论 文

对 Fu-Wang 代理签名方案的进一步改进

周才学^{①*}, 李发根^②^① 九江学院信息科学与技术学院, 九江 332005^② 电子科技大学计算机科学与工程学院, 成都 611731

* 通信作者. E-mail: charlesjjx@126.com

收稿日期: 2013-05-07; 接受日期: 2013-07-03; 网络出版日期: 2014-05-09

国家自然科学基金 (批准号: 61073176) 和九江学院校级重点课题 (批准号: 2013ZD02) 资助项目

摘要 代理签名可以让原始签名者把他的签名权委托给代理签名者, 然后代理签名者就可以代表原始签名者对消息签名. 本文重新给出了代理签名的形式化定义, 并定义了新的代理签名的安全模型. 然后本文指出 Fu-Wang 的代理签名方案存在原始签名者、代理签名者和第三方攻击者的伪造攻击, 进而本文使用在散列函数中绑定公钥的方法和在标准签名、代理授权和代理签名生成时在消息前附加不同的特殊数字串的方法, 给出了 Fu-Wang 方案的进一步改进, 并在新的安全模型下给出了改进方案的安全性证明, 对改进方案的效率也进行了分析. 结果表明, 改进方案是安全的和高效的.

关键词 代理签名 代理聚合签名 伪造攻击 双线性对 安全模型

1 引言

代理签名是 Mambo 等^[1]于 1996 年提出的概念, 当原始签名者因健康、资源限制或其他原因不能履行签名职责时, 便将签名权委托给代理签名人, 由代理签名人代替他进行签名. 代理签名在实际应用中具有广阔的应用前景, 比如网格计算^[2]、移动 Agent 应用^[3]等领域. 代理签名的概念自被提出后, 得到了业界的普遍关注. 人们在基本代理签名的基础上又扩展了这一概念, 提出了门限代理签名^[4]、多代理签名^[5]、代理多签名^[6]、多代理多签名^[7]、门限代理门限签名^[8]和混合代理多签名^[9]等. 这些扩展研究满足了代理签名在实际使用中的不同需求, 是对基本代理签名方案的很好补充. 人们还把代理签名与不同的密码体制相结合, 提出了基于身份的代理签名^[10]、无证书代理签名^[11]、基于证书的代理签名^[12]和自认证公钥代理签名^[13]等. 此外, 人们还把代理签名与其他特殊签名相结合, 提出了前向安全代理签名^[14]、盲代理签名^[15]、指定验证者代理签名^[16]等.

在代理签名的可证明安全方面, Boldyreva 等^[17]首先给出了代理签名的形式化定义和安全模型. 在他们的安全模型中, 攻击者的目标是冒充原始签名者或代理签名者伪造一个标准签名或代理签名. 随后, Herranz 等^[18]讨论了完全分布式的代理签名的安全模型, Malkin 等^[19]讨论了层次代理签名的安全模型. 2004 年, Wang 等^[20]指出文献^[17]的安全模型存在 2 个缺陷. 2008 年, Schuldt 等^[21]进一步给出了更强的安全模型, 他们指出, 以前的模型要求攻击者在注册公钥时要提供知道相应私钥的证明, 而他们的模型可以去掉这一限制. 于是系统就必须考虑攻击者的公钥替换攻击, 即攻击者可以

引用格式: 周才学, 李发根. 对 Fu-Wang 代理签名方案的进一步改进. 中国科学: 信息科学, 2014, 44: 857-870, doi: 10.1360/N112013-00052

特意构造一个公钥, 然后到 CA(certification authority) 去申请证书, 而相应的私钥未知. 在实际应用中, CA 出于效率或其他原因可能并不要求用户在申请公钥证书时提供知道相应私钥的证明, 这种公钥替换攻击对多签名也构成威胁^[22]. 除了以上一些安全模型外, 在代理签名的发展过程中, 人们还提出了基于身份的代理签名的安全模型^[23]、无证书代理签名的安全模型^[24]、代理多签名的安全模型^[25]等.

然而所有以前的安全模型都没有考虑这样一种情况. 在一个代理签名方案中, 原始签名者授权给代理签名者是通过授权信息 m_w 产生一个签名来实现的, 代理签名者在产生代理签名时也要用到一个签名算法, 而这 2 个签名算法可以不同, 我们称前一个为签名算法 1, 后一个为签名算法 2. 在以前的安全模型中, 如果攻击者伪造了一个签名算法 1 的标准签名, 则方案被攻破. 实际上如果攻击者能伪造一个签名算法 2 的标准签名, 则方案也应该被视为攻破. 如 Lee 等^[26] 攻击 Zhang^[4] 方案, 就是攻击者能伪造一个原始签名者的签名算法 2 的标准签名; 再如李发根等^[27] 攻击 Lu 等^[28] 的方案, 就是一个原始签名者伪造了代理签名者的签名算法 2 的标准签名. 综合以上情况, 本文给出了新的代理签名的形式化定义和安全模型.

2008 年, Lu 等^[28] 提出 2 个代理签名方案, 一个是基本代理签名方案, 另一个是代理聚合签名方案, 方案的效率较高, 但 2010 年李发根等^[27] 指出 Lu 等的方案是不安全的, 原始签名者可以从代理签名中获得代理签名者对签名消息的标准 BLS 签名^[29], 原始签名者也可以通过代理签名者的标准 BLS 签名, 伪造一个该消息的代理签名或代理聚合签名, 然而李发根等没有给出改进方案. 2012 年, Fu-Wang^[30] 针对李发根等的攻击方法给出了 Lu 等方案的改进方案. 本文指出, Fu-Wang 的改进方案仍然不安全, 原始签名者、代理签名者和第三方攻击者都可以伪造代理签名. 然后, 本文给出 Fu-Wang 方案的进一步改进, 并在新的安全模型下给出了改进方案的安全性证明, 对效率也进行了分析. 结果表明, 改进方案是安全的和高效的.

2 一些基本概念

双线性对: $(G_1, +)$ 和 $(G_2, \times)$ 是 2 个具有相同素数阶 q 的循环群, $e: G_1 \times G_1 \rightarrow G_2$ 是一个可计算的双线性映射, 满足以下一些性质:

1. 双线性性: 对任意 $aP, bP \in G_1$, $e(aP, bP) = e(P, P)^{ab}$;
2. 非退化性: 存在 $P, Q \in G_1$, 满足 $e(P, Q) \neq 1_{G_2}$;
3. 可计算性: 对任意 $P, Q \in G_1$, 存在一个有效的算法计算 $e(P, Q)$.

