计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(3):217−220 [doi: 10.15888/j.cnki.csa.006240]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

对前向安全代理盲签名方案的分析与改进①

廖小平

(四川文理学院 智能制造学院, 达州 635000)
(达州智能制造产业技术研究院, 达州 635000)
通讯作者: 廖小平, E-mail: wuzhechangjiang@126.com

摘　要: 周萍等人提出了一个前向安全代理盲签名方案, 对该方案进行分析, 指出该方案存在信息拥有者可以否认签名的问题, 即信息拥有者否认用于签名的信息是自己提供的, 该信息可能是伪造的. 并在此基础上提出了改进的方案. 实验表明改进的方案不仅具有原方案的优良特性, 还解决了信息拥有者否认签名的问题.

关键词: 数字签名; 前向安全; 代理签名; 盲签名

引用格式: 廖小平.对前向安全代理盲签名方案的分析与改进.计算机系统应用,2018,27(3):217–220. http://www.c-s-a.org.cn/1003-3254/6240.html

Analysis and Improvement of Forward Secure Proxy Blind Signature Scheme

LIAO Xiao-Ping

(School of Intelligent Manufacturing, Sichuan University of Arts and Science, Dazhou 635000, China)
(Institute of Dazhou Intelligent Manufacturing Technology, Dazhou 635000, China)

Abstract: Professor Zhou Ping, *et al*. has proposed a scheme of forward secure proxy blind signature. This study analyzes the scheme, and points out the problems that information owners can deny the signature scheme. That is, the owner denies that the signature information is provided by themselves, which may be fake. The improvement is put forward based on the above analysis. The experiment shows that the improved scheme not only keeps the excellent qualities of the original plan, but also solves the problem of the information owner's denial of signature.

Key words: digital signature; forward security security; proxy signature; blind signature

数字签名的概念首先由 Diffie 和 Hellman[1]提出, 可用于合同、证书文件等的证明, 也可作为复杂安全协议的组成部分. 随着研究的深入, 许多具有特殊性质的数字签名方案相继被提出, 如盲签名[2]、代理签名[3], 或两种技术相结合的代理盲签名方案, 所有的数字签名方案中都需要安全地保存签名密钥, 因为一旦签名密钥泄露, 由这个签名密钥所签署的所有签名都将变得无效, 为了解决这个问题, 前向安全[4]技术被提出, 前向安全技术在很大程度上解决了因签名密钥泄露而带来的严重危害, 如在文献[5,6]中分别给出了安全的方案. 肖红光等人提出首个前向安全代理盲签名方案[7], 但该方案的前向安全性仅限于代理私钥, 而签名并不具备前向安全性, 文献[8]进一步指出该方案不能抵抗原始签名人的伪造攻击, 同时通过对代理授权方式和盲签名过程的改进提出了一个新的方案. 张席等提出了一种新的前向安全代理盲签名方案[9], 但该方案不能抵抗伪造攻击, 不具备不可伪造性. Manoj 等设计了一个前向安全的代理盲签名方案[10], 文献[11]中发现该方案在代理授权和代理盲签名阶段均存在伪造攻击, 并基于离散对数给出了改进的前向安全代理盲签名方案, 改进后方案的特点是在代理授权阶段将单向散列函数嵌入到签名中, 并对签名阶段进行了改进. 周萍等人基于二次剩余难题, 提出两种前向安全的代理盲签名方案[12], 随后在其博士论文中[13]对其进行了改进, 经分析

① 基金项目: 国家档案局科技项目计划项目 (2014-X-65); 四川省教育厅重点资助科研项目 (16ZA0353); 四川文理学院项目 (2016KZ008Y, 2015GJ011Z)
收稿时间: 2017-06-12; 修改时间: 2017-06-27; 采用时间: 2017-07-08; csa 在线出版时间: 2018-02-09

发现无论是原方案还是改进后的方案, 都存在信息拥有者对信息进行否认的问题, 因为整个方案中没有信息拥有者的私钥信息, 信息拥有者可以否认签名所用的信息是自己提供的, 针对周萍等人方案 (以下简称 ZP 方案) 存在的安全问题, 本文提出一种改进方案, 改进的方案中信息拥有者无法否认自己提供的信息, 信息拥有者参与了签名的过程, 改进的方案既保持了原方案的优点, 又能防止信息拥有者否认, 从而使方案具有更好的实用性.

1 ZP 方案

ZP 方案回顾, 方案的参与者包括: 原始签名者 A, 代理签名者 B、信息拥有者 C, m_w 是授权证书, 内容包含 A 和 B 的身份、授权代理签名的权限、范围和代理签名有效期等信息, 将有效周期划分为 T 个时间段.

