一种改进的代理多重签名方案

谷利泽[1], 高 宏[2], 杨义先[1]
(1. 北京邮电大学信息安全中心, 北邮国家重点实验室, 北京 100876;
2. 北京市朝阳区光华路 1 号嘉里中心北楼 601 英特尔公司, 北京 100020)

摘 要: 在 Kim-like 代理多重签名方案的基础上, 提出一个改进的代理多重签名方案, 它解决原方案存在的两个问题: (1) 安全性, 任意一个原始签名者能伪造代理多重签名. (2) 效率, 代理多重签名的长度和验证其签名效率与原始签名者的个数有关.

关键词: 代理签名; 多重签名; 代理多重签名; 安全性; 高效性
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2005) 01-0088-03

An Improved Proxy Multi-Signature Scheme

GU Li-ze[1], GAO Hong[2], YANG Yi-xian[1]
(1. Information Engineering School, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. 6th floor, North Office Tower, # 601 Beijing Kerry Centre, 1, GuangHua Road, ChaoYang District, Beijing 100020, China)

Abstract: On the basis of the Kim-like. s proxy multi-signature scheme, we propose an improved proxy multi-signature scheme, which resolves two problems in the Kim-like s proxy multi-signature scheme: (1) Security, anyone of the multi-original signers can forge a valid proxy multi-signature for any message. (2) Efficiency, the size of the proxy multi-signature and the efficiency of checking whether it is avail are dependent on the number of the original signers.

Key words: proxy signature; multi-signature; proxy multi-signature; security; high efficiency

1 引言

所谓代理多重签名方案是指两个以上的原始签名者将他们的签名权同时指派给一个代理签名者, 这个代理签名者代表多个原始签名者实现他们的多重签名. 代理多重签名在现实生活中是比较常见的, 例如, 一个公司发表的声明涉及到财务部、开发部、销售部、售后服务部等部门, 需要这些部门签名认可, 如果这类声明较多, 这些部门指定一个它们都信赖的人或部门代表它们签名, 与这些部门共同生成多重签名相比, 其效率大大提高.

文献[1]提出一个 Kim-like 代理多重签名方案, 它存在以下两方面问题:

(1) 安全性: 任何一个原始签名者能伪造代理多重签名.

(2) 效率: 代理多重签名的长度和验证效率与原始签名者个数有关.

2 符号的约定

下面介绍后面使用的符号含义:

p: 大素数(满足安全要求). g: 域 GF(p) 的本原元.

q: 是 p- 1 的大素数因子, 且满足 $g^q \equiv 1 \pmod p$.

h: 安全的哈希函数. m: 签名的消息.

A_i: 第 i 个原始签名者(i= 1, , , n). B: 代理签名者.

m_w: 描述原始签名者授权代理签名者代理权限的约定, 称为代理授权书, 包括 A_i 的标识、B 的代理期限、签名消息范围等信息(i= 1, , , n).

x_i: 原始签名者 A_i 的私钥(i= 1, , , n).

y_i: 原始签名者 A_i 的公钥, $y_i = g^{x_i} \bmod p$(i= 1, , , n).

x_B: 代理签名者 B 的私钥.

y_b: 代理签名者 B 的公钥, $y_B = g^{x_B} \bmod p$.

x_p: 原始签名者 A_i 和代理签名者 B 共同生成的代理私钥(i= 1, , , n). y_p: 与 x_p 相对应的代理公钥, $y_p = g^{x_p} \bmod p$.

Sig(x, m): 基于离散对数的数字签名算法, 参数 x: 签名者私钥, 参数 m: 签名的消息, 签名返回值为 R.

Ver(y, R, m): 与签名算法 Sig 相对应的签名验证算法, 参数 y: 签名者公钥, 返回值为真或假.

Th: 使用安全哈希函数计算消息哈希值所用的时间.

Te: 计算一次求幂运算所用时间.

Tm: 计算一次乘积运算所用时间.

Tc: 验证公钥证书所用的时间.

Tv: 执行验证算法 Ver(y, R, m) 所用的时间.