离散对数 (discrete logarithm, DL) 问题: 给定 2 个群元素 P 和 Q , 找到一个正整数 $a \in \mathbb{Z}_q^*$, 使得 $Q = aP$ 成立.

计算 Diffie-Hellman (computational Diffie-Hellman, CDH) 问题: 给定 $P, aP, bP \in G_1, a, b \in \mathbb{Z}_q^*$, a, b 的值未知, 要求计算 $abP \in G_1$.

3 代理签名的形式化定义和安全模型

3.1 代理签名的形式化定义

一个代理签名方案由以下 9 个算法构成:

G : 初始化算法. 输入安全参数 1^k , 产生系统参数和用户的公私钥对, 原始签名者和代理签名者的公私钥对分别为 $(pk_o, sk_o), (pk_p, sk_p)$.

S_1 : 标准签名算法 1. 输入消息 m 和签名者的私钥 sk , 产生一个签名 σ_1 .

S_2 : 标准签名算法 2. 输入消息 m 和签名者的私钥 sk , 产生一个签名 σ_2 .

V_1 : 标准签名验证算法 1. 输入 (pk, σ_1) , 输出 0 或 1. 若输出是 1, 则称 σ_1 是一个关于 (pk, m) 的正确签名.

V_2 : 标准签名验证算法 2. 输入 (pk, σ_2) , 输出 0 或 1. 若输出是 1, 则称 σ_2 是一个关于 (pk, m) 的正确签名.

D : 授权算法. 原始签名者用它来签署一个授权 w , w 包含授权信息的类型, 原始签名者和代理签名者的身份及公钥和代理的有效期限等信息. 原始签名者用算法 S_1 产生一个签名 (w, cert) 并把它传给代理签名者.

P : 代理密钥产生算法. 代理签名者用原始签名者的公钥 pk_o 验证 (w, cert) 的正确性, 如果正确则接受该授权并用自己的私钥 sk_p 和该授权产生一个代理签名私钥 sk_p .

PS: 代理签名产生算法. 输入代理签名私钥 sk_p 、授权 w 和消息 $m \in \{0, 1\}^*$, 代理签名者用算法 S_2 产生一个代理签名 $p\sigma$.

PV: 代理签名验证算法. 输入 $(pk_o, pk_p, w, m, p\sigma)$, 输出 0 或 1. 如果输出是 1, 则称 $p\sigma$ 是一个关于消息 m 的正确的代理签名, 其中原始签名者为 pk_o , 代理签名者为 pk_p .

以上算法要求 $\Pr[V_1(pk, m, S_1(sk, m)) = \text{accept}] = 1$, $\Pr[V_2(pk, m, S_2(sk, m)) = \text{accept}] = 1$, $\Pr[PV(pk_o, pk_p, w, m, PS(sk_p, w, m)) = \text{accept}] = 1$.

3.2 安全模型

系统中有多个参与人, 攻击者可能和某些原始签名者或代理签名者合谋. 考虑一种极端的情况, 系统只有一个诚实的用户, 比方叫用户 1. 考虑最强的攻击者, 即用户 $i \in \{2, 3, \dots, n\}$, 他可以充当原始签名者或代理签名者与用户 1 执行代理授权协议, 系统允许用户 1 进行自代理, 并且原始签名者和代理签名者之间不需要安全信道. 攻击者可以访问标准签名预言机和代理签名预言机. 考虑适应性选择消息攻击和适应性选择授权攻击, 攻击者的目标是冒充原始签名者或代理签名者伪造一个标准签名或代理签名.

定义 1 代理签名的安全性. 在适应性选择消息和适应性选择授权攻击下, 如果一个存在性伪造是计算上不可行的, 则称一个代理签名方案是安全的.

具体的安全模型定义如下, 攻击者的优势定义为他在以下游戏中获胜的概率:

1. 首先, 输入 1^k , 挑战者 C 运行算法 G , 产生系统参数和用户 1 的公私钥对 (pk_1, sk_1) , 保密 sk_1 .
2. C 把公钥 pk_1 给攻击者 A , A 能访问 3 个签名预言机, 即标准签名预言机 $O_{s1}(sk_1, \cdot)$, $O_{s2}(sk_1, \cdot)$ 和代理签名预言机 $O_{ps}(sk_p, \cdot)$.
3. 除了挑战公钥 pk_1 外, A 能选择所有其他公钥, 即 A 可以注册所有公钥 $(pk_2, \dots, pk_n)$. 注册公钥时, 可以不用知道相应的私钥.
4. 用户 $j \in \{2, 3, \dots, n\}$ 授权用户 1. 用户 j 产生一个授权 (w, cert) , C 验证其正确性后接受该授权并把 (w, cert) 加入到表 Warrp 中.
5. 用户 1 授权用户 $j \in \{2, 3, \dots, n\}$. 输入为 w_i (可以由 A 选择), C 用 sk_1 运行算法 D 产生相应的代理授权签名 (w_i, cert_i) 返回给 A , C 把 w_i 加入到表 Warro 中.
6. 用户 1 授权用户 1 (用户 1 的自代理). 输入为 w_i (可以由 A 选择), C 运行算法 D 产生相应的代理授权签名 (w_i, cert_i) . C 把 (w_i, cert_i) 加入到表 Warrs 中.

7. 标准签名 1 询问. 输入为 m_i , C 用 sk_1 运行算法 S_1 产生相应的签名并返回给 A , C 把 m_i 加入到表 S_{1-qu} 中.

8. 标准签名 2 询问. 输入为 m_i , C 用 sk_1 运行算法 S_2 产生相应的签名并返回给 A , C 把 m_i 加入到表 S_{2-qu} 中.

9. 代理签名询问. 代理签名者为用户 1, 原始签名者为用户 $j \in \{1, 2, 3, \dots, n\}$ (包括自代理). 询问的输入为 (w_i, m_i) , 其中 $w_i \in \{Warrp \cup Warrs\}$, m_i 适合 w_i . C 运行算法 P 产生代理私钥 sk_{pi} , 再运行算法 PS 产生一个代理签名给 A , C 把 (w_i, m_i) 加入到表 PS_{qu} .

假如以下任一事件发生, 则攻击者 A 获胜:

E1: A 输出一个伪造 (m', σ) , 而 $V_1(pk_1, m', \sigma) = 1$, 且没有对 m' 作 $O_{s1}(sk_1, \cdot)$ 询问, 即 A 伪造了一个用户 1 的标准签名 1.

