一种基于中国剩余定理的群签名方案

陈泽文[1], 张龙军[2], 王育民[3], 黄继武[1], 黄达人[1]
(1. 广州中山大学信息科学与技术学院, 广东广州 510275; 2. 上海交通大学计算机科学与工程系, 上海 200030;
3. 西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 在群签名方案中, 群中任意成员可以代表整个群体生成签名. 在有争议的情况下, 群管理人可以确定签名人的身份. 成员的撤消是群签名中的一个重要问题, 在目前已知的各种撤消方案中, 还不存在一种方案可以在不改变其它有效群成员的密钥的情况下, 安全地撤消群成员. 并且增加或撤消一个成员至少都需要指数运算, 因此计算复杂度高. 本文提出了一种基于中国剩余定理的群签名方案. 该方案有三个特征: (1) 在不改变其它有效群成员的密钥的情况下, 可以安全地增加或撤消群成员; (2) 增加或撤消的过程中只需要乘法运算, 并且在撤消时群公钥的长度不变; (3) 安全性是基于大数分解的困难性.

关键词: 群签名; 中国剩余定理; 成员撤消
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2004) 07-1062-04

A Group Signature Scheme Based on Chinese Remainder Theorem

CHEN Ze-wen[1], ZHANG Long-jun[2], WANG Yu-min[3], HUANG Ji-wu[1], HUANG Da-ren[1]
(1. School of Informational Science and Technology, Zhongshan University, Guangzhou, Guangdong 510275, China;
2. Department of Computer Science and Engineer, Shanghai Jiaotong University, Shanghai 200030, China;
3. National Lab of ISN, Xidian University, Xi. an, Shaanxi 710071, China)

Abstract: Group signature schemes allow any member of a group to sign message on behalf of the group. In case of dispute, the group manager can reveal the identity of actual signer. Revocation of membership is an important problem in group signature schemes, but among the existing group schemes, there is not any scheme which can safely delete the group member without changing secret keys of the other available group members and the cost of deleting group member is high. A new scheme based on Chinese remainder theorem is proposed in this paper and it has three merits. First, the group manager can safely add or delete members while keeping the secretkeys of the other available members unchanged. Second, only mutiplitation is needed and the length of group center. s public keys is unchanged during the revocation. Third, the security of this scheme relies on the factoring of large integers.

Key words: group signature; Chinese remainder theorem; revocation

1 引言

群签名是 D Chaum 和 E van Heyst[1] 于 1991 年提出的. 在一个群签名方案中, 一个群体中的任意一个成员可以代表整个群体对消息进行签名, 并且在有争议的时候, 可以由群管理人来确定签名人的身份. 与其它数字签名一样, 群签名是可以通过群公钥来公开验证的. 由于群签名在电子投票、电子商务等实际问题中具有广泛的应用, 因此引起许多研究者的注意. L Chen 和 T Pedersen[5] 提出了几个新的群签名方案, 并回答了文献[1] 中的一些公开问题, 同时首次提出了允许在一个群体中增加新成员的群签名方案. 1997 年, J Camenish 和 M Stadler[2] 首次提出了适用于大的群体的群签名方案. 从那以后, 人们提出了各种各样的群签名方案[2~4, 7~11], 这些研究主要考虑的是安全性和效率性. 但这些群签名方案都没有考虑到如何安全、有效地撤消一个群成员. 直到 2000 年, H J Kim、J I Lim 及 D H Lee[11] 才首次提出了一个可以撤消群成员的群签名方案. 但在他们的方案中, 存在一个更新密钥, 每次增加或撤消一个成员时, 都要改变更新密钥, 而其它的群成员都要根据这个改变的更新密钥去更新自己的秘密性质钥(secret property key), 并且在更新秘密性质钥时需要大量的指数运算, 这给其他成员带来繁重的和额外的开销. 在实际应用中, 每个成员并不希望当其它的成员离开或者加入时, 影响到自己的签名密钥.