3 文献[1]的方案

3.1 代理授权阶段

(1) 每个 A_i 完成的子代理授权过程(其中 i= 1, , , n):

¹ A_i 计算: $k_i \in_R Z_q^*$, $K_i = g^{k_i} \bmod p$, $e_i = h(m_w, K_i)$
$R_i = x_i e_i + k_i \bmod q$

º A_i 通过安全通道向 B 发送代理信息(R_i, K_i, m_w).

» B 验证(R_i, K_i, m_w)的有效性:

计算: $e_i = h(m_w, K_i)$. 验证等式: $g^{R_i} \stackrel{?}{=} y_i^{e_i} K_i \bmod p$.

如果等式成立, B 接受A_i 的代理授权, 否则, 拒绝 A_i 的代理授权.

收稿日期: 2003-12-24; 修回日期: 2004-09-04
基金项目: 国家 973 项目(No. G1999035804); 国家自然科学基金(No. 60372094, 90204017)

(2) 代理生成过程:

如果所有的(R_i, K_i, m_w) $(i = 1, \cdots, n)$ 都有效, B 计算 $x_p = \sum_{i=1}^{n} R_i \bmod q$, x_p 是 B 的代理私钥.

3.1.2　代理签名阶段

代理签名者 B 使用代理私钥 x_p 代表原始签名者 $A_1, \cdots, A_n$ 对消息 m 进行签名, $R_p = Sig(x_p, m)$, 其建立的代理多重签名为 $(m, R_p, K_1, \cdots, K_n, m_w)$.

3.1.3　代理签名验证阶段

验证者根据代理多重签名 $(m, R_p, K_1, \cdots, K_n, m_w)$ 进行以下操作:

计算: $e_i = h(m_w, K_i)$ $(i = 1, \cdots, n)$.

$$y_p = y_1^{e_1} \cdots y_n^{e_n} K_1 \cdots K_n \bmod p$$

验证等式: $Ver(y_p, R_p, m) \stackrel{?}{=} true$.

若等式成立, 则代理多重签名 $(m, R_p, K_1, \cdots, K_n, m_w)$ 有效, 否则无效.

3.1.4　方案的分析

(1) 安全性分析

结论 1　在这个方案中, 如果存在一个有效的代理多重签名 $(m, R_p, K_1, \cdots, K_n, m_w)$, 那么任何原始签名者 A_i 可以伪造任何消息 mc 的代理多重签名. 下面对这个结论进行证明:

假设 A_i 是伪造者, A_i 可以通过以下步骤伪造消息 mc 的代理多重签名:

① A_i 计算: $e_j = h(m_w, K_j)$ $(j = 1, \cdots, i-1, i+1, \cdots, n)$.

② A_i 随机选取 $A_i \in_R Z_q^*$ 并计算 $Kc_i = g^A (y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} y_{i+1}^{e_{i+1}} \cdots y_n^{e_n} K_1 \cdots K_{i-1} K_{i+1} \cdots K_n)^{-1} \bmod p$.

③ A_i 使用 $xc_p = A + x_i h(m_w, Kc_i) \bmod q$ 作为代理签名私钥生成消息 mc 的签名 $Rc_P = Sig(xc_P, mc)$, mc 的代理多重签名为 $(mc, Rc_P, K_1, \cdots, K_{i-1}, Kc_i, K_{i+1}, \cdots, K_n, m_w)$. $(mc, Rc_P, K_1, \cdots, K_{i-1}, Kc_i, K_{i+1}, \cdots, K_n, m_w)$ 是一个有效的代理多重签名, 这是因为: 验证者通过代理多重签名 $(mc, Rc_P, K_1, \cdots, K_{i-1}, Kc_i, K_{i+1}, \cdots, K_n, m_w)$ 计算 yc_p, 即

$$\begin{aligned} yc_p &= y_1^{e_1} \cdots y_n^{e_n} K_1 \cdots K_{i-1} Kc_i K_{i+1} \cdots K_n \bmod p \quad (\text{其中 } e_i = h(m_w, Kc_i)) \\ &= y_1^{e_1} \cdots y_n^{e_n} K_1 \cdots K_{i-1} g^A (y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} y_{i+1}^{e_{i+1}} \cdots y_n^{e_n} K_1 \cdots K_{i-1} K_{i+1} \cdots K_n)^{-1} * K_{i+1} \cdots K_n \bmod p \\ &= y_i^{e_i} g^A \bmod p = g^{A + x_i h(m_w, Kc_i)} \bmod p = g^{xc_P} \bmod p \end{aligned}$$

所以, $Ver(yc_p, Rc_p, mc) = true$.