1.1 系统参数

选择一个 q 阶的元 $g \in Q_n$, 其中 Q_n 是 Z_n^* 中所有模 n 平方剩余数构成的乘法子群. A 任意选取三个大素数 q, q_1, q_2, 并且计算出 $p_1 = 2qq_1 + 1$, $p_2 = 2qq_2 + 1$, $n_1 = p_1p_2$, 并将 n_1 通过安全信道发送给 B. B 也任意选取两个大素数 p_3 和 p_4, 并且计算 $n_2 = p_3p_4$, $n = n_1n_2$, 并且将 n_2 和 n 通过安全信道发送给 A. 选择两个抗强碰撞安全单向哈希函数:

$$H_1 : Z_n^* \times \{0,1\}^* \to Z_q^*$$
$$H_2 : Z_{T+1}^* \times Z_n^* \times \{0,1\}^* \times \{0,1\}^* \to Z_q^*$$

原始签名者 A 任意选择一个 x_A 作为自己的私钥, $x_A \in_R Z_q^*$, 计算出公钥 $y_A = g^{x_A} \bmod n$, $y_A \in Z_n^*$.

代理签名者 B 任意选择一个 x_B 作为自己的初始私钥, $x_{B_0} \in Z_n^q$, 计算出公钥 $y_B = x_{B_0}^{2^{T+1}} \bmod n$, $y_B \in Z_n^*$, 其中 T 为代理签名者 B 签名密钥有效期内划分的时间段数. 再选择公私钥对 (x'_B, y'_B), 且 $x'_B \in Z_q^*$, $y'_B = g^{x'_B} \bmod n$, $y'_B \in Z_n^*$, 然后 B 将 y_B 和 y'_B 发送给原始签名者 A.

信息拥有者 C 任意选择一个 x_C 作为自己的私钥, $x_C \in_R Z_q^*$, 计算出公钥 $y_C = g^{x_C} \bmod n$, $y_C \in Z_n^*$.

原始签名者 A 公开系统的参数 $\{H_1, H_2, n, g, y_A, y_B, y'_B, T\}$ 并且 A 和 B 删除 $\{q, q_1, q_2, p_3, p_4, n_1, n_2\}$.

1.2 代理授权

(1) 原始签名者 A 任意选取 k_A, $k_A \in_R Z_q^*$, 计算: $r_A = g^{k_A} \bmod n$, $h = H_1(r_A, m_w)$, $\sigma' = hx_A + k_A \pmod q$, 然后将 (r_A, σ', m_w) 通过秘密信道发送给代理签名者 B.

(2) 代理签名者 B 收到原始签名者 A 发送来的 (r_A, σ', m_w) 后, 验证等式 $g^{\sigma'} = y_A^{H_1(r_A, m_w)} r_A \pmod n$ 是否成立, 如果不成立, 要求原始签名者 A 重新发送授权信息, 或者代理签名者 B 停止代理, 如果成立, 则接受原始签名者 A 发送的代理授权信息 (r_A, σ', m_w), 并且计算 $\sigma = \sigma' + x'_B \pmod q$.

1.3 更新代理密钥

在 $i (1 \le i \le T)$ 时段即将开始时, 代理签名者 B 利用 $i-1$ 时段的私钥 $x_{B_{i-1}}$ 通过密钥更新算法 $x_{B_i} = x_{B_{i-1}}^2 \pmod q$ 计算得到第 i 时段的私钥, 然后将 $i-1$ 时段的私钥 $x_{B_{i-1}}$ 安全的删除, 则代理签名者 B 在第 $i (1 \le i \le T)$ 时段的签名密钥为 (x_{B_i}, σ).

1.4 代理盲签名生成

设 C 拥有信息 m, 需要 B 代表 A 对 m 进行签名, A, B, C 三者共同通过以下步骤完成对 m 的代理盲签名.

(1) 代理签名者 B 任意选择两个数 $k_B, u \in_R Z_q^*$, 并且计算: $r_B = g^{k_B} \bmod n$, $w = x_{B_i} g^u \bmod n$, 然后将 (r_A, r_B, w, m_w) 通过秘密信道发送给信息拥有者 C.