基于以上考虑, 本文提出一种基于中国剩余定理的群签名方案, 可以在不改变其它有效成员的签名密钥的情况下, 安全地增加或撤消一个群成员. 在增加或撤消成员的过程中, 只

收稿日期: 2002-05-16; 修回日期: 2004-02-11
基金项目: 国家杰出青年基金(No. 60325208)、国家自然科学基金(No. 60133010, 60172067)、教育部跨世纪优秀人才基金、教育部博士点基金(No. 20020558038)

需要乘法运算并且在撤销过程中, 不改变群公钥的长度. 本文结构如下: 第 2.1.1 节和 2.1.2 节分别给出了群签名的定义、安全性要求以及中国剩余定理; 2.1.3 节中具体描述了所提出的基于中国剩余定理的群签名方案; 该方案的安全性在第 3 节中讨论; 最后给出结论.

2　基于中国剩余定理的新的群签名方案

2.1.1　群签名的定义及安全性要求

定义　一个群签名方案是包含以下过程的数字签名方案:

(1) 建立: 一个群中心用于产生群公钥和群成员及群管理人的密钥的算法.

(2) 加入: 一个用户和群中心之间的使用户成为群成员的交互协议.

(3) 撤消: 一个用来撤消群成员的算法.

(4) 签名: 一个算法, 当输入一个消息和一个群成员的签名密钥后, 输出对消息的签名.

(5) 验证: 一个在输入对消息的签名及群公钥后确定签名是否有效的算法.

(6) 打开: 一个在给定签名及群私钥的条件下确定签名人身份的算法.

群签名的安全性要求:

(1) 匿名性. 给定一个群签名后, 除了群管理人之外, 任何人确定签名人的身份在计算上是困难的.

(2) 防伪造性. 只有合法的群成员才能产生有效的群签名.

(3) 可跟踪性. 群管理人在必要的时候可以打开一个签名以确定签名人的身份, 而且签名人不能阻止一个合法签名的打开.

(4) 防陷害攻击. 任何成员及群管理人都不能以其他成员的名义产生合法的群签名.

(5) 抗联合攻击. 即使一些成员串通在一起也不能产生一个合法的不能被跟踪的群签名.

(6) 不可关联性. 除了群管理人外, 任何人想判断两个或两个以上的消息是否由同一个成员产生是困难的.

2.1.2　中国剩余定理

设 $p_1, p_2, \cdots, p_k$ 是两两互素的 k 个正整数, $k \geqslant 2$, 令

$$P = p_1 p_2 \cdots p_k = p_1 P_1 = p_2 P_2 = \cdots = p_k P_k$$

其中: $P_i = \frac{P}{p_i}$, $i = 1, 2, \cdots, k$.

则同时满足同余方程组

$$\begin{cases} c \equiv y_1 \pmod{p_1} \\ c \equiv y_2 \pmod{p_2} \\ \cdots\cdots \\ c \equiv y_k \pmod{p_k} \end{cases}$$

的正整数解是:

$$c \equiv y_1 Pc_1 P_1 + y_2 Pc_2 P_2 + \cdots + y_k Pc_k P_k \pmod{P}$$

其中 Pc_i 是满足同余方程:

$$Pc_i P_i \equiv 1 \pmod{p_i}, \quad i = 1, 2, \cdots, k$$

的正整数解.

2.1.3　基于中国剩余定理的群签名方案

本方案中存在着三个实体: 群中心, 群管理人, 群成员. 其中群中心用来建立整个系统及为每个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签名, 确定签名者的身份.

2.1.3.1　系统的建立　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 $ed \equiv 1 \pmod{\varphi(n)}$, 其中 $\varphi()$ 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 $x_i \neq y_i \equiv 1 \pmod{\varphi(n)}$, 选择素数 p_i 大于 y_i, 使当 $i \neq j$ 时, $\gcd(p_i, p_j) = 1$, 这里的 gcd 表示最大公约数, 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, 相信是群中心送来的, 并将 (x_i, p_i, p_i^d) 作为签名密钥保存. 群中心将 (ID_i, y_i) 送给群管理人, 其中 ID_i 是用户 U_i 的身份.