E2: A 输出一个伪造 (m', σ) , 而 $V_2(pk_1, m', \sigma) = 1$, 且没有对 m' 作 $O_{s2}(sk_1, \cdot)$ 询问, 即 A 伪造了一个用户 1 的标准签名 2.

E3: A 输出一个伪造 $(w', m', p\sigma)$, 而 $PV(pk_i, pk_1, w', m', p\sigma) = 1$ ($i \in \{1, 2, \dots, n\}$), $(w', m') \notin PS_{qu}$. 即 A 伪造了一个原始签名者为用户 i 代理签名者为用户 1 的代理签名, 包括自代理.

E4: A 输出一个伪造 $(w', m', p\sigma)$, 而 $PV(pk_1, pk_i, w', m', p\sigma) = 1$ ($i \in \{2, \dots, n\}$), $w' \notin Warro$. 即 A 伪造了一个原始签名者为用户 1 代理签名者为用户 i 的代理签名.

4 Fu-Wang 方案

4.1 基本代理签名方案

基本代理签名算法由 4 个部分组成:

系统初始化: 给定安全参数 k , 可信中心 TA 选择具有相同素数阶 q 的 2 个群 G_1 和 G_2 , 一个生成元 $P \in G_1$ 和一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$. 然后, TA 选择两个哈希函数 $H: \{0, 1\}^* \rightarrow G_1$, $H_1: \{0, 1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$. 最后, TA 公布 $\{G_1, G_2, e, q, P, H, H_1\}$ 作为系统参数.

原始签名者 A 随机选择 $x_a \in \mathbb{Z}_q^*$ 作为他的私钥, 公布 $P_a = x_a P$ 作为他的公钥. 同样, 代理签名者 B 随机选择 $x_b \in \mathbb{Z}_q^*$ 作为他的私钥, 公布 $P_b = x_b P$ 作为他的公钥.

代理产生: 原始签名者 A 将签名权委托给代理签名者 B , 过程如下:

1. 原始签名者 A 首先产生并公布代理授权 m_w , 该代理授权记录着对代理消息类型的限制, 代理的有效期等信息.

2. 然后, A 选择一个随机数 $k \in \mathbb{Z}_q^*$, 计算 $R = kP$, $s = k - x_a H_1(m_w, R) \bmod q$.

3. 最后, A 公布 R 并通过安全信道发送 s 给代理签名者 B .

4. B 收到 s 后, 验证以下等式是否成立: $R = sP + H_1(m_w, R)P_a$, 如果成立, B 接受 s , 否则拒绝.

5. 一旦 s 被接受, B 随机选择 $k_b \in \mathbb{Z}_q^*$, 如下计算代理私钥:

$$s_p = s - (x_b + k_b) \cdot H_1(m_w, R) \bmod q.$$

于是, 隐含的代理公钥为 $P_p = s_p \cdot P = R - H_1(m_w, R) \cdot (P_a + P_b + R_b)$, 其中 $R_b = k_b P$.

代理签名产生: 代理签名者 B 代表原始签名者 A 对消息 $m \in \{0, 1\}^*$ 进行签名, 步骤如下:

1. 计算 $H(m) \in G_1$.

2. 计算 $\sigma = s_p \cdot H(m)$. 即消息 m 的代理签名为 (m_w, m, R, R_b, σ) .

代理签名验证: 验证者收到 (m_w, m, R, R_b, σ) 后, 验证以下等式是否成立:

$$e(\sigma, P) = e(H(m), R - H_1(m_w, R) \cdot (P_a + P_b + R_b)).$$

如果成立, 接受代理签名, 否则拒绝.

4.2 代理聚合签名方案

代理聚合签名是给定由不同的 n 个用户产生的对 n 个不同消息的 n 个代理签名, 合成者可以把这 n 个代理签名聚合成一个代理签名, 验证者只要验证这个单个代理签名就可以确信这 n 个用户是否确实签署了 n 个原始的消息.

代理聚合签名算法也是由 4 个部分组成:

系统初始化: 参数生成过程同基本代理签名方案, 最后, TA 公布 $\{G_1, G_2, e, q, P, H, H_1\}$ 作为系统参数. 原始签名者 A 随机选择 $x_a \in \mathbb{Z}_q^*$ 作为他的私钥, 公布 $P_a = x_a P$ 作为他的公钥. 每个代理签名者 $B_i, 1 \leq i \leq n$ 随机选择 $x_{b_i} \in \mathbb{Z}_q^*$ 作为他的私钥, 公布 $P_{b_i} = x_{b_i} \cdot P$ 作为他的公钥.

代理产生: 原始签名者 A 把他的 n 个不同的签名权力委托给 n 个不同的代理签名者 $B_1, B_2, \dots, B_n$, A 执行以下步骤:

1. 原始签名者 A 首先产生并公布 n 个不同的代理授权 $m_{w_i}, 1 \leq i \leq n$, 每个代理授权 m_{w_i} 记录着对不同的代理消息类型的限制, 代理的有效期等信息.
2. 然后, A 选择 n 个随机数 $k_i \in \mathbb{Z}_q^*, 1 \leq i \leq n$, 计算 $R_i = k_i P, s_i = k_i - x_a H_1(m_{w_i}, R_i) \bmod q$.
3. 最后, A 公布所有的 $R_i, 1 \leq i \leq n$ 并通过安全信道发送 s_i 给代理签名者 B_i .
4. $B_i, 1 \leq i \leq n$ 收到 s_i 后, 验证以下等式是否成立: $R_i = s_i P + H_1(m_{w_i}, R_i) P_a$, 如果成立, B_i 接受 s_i , 否则拒绝.
5. 一旦 s_i 被接受, B_i 随机选择 $k_{b_i} \in \mathbb{Z}_q^*$, 然后如下计算代理私钥:

$$s_{p_i} = s_i - (x_{b_i} + k_{b_i}) \cdot H_1(m_{w_i}, R_i) \bmod q.$$

于是, 隐含的代理公钥为 $P_{p_i} = s_{p_i} \cdot P = R_i - H_1(m_{w_i}, R_i) \cdot (P_a + P_{b_i} + R_{b_i})$, 其中 $R_{b_i} = k_{b_i} \cdot P$.