也就是说, 任何一个原始签名者能伪造任何消息代理多重签名, 文献[1]的 Kim-like 代理多重签名方案是不安全的.

(2) 效率分析

① 代理多重签名长度

由于 $|R_P| = |p| + |q|$, 所以, 代理多重签名 $(m, R_P, K_1, \cdots, K_n, m_w)$ 的长度是 $|m| + (n+1) * |p| + |q| + |m_w|$, 它的长度与原始签名者的个数 n 有关.

② 验证代理多重签名效率

根据 3.1.3 代理验证阶段可知, 其验证计算时间量为 $n * Th + n * Tc + n * Te + (2n-1) * Tm + Tv$.

代理多重签名 $(m, R_p, K_1, \cdots, K_n, m_w)$ 的验证计算时间量与原始签名者的个数 n 有关.

4　改进方案

4.1.1　代理授权阶段

(1) 初始阶段: 在生成代理授权书 m_w 时原始签名者已经确定, 可以计算原始签名者公钥积 $Y = y_1, \cdots, y_n \bmod p$, 并把 Y 添加到 m_w 中, 把 m_w 发给所有 A_i $(i = 1, \cdots, n)$.

(2) 每个 A_i 完成的子代理授权过程 (其中 $i = 1, \cdots, n$):

① A_i 随机选择 $k_i \in_R Z_q^*$ 并计算 $K_i = g^{k_i} \bmod p$, 并把 K_i 发送给其他 A_j $(j = 1, \cdots, i-1, i+1, \cdots, n)$ 和代理签名者 B. ② A_i 计算 $K = \sum_{i=1}^{n} K_i \bmod p$ 和 $R_i = x_i h(m_w, K) + k_i K \bmod q$, 把 (R_i, K_i, m_w) 发送给 B. ③ B 首先计算 $K = \sum_{i=1}^{n} K_i \bmod p$.

然后, B 对收到每个 A_i 的 (R_i, K_i, m_w) 进行验证: 等式 $g^{R_i} \stackrel{?}{=} y_i^{h(m_w, K)} K_i^K \bmod p$ 是否成立, 如果等式成立, B 接受 A_i 的代理授权, 否则, 拒绝 A_i 的代理授权.

(3) 生成代理密钥

如果所有的 (R_i, K_i, m_w) $(i = 1, \cdots, n)$ 都有效, B 计算 $x_p = \sum_{i=1}^{n} R_i + x_B \bmod q$, x_p 是 B 的代理私钥.

4.1.2　代理签名阶段

(1) 代理签名者 B 检查消息 m 是否满足 m_w 的约定, 如果满足进入第二步, 否则拒绝签名.

(2) 代理签名者 B 使用代理私钥 x_p 代表原始签名者 $A_1, \cdots, A_n$ 对消息 m 进行签名 $R_P = Sig(x_P, m)$, 其建立的代理多重签名为 (m, R_P, K, m_w).

4.1.3　代理签名验证阶段

验证者对代理多重签名 (m, R_P, K, m_w) 做以下验证:

① 检查消息 m 是否满足 m_w 的约定, 如果满足进入第二步, 否则, 判定这个签名无效.

② 计算 $y_p = Y^{h(m_w, K)} K^K y_B \bmod p$, 其中 Y 是从 m_w 中得到.

③ 验证等式 $Ver(y_p, R_P, m) = true$ 是否成立.

若通过上面全部验证, 这个代理多重签名是有效的.