不失一般性, 设系统现在有 k 个成员. 利用中国剩余定理, 可以求出同余方程组

$$c \equiv y_i \pmod{p_i}, \quad i = 1, \cdots, k$$

的解为

$$c \equiv y_1 Pc_1 P_1 + y_2 Pc_2 P_2 + \cdots + y_k Pc_k P_k \pmod{P}$$

其中 Pc_i, P_i, P 如 2.2 所给. 将 (n, e, c) 作为群公钥发布.

2.1.3.2　成员加入　假设 Bob 想成为群中的一个成员, 并向群中心提出申请. 群中心首先随机选择 $x_{k+1} \in Z_n$, 由 $x_{k+1} y_{k+1} \equiv 1 \pmod{\varphi(n)}$, 可以求出 y_{k+1}, 然后选择大于 y_{k+1} 的素数 p_{k+1}, 使 $\gcd(p_{k+1}, p_i) = 1$, $i = 1, \cdots, k$. 重新计算 $c \equiv y_1 Pc_1 P_1 + y_2 Pc_2 P_2 + \cdots + y_k Pc_k P_k + y_{k+1} Pc_{k+1} P_{k+1} \pmod{P}$ 其中新的 P, Pc_1, P_1 都能通过原来的 P, Pc_1, P_1 给出, 即

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

$P_i = P_i p_{k+1}$, $Pc_i = (Pc_i p_{k+1}) \pmod{p_i}$, $i = 1, \cdots, k$ 其中 $pc_{k+1} p_{k+1} \equiv 1 \pmod{p_i}$. 群中心发布新的 c, 并将 $x_{k+1}, p_{k+1} p_{k+1}^d$ 送给 Bob, 将 (ID_{k+1}, y_{k+1}) 送给群管理人. 则 Bob 成为一个新的群成员, 此时不改变其它有效成员的签名密钥, 并且在此过程中, 只需要乘法运算而不需要指数运算, 因此效率比较高. 此时, 群公钥只有 c 发生改变, 但并不改变群公钥的个数.

2.1.3.3　成员撤消　这个过程与加入的过程类似. 设现在有 k 个成员, 并且

$$c \equiv y_1 Pc_1 P_1 + y_2 Pc_2 P_2 + \cdots + y_k Pc_k P_k \pmod{P}$$

为了撤消群中的 U_j 成员, 群中心将 y_j 改为另外的一个随机数 yc_j, 并且重新计算 c,

$$c \equiv y_1 Pc_1 P_1 + y_2 Pc_2 P_2 + \cdots + yc_j Pc_j P_j + \cdots + y_k Pc_k P_k \pmod{P}$$

发布新的 c. 从上面的撤消过程可以看出, 要撤消一个群成员, 对于群中心来讲, 只需要改变 c 的值和进行几个简单的计算并且由于 P 是固定不变, 因而 c 的长度不变, 从而整个群中心公钥的长度不变. 而对于有效的群成员, 此时并不需要更新自己的签名密钥. 所以上面的撤消过程, 不管是对群中心还是群成员都是简单和高效.

2.1.3.4　签名　成员 U_i 现在用 (x_i, p_i^d) 来对一个消息 m 进行签名, 成员 U_i 计算 $s_i = m^{x_i} \pmod{n}$, 则 (m, s_i, p_i^d) 就是成员 U_i

对 m 的签名.