代理聚合签名产生: 假设有一个消息 $m \in \{0, 1\}^*$ 要签名, 它由 n 个不同的子消息 $m_1, m_2, \dots, m_n$ 组成. 于是每个代理签名者 $B_i, 1 \leq i \leq n$ 在他的授权范围内用他的代理私钥签署一个相应的子消息 m_i , 步骤如下:

1. 首先, 每个代理签名者 $B_i, 1 \leq i \leq n$ 用他的代理私钥 s_{p_i} 对子消息 m_i 产生一个签名 $\sigma_i = s_{p_i} \cdot H(m_i)$.
2. 然后, 合成者把这 n 个不同的代理签名聚合成一个 $\sigma, \sigma = \sum_{i=1}^n \sigma_i$, 则消息 m 的代理聚合签名为 $(m_{w_1}, m_{w_2}, \dots, m_{w_n}, m_1, m_2, \dots, m_n, R_1, R_2, \dots, R_n, R_{b_1}, R_{b_2}, \dots, R_{b_n}, \sigma)$.

代理聚合签名验证: 验证者收到 $(m_{w_1}, m_{w_2}, \dots, m_{w_n}, m_1, m_2, \dots, m_n, R_1, R_2, \dots, R_n, R_{b_1}, R_{b_2}, \dots, R_{b_n}, \sigma)$ 后, 验证以下等式是否成立:

$$e(\sigma, P) = \prod_{i=1}^n e(H(m_i), R_i - H_1(m_{w_i}, R_i) \cdot (P_a + P_{b_i} + R_{b_i})).$$

如果成立, 接受代理签名, 否则拒绝.

5 Fu-Wang 方案的安全缺陷

对 Fu-Wang 基本代理签名方案的攻击:

攻击方法 1:

假设原始签名者 A 获得一个代理签名者 B 的标准 BLS 签名 $\sigma_b = x_b H(m)$, 则有 $e(\sigma_b, P) = e(H(m), P_b)$, 原始签名者的伪造攻击如下:

1. 原始签名者产生一个授权 m'_w , 使得 m 适合 m'_w .
2. 再任取随机数 $k, k_b \in \mathbb{Z}_q^*$, 计算 $R = kP, R_b = k_b P$.
3. 计算 $\sigma' = kH(m) - (x_a H(m) + \sigma_b + k_b H(m))H_1(m'_w, R)$. 则伪造的代理签名为 $(m'_w, m, R, R_b, \sigma')$.
4. 以上伪造的代理签名能通过验证, 验证如下:

$$e(\sigma', P) = e((kH(m) - (x_a H(m) + \sigma_b + k_b H(m))H_1(m'_w, R)), P) = e(H(m), R - H_1(m'_w, R) \cdot (P_a + P_b + R_b)).$$

这样 A 在不知道 B 的私钥的情况下, 伪造了 B 的代理签名, 损害了 B 的利益.

显然以上攻击方法也适合攻击 Fu-Wang 的代理聚合方案.

攻击方法 2:

假设代理签名者 B 获得一个原始签名者 A 的标准 BLS 签名 $\sigma_a = x_a H(m)$, 则有 $e(\sigma_a, P) = e(H(m), P_a)$, 代理签名者的伪造攻击如下:

1. 代理签名者产生一个授权 m'_w , 使得 m 适合 m'_w .
2. 再任取随机数 $k, k_b \in \mathbb{Z}_q^*$, 计算 $R = kP, R_b = k_b P$.
3. 计算 $\sigma' = kH(m) - (\sigma_a + x_b H(m) + k_b H(m))H_1(m'_w, R)$. 则伪造的代理签名为 $(m'_w, m, R, R_b, \sigma')$.
4. 以上伪造的代理签名能通过验证, 验证如下:

$$e(\sigma', P) = e((kH(m) - (\sigma_a + x_b H(m) + k_b H(m))H_1(m'_w, R)), P) = e(H(m), R - H_1(m'_w, R) \cdot (P_a + P_b + R_b)).$$

这样 B 在没有 A 的授权的情况下, 伪造了代表原始签名者 A 的代理签名, 损害了 A 的利益.

显然以上攻击方法也适合攻击 Fu-Wang 的代理聚合方案.

攻击方法 3:

原始签名者的伪造攻击, 步骤如下:

1. 原始签名者 A 任选一个 $t \in \mathbb{Z}_q^*$, 他在 CA 处注册新的公钥 $P'_a = tP - P_b$, 相应的私钥未知.
2. A 任选 $k, k_b \in \mathbb{Z}_q^*$, 计算 $R = kP, R_b = k_b P$, 然后计算代理私钥如下: $s'_p = k - (t + k_b) \cdot H_1(m_w, R) \bmod q$.

3. A 用以上生成的代理私钥对任意符合 m_w 的消息 m 签名, $\sigma = s'_p \cdot H(m)$. 则伪造的代理签名为 $(m'_w, m, R, R_b, \sigma)$.

4. 显然以上产生的签名是正确的, 验证如下: $e(\sigma, P) = e(s'_p H(m), P) = e((k - (t + k_b)H_1(m_w, R))H(m), P) = e(H(m), R - (t + k_b)PH_1(m_w, R)) = e(H(m), R - H_1(m_w, R)(P'_a + P_b + R_b))$. 这样 A 在不知道 B 的私钥的情况下, 伪造了 B 的代理签名, 损害了 B 的利益.

攻击方法 4:

代理签名者的伪造攻击, 步骤如下:

1. 代理签名者 B 任选一个 $t \in \mathbb{Z}_q^*$, 他在 CA 处注册新的公钥 $P'_b = tP - P_a$, 相应的私钥未知.
2. B 再任意伪造一个代理授权 m'_w , 随机选取一个 $k, k_b \in \mathbb{Z}_q^*$, 计算 $R = kP, R_b = k_b P$, 然后计算代理私钥如下: $s'_p = k - (t + k_b) \cdot H_1(m'_w, R) \bmod q$.

3. B 用以上生成的代理私钥对任意符合 m'_w 的消息 m 签名, $\sigma = s'_p \cdot H(m)$. 则伪造的代理签名为 $(m'_w, m, R, R_b, \sigma)$.

4. 显然以上产生的签名是正确的, 验证如下:

$$\begin{aligned} e(\sigma, P) &= e(s'_p H(m), P) = e((k - (t + k_b)H_1(m'_w, R))H(m), P) = e(H(m), R - (t + k_b)PH_1(m'_w, R)) \\ &= e(H(m), R - H_1(m'_w, R)(P_a + P'_b + R_b)). \end{aligned}$$

这样 B 在没有 A 的授权的情况下, 伪造了代表原始签名者 A 的代理签名, 损害了 A 的利益.

显然以上攻击方法也适合攻击 Fu-Wang 的代理聚合方案.

