一种高效的群签名

张键红[1], 伍前红[2], 邹建成[1], 王育民[2]
(1. 北方工业大学理学院, 北京 100041; 2. 西安电子科技大学 ISN 国家实验室, 陕西西安 710071)

摘 要: 基于强 RSA 假设, 本文提出了一种高效的群签名方案. 由于该方案没有采用知识签名作为基本构件使得该方案的签名算法和验证算法都非常简单, 以至于该方案一个突出优点是签名与验证所需的总计算量仅仅为 9 次模指数运算远远少于目前最好的 ACJT 签名方案; 最后, 我们分析该方案的效率, 与 ACJT 等几种方案相比在计算效率上有明显的提高.

关键词: 群签名; 匿名性; 抵制勾结性; 不相关性
中图分类号: TP918.2 文献标识码: A 文章编号: 0372-2112 (2005) 06-1113-03

An Efficient Group Signature Scheme

ZHANG Jian-hong[1], WU Qian-hong[2], ZOU Jian-cheng[1], WANG Yu-min[2]
(1. *College of Sciences, North China University of Technology, Shijingshan District, Beijing 100041, China;*
2. *State Key Lab on ISN, Xidian University, Xi'an, Shaanxi 710071, China*)

Abstract: We propose a new efficient group signature scheme based on Strong RSA assumption. Because the scheme doesn't adopt knowledge proof signature as building block, it is simple to sign algorithm and verify algorithm in the scheme, so that the primary merit of the scheme is that the total computation of signature and verification is only 9 exponent operations and much less than the state-of-the-art ACJT scheme in computation cost. Finally, we analyze the efficiency of the proposed scheme and show that the scheme is more efficient than group signature schemes such as ACJT scheme in complexity.

Key words: unlinkability; group signature; anonymity; coalition-resistant

1 引言

随着电子商务的飞速发展, 手写签名正在被数字签名所替代. 由于数字签名技术在不同领域的广泛应用, 人们对数字签名也提出了不同的要求, 因而, 为了适应不同情况的需要, 不同类型的数字签名方案相继被提出, 如一次签名、盲签名、代理签名、群签名等. 自 1991 年, Chaum 和 Heyst 在文[1]提出了群签名概念以后, 群签名就在不同的领域得到广泛应用如: 电子货币、电子选举等; 群签名就是允许任何群成员代表群进行匿名地签名, 如发生争执, 群管理员能够揭示签名者的真实身份, 同时, 区分两个不同的群签名是否来自于同一个人在计算上是不可行的. 近年来, 许多不同的群签名方案[1~8]被提出, 一些方案的签名长度或群公钥长度随着群成员的人数增多线性增加, 不适合大规模的群. Camenisch 和 Stadler 在文[6]提出了第一个具有固定长度的群公钥和签名的签名方案. Ateniese Tsudik 在文[2]中改进了 Camenisch-Stadler 方案是目前较好的一种群签名方案. 但由于通过知识证明签名来实现群签名, 所以在效率上并不高. 在本文, 我们基于 RSA 签名给出了一种高效的群签名方案, 与文[2, 4, 5]的群签名方案相比有更高的效率仅需 9 次模指数运算.

2 群签名

一个群签名方案就是允许任意群成员代表群进行匿名地签名, 同时, 一个用户可以用群公钥来验证签名的正确性, 然而, 验证者却不能得到有关群成员的任何消息, 签名和群成员之间没有关联性, 并且不能决定两个不同的群签名是否来自同一个签名者, 如果发生争执, 验证者可以求助群管理员来揭露签名者的真实身份.

通常, 一个群签名由下列算法组成:

- 系统建立: 群管理员选择秘密钥, 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, 并注册她的身份.
- 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, 运行打开算法来提取成员资格揭示签名者的真实身份.

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, 决定该签名是由哪个群成员产生在计算上是不可能的, 除了群管理员外.

收稿日期: 2003-05-30; 修回日期: 2005-02-18
基金项目: 973 国家重大项目(G19990358-04); 北方工业大学博士启动基金

• 不相关性: 决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: 一个正确的签名可以被群管理员揭开签字者的真实身份.

• 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.