2.3.1.5 签名验证 若 Alice 想对签名(m, s_i, p_i^d)进行验证. 首先由群中心的公钥 e, 计算 $p_i = (p_i^d)^e \pmod n$ 以及 $y_i = c \pmod{p_i}$, 接着验证式子 $h(m) = s_i^{y_i} \pmod n$ 是否成立. 若成立则签名正确, 否则签名不正确. 验证过程如下:

$$s_i^{y_i} \pmod n = (h(m)^{x_i})^{y_i} \pmod n \pmod n = h(m)$$

2.3.1.6 签名的打开 给出签名(m, s_i, p_i^d,) 后, 群管理人计算 $p_i = (p_i^d)^e \pmod n$, $y_i = c \pmod{p_i}$, 通过与 y_i 相应的 ID_i, 就可以给出签名成员的身份.

3 签名方案的安全性分析

这里安全性的分析可分为三种可能的攻击: (1) 得到 U_i 的签名密钥; (2) 伪造群成员签名; (3) 联合攻击. 下面就对这三种情形进行分析.

3.1.3.1.1 得到签名密钥 若 Alice 想从签名(m, s_i, p_i^d,) 来获得成员 U_i 的签名密钥, 由 p_i^d 和群中心的公钥 e, 可以求得 p_i, 从而可通过 $y_i = c \pmod{p_i}$, 即可以获得成员 U_i 的公钥 y_i, 这时想通过 y_i 来得到 x_i, 则必须知道 n 的分解, 这在计算上是困难的.

3.1.3.1.2 伪造签名 在这里又分三种情形: (1) Alice 以前就不是群成员; (2) Alice 以前是群的成员, 但现在被撤消了. (3) Alice 现在是群成员, 想伪造另外一个成员签名.

(1) Alice 以前就不是群成员, 则 Alice 想伪造签名, 则必须获得某个成员 U_i 的公钥 y_i, 密钥 x_i 及 p_i^d, 同 3.3.1 分析的一样, 这时必须知道 n 的分解.

(2) Alice 以前是群的 i 成员, 现在已经被撤消了. 但现在 Alice 知道(x_i, y_i, p_i, p_i^d), 由于 Alice 已经被撤消, 因此 y_i 已经被改为 yc_i, 此时 Alice 不知道 n 的分解, 所以 Alice 想通过 yc_i 来获得 xc_i, 使 $xc_i yc_i = 1 \pmod{\varphi(n)}$ 是不可行的. 另外 Alice 也可以通过对 c- y_i 进行分解, 使得 c- y_i = n- pc_i, 其中 pc_i 是个素数, 这时 Alice 有(x_i, y_i, p_i^d, pc_i), 并且 $y_i = c \pmod{pc_i}$ 及 $x_i y_i = 1 \pmod{\varphi(n)}$, 这时 Alice 想对一个消息进行合法的签名, 她还必须计算 $(pc_i)^d$, 但 d 是群中心的私钥, Alice 无法从群中心的公钥 e 来得到 d, 所以这是 Alice 无法进行伪造签名.

(3) 若 Alice 现在是 U_i 群成员, 想伪造另外一个合法成员 U_j 签名. 此时 Alice 知道自己的签名密钥(x_i, y_i, p_i, p_i^d), 并且她可以获得 U_j 的签名来获得 U_j 的签名密钥(y_j, p_j, p_j^d). 类似前面的分析, Alice 想获得 x_j 是困难的.

3.1.3.1.3 联合攻击 假设一些成员和群管理人联合在一起, 想伪造 U_j 进行签名, 则他们必须获得 U_j 的签名密钥(x_j, y_j, p_j, p_j^d). 同第 3.1.3.1.2 一样, 这些成员跟群管理人可以知道(y_j, p_j, p_j^d), 由于都不知道 n 的分解, 并且分解的困难性是可以抵抗联合攻击, 所以这些成员跟群管理人联合起来也无法得到 x_j. 从而无法伪造 U_j 产生合法的签名.

这里需要说明的是本方案并不满足不关联性. 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[14].