攻击方法 5:

第三方攻击者 C 的攻击步骤如下:

1. 第三方攻击者 C 任选一个 $t \in \mathbb{Z}_q^*$, 设 $R'_b = tP - P_a - P_b$.

2. C 再任意伪造一个代理授权 m'_w , 随机选取一个 $k \in \mathbb{Z}_q^*$, 计算 $R = kP$, 然后计算代理私钥如下:
 $s'_p = k - t \cdot H_1(m'_w, R) \bmod q$.

3. C 用以上生成的代理私钥对任意符合 m'_w 的消息 m 签名, $\sigma = s'_p \cdot H(m)$. 则伪造的代理签名为 $(m'_w, m, R, R'_b, \sigma)$.

4. 显然以上产生的签名是正确的, 验证如下:

$$\begin{aligned} e(\sigma, P) &= e(s'_p H(m), P) = e((k - tH_1(m'_w, R))H(m), P) = e(H(m), R - tPH_1(m'_w, R)) \\ &= e(H(m), R - H_1(m'_w, R)(P'_a + P_b + R'_b)). \end{aligned}$$

这样任意第三方都可以伪造原始签名者为 A 代理签名者为 B 的代理签名, 损害了 A, B 的利益.

显然, 以上攻击方法也适合攻击 Fu-Wang 的代理聚合签名方案. 由攻击方法 1, 2, 5 还可看出, 如果要求用户在注册公钥时要提供知道相应私钥的证明, 则 Fu-Wang 的方案也是不安全的.

6 对 Fu-Wang 代理签名方案的进一步改进

6.1 基本代理签名方案的进一步改进

算法由 8 个算法组成.

系统初始化: 初始化过程中, H_1 改为 $H_1: \{0, 1\}^* \times G_1 \times G_1 \rightarrow \mathbb{Z}_q^*$, 其他与 4.1 小节基本代理签名方案的初始化过程相同.

标准签名 1:

1. 输入消息 m , 签名者 A 选择一个随机数 $k \in \mathbb{Z}_q^*$, 计算 $R = kP$, $s = k - x_a H_1(11||m, R, P_a) \bmod q$.
2. A 发送 (m, R, s) 给验证者 B .

标准签名 1 验证: 验证者 B 收到 (m, R, s) 后, 验证以下等式是否成立: $R = sP + H_1(11||m, R, P_a)P_a$, 如果成立, B 接受签名, 否则拒绝.

标准签名 2:

1. 输入消息 m , 签名者 A 计算 $\sigma = x_a H(11||m) \bmod q$.
2. A 发送 σ 给验证者 B .

标准签名 2 验证: 验证者 B 收到 σ 后, 验证以下等式是否成立: $e(\sigma, P) = e(H(11||m), P_a)$, 如果成立, B 接受签名, 否则拒绝.

代理产生: 原始签名者 A 将签名权委托给代理签名者 B , 过程如下:

1. 原始签名者 A 首先产生并公布代理授权 m_w , 该代理授权记录着对代理消息类型的限制、代理的有效期、原始签名人和代理签名人的身份和公钥等信息.
2. 然后, A 选择一个随机数 $k \in \mathbb{Z}_q^*$, 计算 $R = kP$, $s = k - x_a H_1(00||m_w, R, P_a) \bmod q$.
3. 最后, A 通过公开信道发送 (m_w, R, s) 给代理签名者 B .
4. B 收到 s 后, 验证以下等式是否成立: $R = sP + H_1(00||m_w, R, P_a)P_a$, 如果成立, B 接受 s , 否则拒绝.
5. 一旦 s 被接受, B 如下计算代理私钥:

$$s_p = s - x_b \cdot H_1(00||m_w, R, P_b) \bmod q.$$

于是, 隐含的代理公钥为 $P_p = s_p \cdot P = R - H_1(00||m_w, R, P_a) \cdot P_a - H_1(00||m_w, R, P_b) \cdot P_b$.

代理签名产生: 代理签名者 B 代表原始签名者 A 对消息 $m \in \{0, 1\}^*$ 进行签名, 步骤如下:

1. 计算 $H(01||m) \in G_1$.
2. 计算 $\sigma = s_p \cdot H(01||m)$. 即消息 m 的代理签名为 (m_w, m, R, σ) .

代理签名验证: 验证者收到 (m_w, m, R, σ) 后, 首先验证 m 是否适合 m_w , 以及代理的有效期, 原始签名人和代理签名人的身份和公钥是否适合 m_w 等, 然后验证以下等式是否成立:

$$e(\sigma, P) = e(H(01||m), R - H_1(00||m_w, R, P_a) \cdot P_a - H_1(00||m_w, R, P_b) \cdot P_b).$$

如果都成立, 验证者接受代理签名, 否则拒绝.

6.2 代理聚合签名方案的进一步改进

算法由 8 个算法组成

系统初始化: 初始化过程中, H_1 改为 $H_1: \{0, 1\}^* \times G_1 \times G_1 \rightarrow \mathbb{Z}_q^*$, 其他与 4.2 小节代理聚合签名方案的初始化过程相同.

标准签名 1、标准签名 1 验证、标准签名 2、标准签名 2 验证同 6.1 小节.

代理产生: 当原始签名者 A 把他的 n 个不同的签名权力委托给 n 个不同的代理签名者 $B_1, B_2, \dots, B_n$, A 执行以下步骤:

1. 原始签名者 A 首先产生并公布 n 个不同的代理授权 m_{w_i} , $1 \leq i \leq n$, 每个代理授权 m_{w_i} 记录着对不同的代理消息类型的限制、代理的有效期、原始签名人和代理签名人的身份和公钥等信息.
2. 然后, A 选择 n 个随机数 $k_i \in \mathbb{Z}_q^*$, $1 \leq i \leq n$, 计算 $R_i = k_i P$, $s_i = k_i - x_a H_1(00||m_{w_i}, R_i, P_a) \bmod q$.
3. 最后, A 通过公开信道传送 (m_{w_i}, R_i, s_i) , $1 \leq i \leq n$ 给代理签名者 B_i .
4. B_i , $1 \leq i \leq n$ 收到 s_i 后, 验证以下等式是否成立: $R_i = s_i P + H_1(00||m_{w_i}, R_i, P_a)P_a$, 如果成立, 接受 s_i , 否则拒绝.
5. 一旦 s_i 被接受, B_i 如下计算代理私钥:

$$s_{p_i} = s_i - x_{b_i} \cdot H_1(00||m_{w_i}, R_i, P_{b_i}) \bmod q.$$

于是, 隐含的代理公钥为 $P_{p_i} = s_{p_i} \cdot P = R_i - H_1(00||m_{w_i}, R_i, P_a) \cdot P_a - H_1(00||m_{w_i}, R_i, P_{b_i}) \cdot P_{b_i}$.