3 一种高效的群签名

3.1 系统参数建立

该群签名方案由三个实体: 群管理员 GM、撤销中心 RC 和群成员 B_i 组成(下面以群成员 Bob 为例). 首先, 撤销中心 RC, 选取五个大素数 p_1, p_2, f, p'_1, p'_2, 且满足 $p_1 = 2fp'_1 + 1$ 和 $p_2 = 2fp'_2 + 1$, 计算 $n_C = p_1 p_2$. 随机选一个整数 e_{RC} 满足 $\gcd(e_{RC}, \varphi(n_C)) = 1$, 计算 d_{RC} 满足 $d_{RC} e_{RC} = 1 \bmod \varphi(n_C)$, 其中 $\varphi(n_C)$ 是欧拉 Totient 函数; $g \in Z^*_{n_C}$ 是一个阶数为 f 的元素. $h(\cdot)$ 是一个无碰撞的哈希函数. SPK 表示知识签名, 详细内容参见文[2], 撤消中心 RC 公开参数为 $(n_C, f, g, e_{RC}, h(\cdot), ID_{RC})$, ID_{RC} 表示撤消中心的身份. SPK[γ: $y = g^{\gamma}$]($\prime\prime$) 表示 y 对 g 的知识签名.

其次, 群管理员 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 $n_G = p_3 p_4$. 随机选一个整数 e_G 满足 $\gcd(e_G, \varphi(n_G))$, 计算 d_G 满足 $d_G e_G = 1 \bmod \varphi(n_G)$; 群管理员的私钥为 $x_G \in Z^*_f$, 公钥为 $y_G = g^{x_G} \bmod n_G$. 公开参数为 (n_G, e_G, y_G, ID_G), ID_G 表示群管理员的身份.

3.2 群成员加入协议(Join Protocol)

如果一个成员 Bob 要加入群, 选择一个随机数 $k \in Z^*_f$, 秘密保存 k, 并计算其身份 $ID_B = g^k \bmod n_C$, 和 $\delta = SPK[\gamma: ID_B = g^{\gamma}](\prime\prime)$ 并把二元组 (ID_B, δ) 发送给群管理员 GM, 其目的是向群成员证明他知道秘密值 k 和提交身份. 群成员首先通过 (ID_B, δ) 验证知识签名的正确性, 其次, 为了生成群成员 Bob 的成员资格证书, GM 随机选择一个数 $\alpha \in Z^*_f$, 并计算

$$r_G = g^{\alpha} \bmod n_G,\ s_G = \alpha + r_G x_G h(ID_B) \bmod f,\ w_G = (ID_G)^{-d_G} \bmod n_G$$

并通过秘密信道发送 (s_G, r_G, w_G) 给 Bob.

当 Bob 接到 (s_G, r_G, w_G) 后,

验证 $g^{s_G} = r_G y_G^{r_G h(ID_B)} \bmod n_C$

$ID_G = w_G^{-e_G} \bmod n_G$

是否成立, 如果成立就接收 (r_G, s_G, w_G).

同时, 群管理员 GM 通过秘密信道发送群成员 Bob 的身份 ID_B, (g^{s_G}, r_G) 给撤消中心 RC, 目的是通知撤消中心 RC, Bob 为群成员.

当撤消中心 RC 接到 ID_B, (g^{s_G}, r_G) 后,

验证 $g^{s_G} = r_G y_G^{r_G h(ID_B)} \bmod n_C$

是否成立, 如果成立, 接收 (g^{s_G}, r_G), 接着计算

$$w_C = (ID_{RC} r_G y_G^{r_G h(ID_B)} ID_B)^{-d_{RC}} \bmod n_C$$

并发送 w_C 给 Bob, 同时撤消中心在自己的群成员数据库中存储 $(w_C, g^{s_G}, r_G, ID_B)$. 当 Bob 接到撤消中心发送的 w_C 后, 首先, 验证 $w_C^{-e_{RC}} = ID_{RC} r_G y_G^{r_G h(ID_B)} ID_B \bmod n_C$ 是否成立, 如果等式成立, 就存储 w_C. 那么群成员 Bob 的成员资格证书为 (r_G, s_G, w_G, w_G).

3.3 群签名的产生(Sign Algorithm)

在签名阶段, 群成员 Bob 通过成员资格证书 (r_G, s_G, w_G, w_G) 对消息 m 进行签名. 群成员 Bob 选取两个随机数 $q_1, q_2, q_3 \in Z^*_f$

计算

$$z_1 = q_3^{e_{RC}} g^{q_1} \bmod n_C$$

$$z_2 = q_2^{e_G} \bmod n_G,\ u = h(z_1, z_2, m)$$

$$r_1 = q_1 + (s_G + k) u \bmod f$$

$$r_2 = q_3 w_C^u \bmod n_C,\ r_3 = q_2 w_G^u \bmod n_G$$

最后所得的群签名为 (u, r_1, r_2, r_3, m).

