以根据其它群成员的签名求出其公钥 y,进而求出对应的私钥 x。这样,他就可以假冒任意一个群成员进行签名,也可以假冒群中心任意添加群成员、撤销群成员。因此该方案几乎不再具有任何群签名所需的安全性。

3　文献[9]的群签名方案

该方案基于 RSA 签名,也包含三个实体:群管理员 GM、撤销中心 RC 和群成员 B_i。GM 和 RC 共同建立系统参数,共同生成群成员的成员资格证书。打开群签名揭示签名者的真实身份则由 RC 完成。群成员可代表群体生成合法的群签名。

系统参数建立:首先,RC 选取五个大素数 p_1, p_2, f, p_1', p_2',满足 $p_1=2fp_1'+1$ 和 $p_2=2fp_2'+1$,计算 $n_C=p_1p_2$。随机选取密钥对(d_{RC}, e_{RC}),满足 $d_{RC}e_{RC} \equiv 1 \pmod{\varphi(n_C)}$。$g \in Z_{n_C}^*$ 是一个阶为 f 的元素,$h(\ )$ 是一个无碰撞的哈希函数。RC 公开参数$(n_C, f, g, e_{RC}, h(\ ), ID_{RC})$,$ID_{RC}$ 表示撤销中心的身份。其次,GM 选取两个大素数 p_3, p_4,且 p_3-1 和 p_4-1 含有大素数因子,计算 $n_G=p_3p_4$。随机选取密钥对(d_G, e_G),满足 $d_Ge_G \equiv 1 \pmod{\varphi(n_G)}$。群管理员的私钥为 $x_G \in Z_f^*$,公钥为 $y_G=g^xG \pmod{n_G}$。GM 公开参数(n_G, e_G, y_G, ID_G),ID_G 表示群管理员的身份。

群成员加入协议:如果一个成员要加入群,那么他选择一个随机数 $k \in Z_f^*$,计算其身份 $ID_B=g^k \pmod{n_C}$,并将其发送给 GM。GM 随机选择一个数 $\alpha \in Z_f^*$,计算 $r_G=g^\alpha \pmod{n_C}$,$s_G=\alpha+r_Gx_Gh(ID_B) \pmod f$,$w_G=(ID_G)^{-d_G} \pmod{n_G}$,将$(s_G, r_G, w_G)$作为成员资格证书秘密发送给该成员。该成员接收到$(s_G, r_G, w_G)$后,验证 $g^{s_G}=r_Gy_G^{r_Gh(ID_B)} \pmod{n_C}$ 和 $ID_G=w_G^{-e_G} \pmod{n_G}$ 是否成立,如成立,则为正确的资格证书,接受。同时群管理员将(ID_B, g^{s_G}, r_G)秘密发送给 RC,RC 首先验证 $g^{s_G}=r_Gy_G^{r_Gh(ID_B)} \pmod{n_C}$ 是否成立,如成立,则接受(ID_B, g^{s_G}, r_G)并计算 $w_C=(ID_{RC}r_Gy_G^{r_Gh(ID_B)}ID_B)^{-d_{RC}} \pmod{n_C}$,然后将 w_C 发送给该成员,同时 RC 在自己的群成员数据库中存储$(w_C, g^{s_G}, r_G, ID_B)$。成员 w_C 收到后,验证 $w_C^{-e_{RC}}=ID_{RC}r_Gy_G^{r_Gh(ID_B)}ID_B \pmod{n_C}$ 是否成立,如成立,则存储 w_C,那么该群成员的完整资格证书为(r_G, s_G, w_C, w_G)。

签名:群成员通过成员资格证书(r_G, s_G, w_C, w_G)对消息 m 进行签名。群成员选取三个随机数 $q_1, q_2, q_3 \in Z_f^*$,计算:$z_1=q_3e_{RC}g^{q_1} \pmod{n_C}$,$z_2=q_2^{e_G} \pmod{n_G}$,$u=h(z_1, z_2, m)$,$r_1=q_1+(s_G+k)u \pmod f$,$r_2=q_3w_C \pmod{n_C}$,$r_3=q_2w_G \pmod{n_G}$,最后所得的群签名是$(u, r_1, r_2, r_3, m)$。

验证:验证者得到群签名(u, r_1, r_2, r_3, m),计算:$z_1'=ID_{RC}^u g^{r_1}r_2e_{RC} \pmod{n_C}$,$z_2'=ID_G^u r_3^{e_G} \pmod{n_G}$,$u'=h(z_1', z_2', m)$,验证 u' 与 u 是否相等,如相等,则说明该签名是一个有效的群签名。

打开:RC 根据(u, r_1, r_2, r_3, m)通过以下计算来提示签名者的真实身份。计算:$\eta=1/u \pmod{\varphi(n_C)}$,$\delta=ID_{RC}^u g^{r_1} \pmod{n_C}$,对群成员数据库中存储的成员记录$(w_C, g^{s_G}, r_G, ID_B)$逐条检验,满足 $ID_B=(g^{r_1}/\delta g^{us_G})^\eta / w_C^{e_{RC}} \pmod{n_C}$ 的 ID_B 就是该签名的真实签名者。