4 结论

本文在中国剩余定理的基础上, 提出了一种新的群签名方案, 这个方案是基于大数分解的困难性. 具有以下几个特点: (1) 在不改变其它有效群成员的签名密钥的情况下, 可以安全地加入或撤消群成员; (2) 在群成员加入或撤消的过程中, 计算复杂度小, 效率高. 并且在撤消成员的过程中, 群公钥的长度保持不变; (3) 安全性好, 可以抵抗联合攻击、防伪造签名等. 而且可以采用时间戳协议的方法来验证一个被撤消的成员的合法签名(没被撤消前的签名) . 即通过时间戳协议, 群管理人可以判断该签名是否为该成员在有效成员时的签名, 若是的话, 根据保留下来的公钥对签名进行验证. 由于本方案在签名、验证、打开等过程的计算复杂度与群成员的个数无关, 故所要求的计算量小. 但在系统的建立、群成员的加入和撤消过程中的计算量跟群体中群成员的个数是线性相关的, 这就要求群中心要有较高的计算能力. 因此本方案适合于在服务端有较高的计算能力, 而对客户端的资源要求不高的情形, 如移动通信网等.

参考文献:

[1] Chaum D, Heyst V E. Group signatures[A]. Proc of EUROCRYPT. 91[C]. Lecture Notes in Computer Science, 1991, 547: 257- 265.

[2] Camenish J, Stadler M. Efficient group signatures for large groups[A]. Proc. of CRYPTO. 97[C]. Lecture Notes in Computer Science, 1997, 1296: 410- 424.

[3] Camenish J, Michels M. A group signature scheme with improved efficiency[A]. Proc. of ASIACRYPT. 98[C]. Lecture Notes in Computer Science, 1998, 1541: 160- 174.

[4] Ateniese G, Tsudik G. Some open issues and new directions in group signatures[OL]. http://www.isi.edu/~gts/pubs.html.

[5] Chen L, Pedersen T. New group signature schemes[A]. Proc. of EUROCRYPT. 94[C]. Lecture Notes in Computer Science. 1995, 950: 171- 181.

[6] Camenish J. Efficient and generalized group signatures[A]. Proceedings of CRYPTO. 93[C]. Lecture Notes in Computer Science, 1993, 1233: 302- 318.

[7] Kims J, Parks J, Won D H. Group signatures for hierarchical multigroups[J]. Lecture Notes in Computer Science, 1998, 1163: 273- 281.

[8] Hysyansksya A, Ramzan Z. Group blind digital signatures: A scalable solution to electronic cash[A]. Pro. of the 2nd Financial Cryptography Conference[C]. Anguilla, BWI, 1998. 184- 197.

[9] Park S, Kims J, Wond H. A practical identity based group signature[A]. Conference on Electronics, Information and Communications (ICEIC. 95)[C]. China, 1995. 64- 67.

[10] Petersen H. How to convert any digital signature scheme into a group signature scheme[M]. Security Protocols Workshop, Paris, 1997. 177- 190.

[11] Hyun Jeong Kim, Jong In Lim, Dong Hoon Lee. 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, 2000, 2015: 150- 161.

[12] 卢开澄. 计算机密码学))) 计算机网络中的数据保密与安全(第二版)[M]. 北京: 清华大学出版社, 1998.
[13] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 1999.
[14] Toru Nakanishi, Toru Fujiwara, Hajime Watanabe. 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.

作者简介:

陈泽文　男, 1975 年生于福建惠安, 中山大学信息科学与技术学院博士研究生, 研究方向为密码和信息安全.

张龙军　男, 上海交通大学计算机科学与工程系博士后, 研究方向为信息安全.

王育民　男, 1936 年出生于陕西西安, 西安电子科技大学通信工程学院教授, 博士生导师, 研究方向为密码学与信息安全.

黄继武　男, 中山大学信息科学与技术学院教授, 博士生导师, 研究方向为多媒体信息安全.

黄达人　男, 中山大学信息科学与技术学院教授, 博士生导师, 研究方向为小波理论及应用.