(2) 信息拥有者 C 任意选择三个随机数 $\alpha, \beta, \lambda \in_R Z_q^*$, 秘密保存, 并且计算: $h = H_1(r_A, m_w)$, $r_c = r_B g^{\alpha \cdot 2^{T+1-i}} \left(y_A^h r_A y'_B\right)^\beta \pmod n$, $W = wg^\lambda \pmod n$, 若 $r_C = 0$, 则 C 必须从新选择 α, β, λ 直到 $r_C \ne 0$ 为止. 计算: $e = H_2(r_C, W, m_w, m, i)$, $e' = e - \beta \pmod q$, 并且将 e' 通过安全信道发送代理签名者 B.

(3) 代理签名者 B 收到 e' 后, 计算: $s' = 2^{T+1-i} \cdot u \cdot r_A + k_B - e'\sigma \pmod q$, 则 s' 就是代理签名者 B 对信息 m 的盲签名, 将 s' 通过安全信道秘密发送给信息拥有者 C.

(4) 信息拥有者 C 收到 s' 后, 计算: $s = s' + \alpha \cdot 2^{T+1-i} + \lambda \cdot 2^{T+1-i} \cdot r_A \pmod q$, 最后得到代理签名者 B 对信息 m 的盲签名是: (s, W, e, r_A, m_w, i).

1.5 验证签名

任何人都可以验证盲签名 (s, W, e, r_A, m_w, i) 的有效性, 验证过程如下:

(1) 验证人首先根据授权信息 m_w 检查签名授权信息是否正确, 如 m 是否在授权签名信息的有效范围内、代理签名权是否过期、代理权限是否在有效范围内等, 如果签名授权信息 m_w 不正确, 则否认签名.

(2) 在验证授权信息 m_w 正确后, 计算: $h = H_1(m_w, r_A)$, $R = \left(W^{-2^{T+1-i}} \cdot y_B\right)^{r_A} \left(y_A^h \cdot r_A \cdot y'_B\right)^e g^s \pmod n$, $e' = H_2(R, W, m_w, m, i)$, 然后比较等式 $e' = e$ 是否成立. 如

果成立, 则(s,W,e,r_A,m_w,i)是信息 m 的有效代理盲签名.

2 ZP 方案安全性分析

对 ZP 方案的正确性、强盲性、前向安全性以及代理签名安全性的分析请参见文献[10], 此处只对不可否认性从三个方面进行分析.

(1) 原始签名人不能否认自己对代理签名人的授权, 即不能否认自己的签名授权, 在代理授权阶段, $\sigma' = hx_A + k_A \pmod q$中包含了原始签名者 A 的私钥 x_A, 并且在验证过程中用到了原始签名者 A 的公钥, 所以原始签名者 A 无法否认自己的签名授权.

(2) 代理签名人不能否认自己的代理签名, 即代理签名人不能对自己的代理签名进行否认, 在代理盲签名生成阶段, $w = x_{B_i} g^u \bmod n$ 和$s' = 2^{T+1-i} \cdot u \cdot r_A + k_B - e'\sigma \pmod q$中包含了代理签名者 B 的签名密钥为$\left(x_{B_i}, \sigma\right)$, 并且在验证的过程中用到了代理签名者 B 的公钥, 所以, 代理签名人不能对自己的代理签名进行否认.

(3) 信息拥有者 C 能对签名进行否认, 即信息拥有者 C 否认提供信息 m 用于签名, 因为在整个签名过程中没有用到信息拥有者 C 的私钥.

通过分析发现, ZP 方案中原始签名者无法否认自己的签名授权, 代理签名人不能对自己的代理签名进行否认, 但信息拥有者可以对签名的信息进行否认, 否认自己提供过信息 m 用于签名.

3 ZP 方案的改进

针对 ZP 方案中存在的安全问题, 提出一种改进方案, 改进方案中的系统参数、代理授权、更新代理密钥与原方案相同.

3.1 代理盲签名生成

A, B, C 三者共同通过以下步骤完成对 m 的代理盲签名.

(1) 代理签名者 B 任意选择两个数$k_B \in_R Z_q^*$, $u \in_R Z_q^*$, 并且计算: $r_B = g^{k_B} \bmod n$, $w = x_{B_i} g^u \bmod n$, 然后将(r_A, r_B, w, m_w)通过秘密信道发送给信息拥有者 C.

(2) 信息拥有者 C 任意选择三个随机数$\alpha,\beta,\lambda \in_R Z_q^*$, 秘密保存, 并且计算: $h = H_1(r_A, m_w)$, $r_c = r_B g^{\alpha \cdot 2^{T+1-i}} \left(y_A^h r_A y_B'\right)^{x_C \beta} \pmod n$, $W = w g^{\lambda} \pmod n$, 若$r_C = 0$, 则 C 必须从新选择 α, β, λ 直到 $r_C \neq 0$ 为止. 计算: $e = H_2(r_C, W, m_w, m, i)$, $e' = e - x_C \beta \pmod q$, 并且将 e'通过安全信道发送代理签名者 B.