代理聚合签名产生: 假设有一个消息 $m \in \{0, 1\}^*$ 要签名, 它由 n 个不同的子消息 $m_1, m_2, \dots, m_n$ 组成. 于是每个代理签名者 B_i , $1 \leq i \leq n$ 在他的授权范围内用他的代理私钥签署一个相应的子消息 m_i , 步骤如下:

1. 首先, 每个代理签名者 B_i , $1 \leq i \leq n$ 用他的代理私钥 s_{p_i} 对子消息 m_i 产生一个签名 $\sigma_i = s_{p_i} \cdot H(01||m_i)$.

2. 然后, 合成者把这 n 个不同的代理签名聚合成一个 σ , $\sigma = \sum_{i=1}^n \sigma_i$, 则消息 m 的代理聚合签名 为 $(m_{w_1}, m_{w_2}, \dots, m_{w_n}, m_1, m_2, \dots, m_n, R_1, R_2, \dots, R_n, \sigma)$.

代理聚合签名验证: 验证者收到 $(m_{w_1}, m_{w_2}, \dots, m_{w_n}, m_1, m_2, \dots, m_n, R_1, R_2, \dots, R_n, \sigma)$ 后, 首先验证 m 是否适合 m_w , 以及代理的有效期, 原始签名人和代理签名人的身份和公钥是否适合 m_w 等, 然后验证以下等式是否成立:

$$e(\sigma, P) = \prod_{i=1}^n e(H(01||m_i), R_i - H_1(00||m_{w_i}, R_i, P_a) \cdot P_a - H_1(00||m_{w_i}, R_i, P_{b_i}) \cdot P_{b_i}).$$

如果都成立, 验证者接受代理签名, 否则拒绝.

7 改进方案的安全性及效率分析

7.1 改进方案的安全性分析

下面只分析改进的基本代理签名方案, 改进的代理聚合签名方案可类似证明.

定理 1 在随机预言机模型中, 在适应性选择消息攻击和适应性选择授权攻击下, 假如存在一个攻击者 A 能在多项式时间内以 ε_1 的优势伪造一个用户 1 的标准签名 1、以 ε_2 的优势伪造一个用户 1 的标准签名 2、以 ε_3 的优势伪造一个用户 1 的代理签名或以 ε_4 的优势伪造一个代表用户 1 的代理签名, 他最多进行 q_{ps} 次代理签名询问, 则存在一个攻击者 B , 他能在多项式时间内以以下优势解决 DL 问题: $(1 - \frac{1}{q_{ps}+1})^{q_{ps}} \varepsilon_1$, 或以以下优势解决 CDH 问题: $(1 - \frac{1}{q_{ps}+1})^{q_{ps}} (\frac{1}{q_{ps}+1})(\varepsilon_2 + \varepsilon_3 + \varepsilon_4)$.

证明 假设存在一个攻击者 A 能够攻破改进的基本代理签名方案, 则利用 A 我们可以够造一个攻击者 B , 他能够以一个不可忽略的概率在多项式时间内成功解决 CDH 问题或 DL 问题.

给定用户 1 的公钥 $P_1 = x_1P$, 攻击者 A 注册其他用户的公钥, 设他们的公钥分别为 $P_2 = x_2P, P_3 = x_3P, \dots, P_n = x_nP$. 给定 n 个元组 $(P, kP - t_1x_1P - t_1x_1P, yP), (P, kP - t_2x_2P - t_1x_1P, yP), \dots, (P, kP - t_nx_nP - t_1x_1P, yP)$ 给 B , 其中 $k, t_1, t_2, \dots, t_n, x_1, x_2, \dots, x_n, y \in \mathbb{Z}_q^*$, $k, x_1, x_2, \dots, x_n, y$ 的值为未知, $kP, yP, x_1P, x_2P, \dots, x_nP, t_1, t_2, \dots, t_n$ 为已知, B 的目标是输出 x_1 以解决 DL 问题, 或输出 $x_1yP, (k - t_1x_1 - t_1x_1)yP, (k - t_2x_2 - t_1x_1)yP, \dots, (k - t_nx_n - t_1x_1)yP$ 之一以解决 CDH 问题 (即已知 $(k - t_ix_i - t_1x_1)P, yP$, 求 $(k - t_ix_i - t_1x_1)yP, i \in \{1, 2, \dots, n\}$).

B 充当安全模型中挑战者的身份与 A 进行交互. 在运行过程中, B 维护 8 张表 Warrp, Warro, Warrs, S_{1-qu} , S_{2-qu} , PS_{qu} , H_{1-list} , H_{list} , 这些表初始都为空. A 能作以下询问, B 回答如下:

1. H_1 询问. 输入为 $(00||m_i, P_{1i}, P_{2i})$ 或 $(11||m_i, P_{1i}, P_{2i})$, ($m_i \in \{0, 1\}^*, P_{1i}, P_{2i} \in G_1$), 如果表 H_{1-list} 中已经存在该元组 $(00||m_i, P_{1i}, P_{2i}, h_{1i})$ 或 $(11||m_i, P_{1i}, P_{2i}, h_{1i})$, 则 B 返回 h_{1i} ; 否则, B 取一个随机数 $h_{1i} \in \mathbb{Z}_q^*$, 把元组 $(00||m_i, P_{1i}, P_{2i}, h_{1i})$ 或 $(11||m_i, P_{1i}, P_{2i}, h_{1i})$ 存入表 H_{1-list} 并返回 h_{1i} 给 A .

2. H 询问. 输入为 $(01||m_i)$ 或 $(11||m_i)$, $m_i \in \{0, 1\}^*$, 如果表 H_{list} 中已经存在该元组 $(01||m_i, h_{2i}, b_i, c_i)$ 或 $(11||m_i, h_{2i}, b_i, c_i)$, 则 B 返回 h_{2i} ; 否则, B 产生一个随机数 $c_i \in \{0, 1\}$, $\Pr[c_i = 0] = \frac{1}{q_{ps}+1}$, B

取一个随机数 $b_i \in \mathbb{Z}_q^*$ 并计算 $h_{2i} = (1 - c_i)yP + b_iP$. B 把元组 $(01||m_i, h_{2i}, b_i, c_i)$ 或 $(11||m_i, h_{2i}, b_i, c_i)$ 加入到 H_{list} 中并返回 h_{2i} 给 A .