5　改进方案的分析

5.1.1　可验证性分析

定理 1　代理签名者 B 使用代理私钥 x_p 对消息 m 签名, 其签名为 (m, R_P, K, m_w), 验证者使用代理公钥 y_p 验证相应的签名, 那么 $y_p = g^{x_p} \bmod p$

证明　已知　$x_p = R_1 + \cdots + R_n + x_B \bmod q$

$$R_i = x_i h(m_w, K) + k_i K \bmod q \quad (i = 1, \cdots, n)$$

$$K = \sum_{i=1}^{n} K_i \bmod p \qquad y_B = g^{x_B} \bmod p$$

$$Y = y_1, \cdots, y_n \bmod p \qquad y_p = Y^{h(m_w, K)} K^K y_B \bmod p$$

所以 $g^{x_p} = g^{R_1 + \cdots + R_n + x_B} \bmod p$

$$= g^{h(m_w, K) \sum_{i=1}^{n} x_i + K \sum_{i=1}^{n} k_i + x_B} \bmod p$$

$$= g^{h(m_w, K) \sum_{i=1}^{n} x_i} g^{K \sum_{i=1}^{n} k_i} g^{x_B} \bmod p$$

$$= Y^{h(m_w,K)}K^{K}y_B \bmod p = y_p$$

所以, $y_p = g^{x_p} \bmod p$.

5.1.2 不可伪造性分析

在改进方案中, 首先证明任何原始签名者 A_i 不能伪造代理多重签名, 不失一般性, 假设 A_n 是伪造者.

(1) 由于 K_n 是由 A_n 生成的, A_n 根据已有代理多重签名 (m, R_p, K, m_w), 选择/ 适当0 的 K_n, 利用等式 $y_p = g^{x_p} \bmod p$ 求得 x_p.

由于 $K = \prod_{i=1}^{n} K_i \bmod p$, 设 $K_c = \prod_{i=1}^{n-1} K_i \bmod p$,

则 $K = K_c K_n \bmod p$. 那么

$$y_p = Y^{h(m_w,K)}K^{K}y_B \bmod p = (Y^{h(m_w,K)}y_B)(K_cK_n)^{KK_n} \bmod p$$

$$= (Y^{h(m_w,K)}y_B)(K_c^{K_c})^{K_n}(K_n^{K_n})^{K_c} = g^{x_p} \bmod p$$

根据上式, 无论 K_n 怎样取值, 求 x_p 都是离散对数问题.

(2) A_n 利用重新注册 y_n 伪造代理多重签名 (m, R_p, m_w, K).

$$y_p = Y^{h(m_w,K)}K^{K}y_B \bmod p = (y_1, y_n)^{h(m_w,K)}K^{K}y_B \bmod p$$

$$= (y_1, y_{n-1})^{h(m_w,K)}y_n^{h(m_w,K)}K^{K}y_B \bmod p = g^{x_p} \bmod p$$

只有 $K^{K}y_B \bmod p = 1$, A_n 通过设置 $y_n = g^{A}(y_1, y_{n-1})^{-1} \bmod p$ (其中 $A \in_R Z_q^*$) 可得 $x_P = A - h(m_w, K)$, 否则求 x_p 同样是离散对数问题. 但 $K^{K}y_B = 1$ 的概率是 $1/p$, 而 p 是保证安全的大素数, 所以 A_n 通过重新注册 y_n 伪造代理多重签名是不现实的.

(3) 综合(1) 和(2) 的证明方法, 可得出结论: A_n 即使结合选择适当的 K_n 和重新注册 y_n 两种手段也不能得到 x_p.

同理可证, 原始签名者中任何几个人合谋也无法伪造代理多重签名 (m, R_p, K, m_w). 在改进方案中生成的代理私钥 x_P 包含代理签名者 B 的私钥 x_B, 所以, 即使所有原始签名者联合也无法生成有效的多重代理签名, 那么除原始签名者之外的人更不可能伪造代理多重签名, 也就是说, 任何人都无法伪造改进方案的代理多重签名.

5.1.3 强代理性

在改进方案中, 生成的代理私钥 x_P 包含代理签名者 B 的私钥, 验证代理签名使用 B 的公钥 y_B, 签名中明确代理签名者身份, 根据 5.2 可知, 任何人都无法伪造改进方案的代理多重签名, 代理签名者 B 不能否认他的代理多重签名, 所以, 改进方案具有强代理性.

5.1.4 效率对比

根据计算时间量和签名长度, 用表格形式定量对比和分析改进方案和文献[1] 方案的效率.