(3) 代理签名者 B 收到 e'后, 计算: $s' = 2^{T+1-i} \cdot u \cdot r_A + k_B - e'\sigma \pmod q$, 则 s'就是代理签名者 B 对信息 m 的盲签名, 将 s'通过安全信道秘密发送给信息拥有者 C.

(4) 信息拥有者 C 收到 s'后, 计算: $s = s' + \alpha \cdot 2^{T+1-i} + \lambda \cdot 2^{T+1-i} \cdot r_A \pmod q$, 最后得到代理签名者 B 对信息 m 的盲签名是: (s, W, e, r_A, m_w, i).

4 改进方案的安全性分析

新方案的强盲性、前向安全性以及代理签名安全性的分析请参见文献[10], 此处只对正确性和信息拥有者 C 的不可否认性进行分析.

4.1 正确性分析

证明: 因为:

$$x_{B_i} = x_{B_{i-1}}^2 \pmod q = x_{B_{i-2}}^{2^2} \pmod q$$
$$= x_{B_{i-3}}^{2^3} \pmod q = \cdots = x_{B_0}^{2^i} \pmod q$$

所以:

$$x_{B_i}^{2^{T+1-i}} \pmod q = x_{B_0}^{2^{T+1}} \pmod q$$
$$y_B = x_{B_0}^{2^{T+1}} = x_{B_i}^{2^{T+1-i}} \bmod n$$

代理签名者 B 收到原始签名者 A 发送来的(r_A, σ', m_w)后, 验证等式$g^{\sigma'} = y_A^{H_1(r_A, m_w)} r_A \pmod n$是否成立, 由:

$$g^{\sigma'} = g^{hx_A + k_A} = g^{hx_A} \cdot g^{k_A} = y_A^h \cdot r_A = y_A^{H_1(r_A, m_w)} r_A \pmod n$$

所以等式成立.

$$g^{\sigma} = g^{\sigma' + x_B'} = g^{\sigma'} \cdot g^{x_B'} = y_A^h \cdot r_A \cdot y_B' \pmod n$$

由签名过程知:

$$\begin{aligned} s &= s' + \alpha \cdot 2^{T+1-i} + \eta \cdot 2^{T+1-i} \cdot r_A \pmod q \\ &= 2^{T+1-i} \cdot u \cdot r_A + k_B - e'\sigma + \alpha \cdot 2^{T+1-i} + \eta \cdot 2^{T+1-i} \cdot r_A \pmod q \\ &= 2^{T+1-i} \cdot u \cdot r_A + k_B - (e - x_C\beta)\sigma + \alpha \cdot 2^{T+1-i} + \eta \cdot 2^{T+1-i} \cdot r_A \pmod q \\ &= 2^{T+1-i} \cdot u \cdot r_A + k_B - e\sigma + x_C\beta\sigma + \alpha \cdot 2^{T+1-i} + \eta \cdot 2^{T+1-i} \cdot r_A \pmod q \\ &= 2^{T+1-i} \cdot u \cdot r_A + k_B + \alpha \cdot 2^{T+1-i} + x_C\beta\sigma - e\sigma + \eta \cdot 2^{T+1-i} \cdot r_A \pmod q \end{aligned}$$

又因为:

$$\begin{aligned} r_c &= r_B g^{\alpha\cdot 2^{T+1-i}}\left(y_A^h r_A y_B'\right)^{x_C\beta} (\mathrm{mod}\, n)\\ &= g^{k_B+\alpha\cdot 2^{T+1-i}}\cdot g^{x_C\beta\sigma} (\mathrm{mod}\, n)\\ &= g^{k_B+\alpha\cdot 2^{T+1-i}+x_C\beta\sigma} (\mathrm{mod}\, n) \end{aligned}$$

所以:

$$\begin{aligned} g^s &= g^{2^{T+1-i}\cdot u\cdot r_A+k_B+\alpha\cdot 2^{T+1-i}+x_C\beta\sigma-e\sigma+\eta\cdot 2^{T+1-i}\cdot r_A} (\mathrm{mod}\, n)\\ &= g^{2^{T+1-i}\cdot u\cdot r_A+\eta\cdot 2^{T+1-i}\cdot r_A}\cdot g^{-e\sigma}\cdot g^{k_B+\alpha\cdot 2^{T+1-i}+x_C\beta\sigma} (\mathrm{mod}\, n)\\ &= g^{(u+\eta)2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n)\\ &= (g^u\cdot g^\eta)^{2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n)\\ &= \left(w x_{B_i}^{-1}\cdot g^\eta\right)^{2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n)\\ &= \left(W x_{B_i}^{-1}\right)^{2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n) \end{aligned}$$