3. 用户 $j \in \{2, \dots, n\}$ 授权用户 1. 用户 j 产生一个授权 (w, R, s) , B 作 $(00||w, R, P_j)$ 的 H_1 询问得 h_{1i} , 验证 $R = sP + h_{1i}P_j$ 是否成立, 成立则接受该授权, 并把元组 (w, R, s) 加入到表 Warrp 中.

4. 用户 1 授权用户 $j \in \{1, 2, \dots, n\}$ (即包括自代理). 输入为 w_i (可以由 A 选择), B 如下处理:

(1) 首先 B 选择 2 个随机数 $u, v \in \mathbb{Z}_q^*$, 计算 $R = uP + vP_1$;

(2) 然后 B 设 $s = u$, $H_1(00||w_i, R, P_1) = v$, 把 $(00||w_i, R, P_1, v)$ 加入到表 $H_{1-\text{list}}$ 中, 如果 $H_{1-\text{list}}$ 中已经存在该元素, 则 B 返回第一步重新选择 u, v ;

(3) 最后, B 返回 (R, s) 给 A 作为对消息 $00||w_i$ 的签名, 显然该签名是在公钥 P_1 下的对 $00||w_i$ 的签名.

如果是用户 1 授权用户 $j \in \{2, 3, \dots, n\}$, 则 B 把 w_i 加入到表 Warro 中; 如果是用户 1 的自代理, 则 B 把 (w_i, R, s) 加入到表 Warrs 中.

5. 标准签名 1 询问. 设 A 对 m_i 进行用户 1 的标准签名 1 询问, B 如下处理:

(1) 首先 B 选择 2 个随机数 $u, v \in \mathbb{Z}_q^*$, 计算 $R = uP + vP_1$;

(2) 然后 B 设 $s = u$, $H_1(11||m_i, R, P_1) = v$, 把 $(11||m_i, R, P_1, v)$ 加入到表 $H_{1-\text{list}}$ 中, 如果 $H_{1-\text{list}}$ 中已经存在该元素, 则 B 返回第一步重新选择 u, v ;

(3) 最后, B 返回 (R, s) 给 A 作为对消息 $11||m_i$ 的签名, 显然该签名是在公钥 P_1 下的对 $11||m_i$ 的签名.

最后, B 把 m_i 加入到表 $S_{1-\text{qu}}$ 中.

6. 标准签名 2 询问. 设 A 对 m_i 进行用户 1 的标准签名 2 询问, B 如下处理:

(1) B 查询表 H_{list} 得元组 $(11||m_i, h_{2i}, b_i, c_i)$ (如果表 H_{list} 中不存在该元组则对 $11||m_i$ 作 H 询问). 如果 $c_i = 0$, 则 B 失败并终止模拟; 否则, $c_i = 1$, 于是 $h_{2i} = b_iP$. B 计算签名为 $\sigma = b_i x_1 P = b_i P_1$, B 返回 σ 给 A 并把 m_i 加入到表 $S_{2-\text{qu}}$ 中.

7. 代理签名询问. 设 A 对 (w_i, m_i) 进行代理签名询问, 其中 $w_i \in \{\text{Warrp} \cup \text{Warrs}\}$, m_i 适合 m_i , B 如下处理:

(1) B 查询表 H_{list} 得元组 $(01||m_i, h_{2i}, b_i, c_i)$ (如果表 H_{list} 中不存在该元组则对 $01||m_i$ 作 H 询问). 如果 $c_i = 0$, 则 B 失败并终止模拟; 否则, $c_i = 1$, 于是 $h_{2i} = b_iP$.

(2) B 对 w_i 查表 $\text{Warrp} \cup \text{Warrs}$ 获得 (R, s) .

(3) B 对 $(00||w_i, R, P_1)$ 作 H_1 询问得 h_{1i} , 设 $t_1 = h_{1i}$, 计算代理签名 $\sigma = sb_iP - t_1b_iP_1$, 显然 σ 是一个代理签名者为用户 1 原始签名者为用户 $i (i \in \{1, 2, 3, \dots, n\})$ (包括自代理) 的代理签名. B 返回 σ 给 A 并把 (w_i, m_i) 加入到表 PS_{qu} 中.

最终 A 停止询问并输出一个伪造.

E1: A 输出一个伪造 (m, σ) , 而 $V_1(pk_1, 11||m, \sigma) = 1$, 且 $m' \notin S_{1-\text{qu}}$, 即 A 伪造了一个用户 1 的标准签名 1. 设伪造的签名 $\sigma = (R, s)$, 则由分叉引理^[31], 可以得到同一消息 m' 的 2 个合法签名 (R, s) 和 (R, s') , 其中 $H_1(11||m', R, P_1) \neq H'_1(11||m', R, P_1)$, 于是由以下 2 个方程: $s = k - x_1 H_1(11||m', R, P_1) \bmod q$, $s' = k - x_1 H'_1(11||m', R, P_1) \bmod q$, B 能够解出 $x_1 = (s - s') / (H'_1(11||m', R, P_1) - H_1(11||m', R, P_1))$ 从而 B 解决了离散对数问题.

E2: A 输出一个伪造 (m', σ) , 而 $V_2(pk_1, 11||m', \sigma) = 1$, 且 $m' \notin S_{2-\text{qu}}$, 即 A 伪造了一个用户 1 的标准签名 2. B 用 m' 查询表 H_{list} 得元组 $(11||m', h_{2i}, b_i, c_i)$. 如果 $c_i = 1$, B 失败并终止; 否则, $c_i = 0$,

于是 $h_{2i} = yP + b_iP$, 由于 $\sigma = x_1 H(11||m') = x_1(yP + b_iP)$, 于是 $x_1 yP = \sigma - b_i P_1$, 即 B 解决了 CDH 问题.