表 1 改进方案与文献[1] 方案的效率对比表

	改进方案	文献[1] 的方案
代理密钥生成阶段	A_i: $(n+1)Tm + Te + Th$ B 验证: $n^*(3Te + Tm + Tc) + Th + (n-1)Tm$	A_i: $Te + Tm + Th$ B 验证: $n^*(2Te + Th + Tm + Tc)$
验证签名	$Th + 2Te + 2Tm + Tc + Tv$	$n^*(Th + Te + Tc) + (2n-1)Tm + Tv$
签名长度	$\lvert m\rvert + 2^*\lvert p\rvert + \lvert q\rvert + \lvert m_w\rvert$	$\lvert m\rvert + (n+1)\lvert p\rvert + \lvert q\rvert + \lvert m_w\rvert$

注: 计算量中模加、减运算所用时间忽略不计, 因为它们运算时间远远低于求幂、乘积、hash 求值等运算所需时间.

根据表 1 分析可知, 在代理密钥生成阶段, 改进方案的计算时间量与文献[1] 方案计算时间量之差为 $n^*Te + (n^2 + n - 1)^*Tm - (n-1)Th$, 一般而言, $Te > Th$, 所以改进方案的计算时间量高于文献[1] 方案, 但生成一个代理密钥, 由它能产生许多代理签名, 验证代理签名的次数更多, 改进方案的每次签名验证计算计算量比文献[1] 方案低 $(n-2)Te + (n-1)(Th + Tc) + (2n-3)Tm$, 代理签名的长度少了 $(n-1)^*\lvert p\rvert$, 改进方案的签名验证效率和签名的长度与原始签名者个数无关, 所以, 改进方案的效率更高, 更具有实用价值.

6 结论

改进的代理多重签名方案克服了文献[1] 的 Kim2like 代理多重签名方案存在的安全问题, 并具有强代理的特点, 而且固定长度的代理多重签名和可控的代理签名验证时间对于实际应用具有很高的价值.

参考文献:

[1] Y Li, G Bai, G Xiao. Proxy multi2signature scheme: a new type of proxy signature schemes[J]. Electronics Letters, 2000, 36(6): 527- 528.

[2] B Lee, H Kim, K Kim. Secure mobile agent using strong nondesignated proxy signature[A]. Proc of ACISP[C]. LNCS 2119, Springer2Verlag, 2001. 474- 486.

[3] H Sun, B Hsieh. On the Security of Some Proxy Signature Schemes [OL]. 2003, http://venona.antioffline.com/2003/068.pdf.

[4] B Lee, H Kim, K Kim. Strong Proxy Signature and Its Applications [A]. International Conference on Information and Communication Security, Proc of SCIS 2001[C]. 603- 608.

[5] S Kim, S Park, D Won. Proxy Signature Revisited[A]. International Conference on Information and Communication Security, Proc of ICICS 97[C]. 1997. 223- 232.

[6] T Okamoto, K Ohta. A Digital Multisignature Scheme Based on the Fiat2Shamir Scheme[A]. Advances in Cryptology2Proceedings of ASIACRYPT. 91[C]. Springer2Verlag, 1991. 139- 148.

[7] 杨义先, 等著. 现代密码新理论[M]. 北京: 科学出版社, 2002. 134- 137.

[8] 祁明, L Harn. 基于离散对数的若干新型代理签名方案[J]. 电子学报, 2000, 28(11): 114- 115.

[9] 王晓明, 符方伟. 一种代理多重数字签名方案的安全性分析[J]. 通信学报, 2002, 23(4): 98- 102.

作者简介:

谷利泽 男, 1965 年出生于辽宁省营口, 现为北京邮电大学博士研究生, 主要研究方向为现代密码学、电子商务和网络安全. E2mail: glz_bupt@263.net.

高 宏 男, 1972 年出生于陕西省西安, 北京邮电大学博士, 现于英特尔(中国) 有限公司工作, 主要研究方向为移动通信业务及其安全.

杨义先 男, 1961 年出生于四川省绵阳, 北京邮电大学教授、博士生导师、长江学者奖励计划特聘教授、香港中文大学信息工程系访问教授, 研究方向为信息安全及电子商务.