3.4 群签名的验证(Verify Algorithm)

当验证者得到群签名 (u, r_1, r_2, r_3, m) 时, 计算:

$$z'_1 = ID_{RC}^u g^{r_1} r_2^{e_{RC}} \bmod n_C$$

$$z'_2 = ID_G^u (r_3)^{e_G} \bmod n_G$$

$$u' = h(z'_1, z'_2, m)$$

并验证: $u \stackrel{?}{=} u'$ 是否成立. 如果成立说明 (u, r_1, r_2, r_3, m) 是一个有效的群签名.

3.5 群签名的打开(Open Algorithm)

如果发生争执, 群管理员可以求助撤消中心来打开一个群签名来揭示签名者的真实身份. 由于撤消中心保存着每个群成员的个人消息 (w_C, ID_B, g^{s_G}), 对一个群签名 (u, r_1, r_2, r_3, m) 而言, 撤消中心 RC 通过以下计算来揭示签名者的真实身份.

Step1: 计算 $\eta = 1/u \bmod \phi(n_C)$

Step2: 计算 $\delta = ID_{RC}^u g^{r_1} \bmod n_C$

Step3: 检验 $ID_B = (g^{r_1}/\delta g^{us_G})^{\eta} / w_C^{e_{RC}} \bmod n_C$ (1)

检验 ID_B, g^{s_G} 是否满足上面的等式(1), 如果满足说明 ID_B 就是该签名的真实签名者.

4 安全与性能分析

在本节, 我们将对上文所提出的新的群签名方案进行安全与性能分析.

定理 如果群签名 (u, r_1, r_2, r_3, m) 是由群成员产生, 那么该签名一定能够通过验证.

证明 由下面关系

$$\begin{aligned} z'_1 &= ID_{RC}^u g^{r_1} r_2^{e_{RC}} \bmod n_C \\ &= ID_{RC}^u g^{q_1 + (s_G + k)u} (q_3 w_C^u)^{e_{RC}} \bmod n_C \\ &= ID_{RC}^u g^{q_1} (r_G y_G^{r_G h(ID_B)})^u ID_B^u ((ID_{RC} r_G y_G^{r_G h(ID_B)} ID_B)^{-d_{RC}})^{ue_{RC}} \\ &\quad q_3^{e_{RC}} \\ &= q_3^{e_{RC}} g^{q_1} = z_1 \end{aligned}$$

$$z'_2 = ID_G^u (r_3)^{e_G} = ID_G^u (q_2 w_G^u)^{e_G} = q_2^{e_G} = z_2$$

所以有 $u = h(z'_1, z'_2, m)$, 因而 (u, r_1, r_2, r_3, m) 可以通过群签名的验证. 从而, 满足群签名的正确性.

匿名性: 在我们的方案中, 群签名是 (u, r_1, r_2, r_3, m) 形式, u 是一个哈希值具有随机性, r_1, r_2, r_3 中都含有随机数, 因而, r_1, r_2, r_3 都具有随机性; 不可能从 u, r_1, r_2, r_3 得到签名者的任何信息, 所以任何人(除签名者以外)都无法从群签名

中得到关于签名者的相关信息.

不相关性: 对于两个不同的群签名(u, r_1, r_2, r_3, m)和$(u', r'_1, r'_2, r'_3, m')$, 由于签名时, 签名者选择两个随机数来计算的$u(u')$, $r_1, r_2, r_3(r'_1, r'_2, r'_3)$, 因而, 每次的签名都不同. 同时, r_1, r_2, r_3和r'_1, r'_2, r'_3是完全独立的, 所以不可能从两个不同的群签名中来决定是否来自于同一个人.

不可伪造性: 就成员的加入阶段而言, 一个合格的群成员拥有成员资格证书(w_G, w_C, s_G); 对群管理员而言, 他只有成员资格证书的一部分(w_G, s_G), 他可以伪造(u, r_1, r_3, m), 但是不能成功的伪造一个r_2来通过验证阶段, 因为他不知道撤消中心的私钥d_{RC}, 因而不伪造一个有效的r_2. 对撤消中心而言, 他也只知道成员资格证书的一部分w_G, 不知道群管理员的私钥d_G; 其次, 虽然撤消中心有g^{s_G}, 但不可能从g^{s_G}求解s_G, 求解s_G等价于求解离散对数, 因此, 无法伪造一个有效的群签名.