4　文献[9]方案的安全性分析

该群签名方案不能有效地打开群签名并找到真实的签名者,任何一个群成员均可被判别为任一个群签名的签名人,因此该方案不满足群签名安全性中的可追踪性要求。

因为打开算法中的检测等式右边为：$(g^{r_1}/\delta g^{u s_G})^{\eta}/w_C^{\varepsilon u}(\mathrm{mod}\ n_C) = (g^{r_1}/ID_{RC}{}^{u} g^{r_1 u s_G})^{1/u}/w_C^{\varepsilon u}(\mathrm{mod}\ n_C) = (ID_{RC} g^{s_G})^{-1} w_C^{-\varepsilon u}(\mathrm{mod}\ n_C) = (ID_{RC} g^{s_G})^{-1} ID_{RC} r_G y_G^{r_G h(ID_B)} ID_B \pmod{n_C} = (ID_{RC} g^{s_G})^{-1} ID_{RC} g^{s_G} ID_B (\mathrm{mod}\ n_C) = ID_B (\mathrm{mod}\ n_C)$ 对任意一条成员记录（w_C，g^{s_G}，r_G，ID_B）都成立，所以用该算法不能找到真正的签名者。之所以出现这种情况，是因为在群签名 (u, r_1, r_2, r_3, m) 中包含成员身份信息的数据 u 和 r_1 在打开等式运算过程中被消去了，结果打开等式中根本没有用到签名中所含的签名者身份信息。

5 结 论

文中对两个群签名方案进行了安全性分析，指出了其中的缺陷。特别设计的群签名方案一般具有高效的优点，但因为群签名方案要求满足的安全性质太多，所以这类方案往往存在一些安全漏洞。如何对已有的特别设计的群签名方案进行改进，弥补其安全缺陷或设计新的高效安全的群签名方案仍然是值得研究的问题。

参考文献：

[1] Chaum D, van Heyst E. Group signatures[C]//Proc of EUROCRYPT'91. Lecture Notes in Computer Science. [s. l.]: [s. n.], 1991: 257-265.

[2] Camenisch J, Stadler M. Efficient group signature schemes for large groups[C]//Crypto'97. Lecture Notes in Computer Science. [s. l.]: [s. n.], 1997: 410-424.

[3] Camenisch J, Michels M. A group signature scheme with improved efficiency[C]//Asiacrypt'98. Lecture Notes in Computer Science. [s. l.]: [s. n.], 1998: 160-174.

[4] Ateniese G, Camenisch J. A practical and provably secure coalitionresistant group signature scheme[C]//Crypto'2000. Lecture Notes in Computer Science. [s. l.]: [s. n.], 2000: 255-270.

[5] Kim S J, Park S J, Won D H. Convertible group signatures [C]//Asiacrypt'96. Lecture Notes in Computer Science. [s. l.]: [s. n.], 1996: 311-321.

[6] Lee W, Chang C. Efficient group signature scheme based on the discrete logarithm[J]. IEE Proc Comput Digital Techniques, 1998, 145 (1): 15-18.

[7] Tseng Y M, Jan J K. Improved group signature based on discrete logarithm problem[J]. Electronics Letters, 1999, 35(1): 37-38.

[8] 陈泽文，张龙军，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.

[9] 张键红，伍前红，邹建成，等. 一种高效的群签名[J]. 电子学报，2005，33(6)：1113-1115.

[10] Stinson D R. 密码学原理与实践[M]. 第 2 版. 冯登国译. 北京：电子工业出版社，2005：165-169.

（上接第 145 页）

参考文献：

[1] Shaw M, Garlan D. Software Architecture: perspectives on an emerging discipline[M]. 北京：清华大学出版社(影印版)，1998.

[2] Perry D, Wolf A L. Foundations for the study of software architecture[J]. ACM Sigsoft Software Engineering Notes, 1992, 17(4): 40-52.

[3] Bass L, Clements P, Kazman R. Software Architecture in Practice[M]. New York: Addison Wesley Publishing, 1998.

[4] 万建成，卢 雷. 软件体系结构的原理、组成与应用[M]. 北京：科学出版社，2002.

[5] 张友生. 软件体系结构[M]. 北京：清华大学出版社，2004.

[6] 张友生，陈松乔. 正交软件体系结构的设计与进化[J]. 小型微型计算机系统，2004，25(2)：295-299.

[7] 孙昌爱，金茂忠，刘 超. 软件体系结构研究综述[J]. 软件学报，2002，13(7)：1228-1237.

[8] 赵会群，孙 晶，王国仁，等. 软件体系结构：一个新的研究领域[J]. 计算机科学，2002，29(11)：146-149.

[9] 董云卫，郝克刚. 一种面向方面的软件体系结构[J]. 微机发展，2004，14(6)：61-63.

[10] 张凤荔，杜小丹. 软件体系结构在软件生存期的应用研究[J]. 微型机与应用，1999(10)：4-5.

[11] 冯 冲，江 贺，冯静芳. 软件体系结构理论与实践[M]. 北京：人民邮电出版社，2004.

[12] 孙昌爱，金茂忠. 软件体系结构描述研究进展[J]. 计算机科学，2003，30(2)：136-139.

[13] 孙志勇，刘宗田，袁兆山. 软件体系结构描述语言 ADL 及其研究进展[J]. 计算机科学，2000，27(1)：36-39.

[14] 周 欣，黄 璜，孙家啸，等. 软件体系结构质量评价概述[J]. 计算机科学，2003，30(1)：49-52.

[15] 赵会群，孙 晶，王国远，等. 软件体系结构性能评价研究[J]. 计算机科学，2003，30(2)：144-146.

[16] 戎 玫，张广泉. 软件体系结构求精方法研究[J]. 计算机科学，2003，30(4)：108-110.

[17] 赵会群，王国仁，高 远. 软件体系结构抽象模型[J]. 计算机学报，2002，25(7)：1-7.

[18] 李 振，肖 书，唐胜群. 实用软件体系结构研究[J]. 计算机工程与应用，2000(8)：169-171.

[19] 韦 群，熊 璋，赵 芳. 软件体系结构开发方法及其应用[J]. 计算机工程与设计，2003，24(3)：77-80.