即得到:

$$g^s = \left(W x_{B_i}^{-1}\right)^{2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n)$$

根据式子求 r_C:

$$\begin{aligned} g^s x_{B_i}^{2^{T+1-i}\cdot r_A} &= (W)^{2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n)\\ g^s\left(x_{B_i}^{2^{T+1-i}}\right)^{r_A} &= (W)^{2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n)\\ g^s y_B^{r_A} &= (W)^{2^{T+1-i}\cdot r_A}\cdot (g^\sigma)^{-e}\cdot r_C (\mathrm{mod}\, n) \end{aligned}$$

所以:

$$\begin{aligned} r_C &= g^s y_B^{r_A}\left(W^{-2^{T+1-i}}\right)^{r_A}\cdot (g^\sigma)^e (\mathrm{mod}\, n)\\ &= \left(W^{-2^{T+1-i}} y_B\right)^{r_A} g^s\cdot\left(y_A^h\cdot r_A\cdot y_B'\right)^e (\mathrm{mod}\, n) \end{aligned}$$

即可得到: $e' = e$成立, 所以该签名方案是正确的.

4.2 信息拥有者 C 的不可否认性分析

在签名形成过程中, 信息拥有者 C 任意选择三个随机数 $\alpha,\beta,\eta\in_R Z_q^*$ 对信息 m 进行盲化, 由 $r_c = r_B g^{\alpha\cdot 2^{T+1-i}}\left(y_A^h r_A y_B'\right)^{x_C\beta} (\mathrm{mod}\, n)$ 和 $e' = e - x_C\beta (\mathrm{mod}\, q)$ 知道签名中包含了信息拥有者 C 的私钥 x_C, 所以, 代理签名人无法否认自己的签名, 信息拥有者也无法否认信息被签名.

5 结束语

文章分析了 ZP 等人提出的前向安全代理盲签名方案, 并给出了改进方案, 经安全分析表明, 改进后的方案不仅保留了原方案的优点, 而且解决了信息拥有者可以对信息进行否认的问题, 可实现特殊应用领域的要求, 应用领域较广.

参考文献

1 Diffie W, Hellman ME. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644–654. [doi: 10.1109/TIT.1976.1055638]

2 Chaum D. Blind signatures for untraceable payments. In: Chaum D, Rivest RL, Sherman AT, eds. Advances in Cryptology. New York. Plenum Press. 1983. 199–233.

3 Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. Proceedings of the 3rd ACM Conference on Computer and Communications Security. New Delhi, India. 1996. 48–57.

4 Anderson R. Two remarks on public key cryptology. Invited Lecture, 4th Annual Conference on Computer and Communications Security. New York, NY, USA. 1997.

5 李运发, 邹德清, 韩宗芬, 等. 基于前向安全的组签名体制研究. 计算机研究与发展, 2006, 43(12): 2069–2075.

6 曹正军, 刘丽华. 两个指定验证人签名方案的安全性分析. 软件学报, 2008, 19(7): 1753–1757.

7 肖红光, 谭作文, 王键. 一种前向安全的代理盲签名方案. 通信技术, 2009, 42(5): 193–196.

8 何滨, 杜伟章. 前向安全代理盲签名方案的分析及改进. 计算机工程与应用, 2015, 51(18): 104–108, 164. [doi: 10.3778/j.issn.1002-8331.1310-0066]

9 张席, 杭欢花. 前向安全的代理盲签名方案. 计算机工程与应用, 2010, 46(24): 101–103, 145. [doi: 10.3778/j.issn.1002-8331.2010.24.030]

10 Manoj KC, Balwant ST. An improved proxy blind signature scheme with forward security. International Journal of Computer Applications, 2014, 85(15): 1–4. [doi: 10.5120/14914-3321]

11 刘二根, 王霞. 前向安全代理盲签名方案的分析与改进. 华东交通大学学报, 2015, 32(6): 110–114.

12 周萍, 何大可. 两种具有前向安全性质的代理盲签名方案. 计算机工程与应用, 2012, 48(5): 51–53, 155.

13 周萍. 特殊数字签名体制的研究[博士学位论文]. 成都: 西南交通大学, 2013. 111–116.