抵制联合攻击: 在我们的方案中, 我们假定群管理员与撤消中心不相互勾结. 对两个不同的群成员而言, 不可能成功的伪造一个群签名, 由于他们要想联合伪造一个群签名等价于伪造一个 ElGmal 签名. 因为, 从群成员的加入阶段可知, 每一个群成员的证书实质是一个对他身份 ID 进行了一个 ElGmal 签名(变体) 和群管理员与撤消中心对群成员身份 ID 的 RSA 签名. 因 ElGmal 签名的不可伪造性, 所以可以得到两个不同的群成员不可能伪造一个有效的群签名.

就效率而言, 我们的群名方案有更高的效率, 在一个签名方案中, 模指数和模求逆运算量是决定算法效率的主要因素, 我们用 Exp 表示模指数运算, Inv 求逆运算, 我们的方案与文[2, 4, 5]运算两相比.

表 1　我们的新方案与文[2, 4, 5]中的方案的计算量比较

	签名	验证	总的计算量
改进的 L-C 方案	7exp+ 1Inv	6exp	13exp+ 1Inv
G-Z 签名方案	4exp	7exp	11exp
ACJT 方案	10exp	12exp	22exp
我们的方案	4exp	5exp	9exp

从表中, 我们可以发现, 我们的方案具有较好的效率.

5　总结

匿名性和不相关性是群签名的两个显著特点, 由于这些特点广泛的 应用于电子拍卖和电子货币等系统, 本文基于强 RSA 假设给出了一种高效的群签名方案, 该方案满足群签名方案所具备的所有性质, 具有固定长度的群公钥和群签名, 签名与验证的所需的总计算量仅为 9 次模指数运算, 与文[2, 4, 5]群签名方案相比在效率上有明显的优势, 非常适合大规模的群体.

参考文献:

[1] G ATENIESE, J CAMENISH, M JOYE, G TSUDIK. A practical and provably secure coalition-resistant group signature scheme[A]. M Bellare. Advances in Cryptology-Crypto' 2000[C]. Berlin: Springer-Verlag: 2000. 255- 270.

[2] G ATENIESE, G TSUDIK. Some open issues and new direction in group signature[A]. M Bellare. Advance in Financial Cryptograpy' 99 [C]. Berlin: Springer-Verlag, 1999. 225- 237.

[3] J CAMENISH, M MICHELS. A group signature with improved efficiency[A]. K Ohta, D Pei. Advance in Cryptology-Proceedings of Asiacrypt' 98[C]. Berlin: Springer-Verlag, 1999. 160- 173.

[4] 陈凯, 祝世雄. 一个新的群签名方案[J]. 计算机工程 (增刊), 2000, 26(26): 117- 122.
CHEN Kai, ZHU Shixiong. A new group signature scheme[J]. Computer Engineer (Supplement), 2000, 26(26): 117- 122.

[5] LEE W R, CHANG C C. Efficient group signature scheme based on the discrete logarithm[J]. IEE Proc Computer Digital Technology, 1998, 145(1): 15- 18.

[6] CHAUM D, HEYST F. Group signature[A]. Rivest. Advance in Cryptology-Proceeding of EUROCRYPT' 91[C]. Berlin: Springer-verlag, 1992. 257- 265.

[7] CONSTANTIN POPESCU. An efficient group signature scheme for large groups[J]. Studies in Informatics and Control, 2001, 10(1): 1232- 1243.

[8] J H ZHANG, Q H WU, Y M WANG. A novel efficient group signature with forward security[A]. International Conference of Information and Communications Security 2003[C]. Berlin: Springer-verlag, 2003. 292 - 299.

作者简介:

张键红　男, 1975 年 11 月出生于河北省石家庄市, 现为北方工业大学理学院信息与计算学科讲师、2004 年毕业西安电子科技大学, 获博士学位, 在国内外发表学术论文 40 余篇, 研究方向: 数字签名, 电子商务安全, 网络安全. E-mail: jhZHANG@ncut.edu.cn

伍前红　男, 1975 年 9 月出生于四川省内江市, 2004 年毕业于西安电子科技大学获博士学位, 主要研究方向为密码学和信息安全. E-mail: wqh555@163.com

邹建成　男, 1966 年 9 月出生于贵州省, 北方工业大学教授, 理学院"应用数学"硕士点学科带头人博士, 主要研究方向为数字图象信息安全理论中的信息隐藏和数字水印、计算机图形学、微分拓扑学中的奇点理论、分歧理论. E-mail: zjc@ncut.edu.cn

王育民　男, 1936 年 7 月出生于北京市, 西安电子科技大学教授、博士导师, IEEE 高级会员, 主要研究方向为为编码与密码, 信息安全与信息论. E-mail: ymwang@xidian.edu.cn