E3: A 输出一个伪造 $(w', m', p\sigma)$, 而 $PV(pk_j, pk_1, w', m', p\sigma) = 1$ ($j \in \{1, 2, \dots, n\}$), $(w', m') \notin PS_{qu}$. 即 A 伪造了一个原始签名者为用户 j 代理签名者为用户 1 的代理签名, 包括自代理. 设伪造的代理签名 $p\sigma = (w', m', R, \sigma)$, B 用 m' 查询表 H_{list} 得元组 $(01||m', h_{2i}, b_i, c_i)$. 如果 $c_i = 1$, B 失败并终止; 否则, $c_i = 0$, 于是 $h_{2i} = yP + b_iP$, 由于 $\sigma = (k - x_j H_1(00||w', R, P_j) - x_1 \cdot H_1(00||w', R, P_1))H(m')$, $j \in \{1, 2, \dots, n\}$, B 对 $(00||w', R, P_j)$ 查询表 H_{1-list} 得 h_{1i} , 令 $t_j = h_{1i}$, 对 $(00||w', R, P_1)$ 查询表 H_{1-list} 得 h_{1i} , 令 $t_1 = h_{1i}$, 由于 $H(m') = h_{2i} = yP + b_iP$, 于是 $\sigma = (kyP - t_j x_j yP - t_1 x_1 yP) + (b_i R - t_j b_i P_j - t_1 b_i P_1)$, $j \in \{1, 2, \dots, n\}$, 于是 $(k - t_j x_j - t_1 x_1)yP = \sigma - (b_i R - t_j b_i P_j - t_1 b_i P_1)$, $j \in \{1, 2, \dots, n\}$, 即 B 解决了 CDH 问题.

E4: A 输出一个伪造 $(w', m', p\sigma)$, 而 $PV(pk_1, pk_j, w', m', p\sigma) = 1$ ($j \in \{2, \dots, n\}$), $w' \notin Warro$. 即 A 伪造了一个原始签名者为用户 1 代理签名者为用户 j 的代理签名. 设伪造的代理签名 $p\sigma = (w', m', R, \sigma)$, B 用 m' 查询表 H_{list} 得元组 $(01||m', h_{2i}, b_i, c_i)$. 如果 $c_i = 1$, B 失败并终止; 否则, $c_i = 0$, 于是 $h_{2i} = yP + b_iP$, 由于 $\sigma = (k - x_1 \cdot H_1(00||w', R, P_1) - x_j H_1(00||w', R, P_j))H(m')$, $j \in \{2, \dots, n\}$, B 对 $(00||w', R, P_1)$ 查询表 H_{1-list} 得 h_{1i} , 令 $t_1 = h_{1i}$, 对 $(00||w', R, P_j)$ 查询表 H_{1-list} 得 h_{1i} , 令 $t_j = h_{1i}$, 由于 $H(m') = h_{2i} = yP + b_iP$, 于是 $\sigma = (kyP - t_1 x_1 yP - t_j x_j yP) + (b_i R - t_1 b_i P_1 - t_j b_i P_j)$, $j \in \{2, \dots, n\}$, 于是 $(k - t_j x_j - t_1 x_1)yP = \sigma - (b_i R - t_j b_i P_j - t_1 b_i P_1)$, $j \in \{2, \dots, n\}$, 即 B 解决了 CDH 问题.

下面分析 B 成功的概率, 在代理签名询问中, 如果 $c_i = 0$, 则 B 失败, 失败的概率为 $\frac{1}{q_{ps}+1}$, 由于总共进行 q_{ps} 次代理签名询问, 成功的概率为 $(1 - \frac{1}{q_{ps}+1})^{q_{ps}}$, 所以 B 解决 DL 问题成功的概率为 $(1 - \frac{1}{q_{ps}+1})^{q_{ps}} \varepsilon_1$. A 输出一个伪造的标准签名 2 或代理签名 (E3, E4), 如果 $c_i = 1$, B 失败, 失败的概率为 $(1 - \frac{1}{q_{ps}+1})$, 成功的概率为 $\frac{1}{q_{ps}+1}$, 所以 B 解决 CDH 问题成功的概率为 $(1 - \frac{1}{q_{ps}+1})^{q_{ps}} (\frac{1}{q_{ps}+1}) (\varepsilon_2 + \varepsilon_3 + \varepsilon_4)$.

综合以上分析, 假如 G_1 中的 DL 问题或 CDH 问题是困难问题, 则改进的基本代理签名方案在适应性选择消息攻击和适应性选择授权攻击下是存在性不可伪造的.

7.2 改进方案的效率分析

由于密文长度和计算开销是影响效率的两个主要方面, 所以我们在密文长度和计算开销方面对它作个比较. 表 1 显示我们的改进的基本代理签名方案、Lu 等的基本代理签名方案和 Fu-Wang 基本代理签名方案的比较结果. 其中 $|l|$ 代表 G_1 中群元素的长度, $|m_w|$ 代表代理授权的长度, T_{pmul} 表示 G_1 中的点乘运算, T_{pair} 表示双线性对运算, T_{mtp} 表示 MapToPoint hash 运算. 当代理签名者和验证者之间要签署多次代理签名时, 某些重复的计算可以节省下来, 在这种情况下, 效率比较列于表 2 (注: 多次签名时, 因为只需传输 m 和 σ , 其他部分每次都相同就不必传输, 所以表 1 和表 2 的密文长度不同). 从表 1 中可以看出, 在密文长度方面, Lu 等的方案和本文改进方案最短, Fu-Wang 方案长了 $|l|$ 比特. 在计算开销方面, 在签名产生阶段, 3 个方案计算开销相同; 在签名验证阶段, 本文改进方案比 Lu 等方案和 Fu-Wang 方案多 1 次点乘运算. 而在表 2 中, 3 个方案的密文长度, 签名阶段的计算开销和签名验证阶段的计算开销都相同.

综上所述, 本文改进方案只是在代理签名者和验证者之间签署单条消息时增加了一次点乘运算, 考虑到双线性对运算的花费大约是点乘运算的 20 倍^[32] 左右, 而本文改进方案并没有增加双线性对运算次数, 所以计算效率的下降不多, 仍然属于高效的方案.

表 1 基本代理签名方案比较 I

Table 1 The comparison of basic proxy signature schemes I

Schemes	Ciphertext length	Proxy signature generation	Proxy signature verification
Lu et al.'s scheme	$2 l + m_w + m $	$T_{\text{mtp}} + T_{\text{pmul}}$	$T_{\text{mtp}} + T_{\text{pmul}} + 2T_{\text{pair}}$
Fu-Wang's scheme	$3 l + m_w + m $	$T_{\text{mtp}} + T_{\text{pmul}}$	$T_{\text{mtp}} + T_{\text{pmul}} + 2T_{\text{pair}}$
Our scheme	$2 l + m_w + m $	$T_{\text{mtp}} + T_{\text{pmul}}$	$T_{\text{mtp}} + 2T_{\text{pmul}} + 2T_{\text{pair}}$

表 2 基本代理签名方案比较 II

Table 2 The comparison of basic proxy signature schemes II

Schemes	Ciphertext length	Proxy signature generation	Proxy signature verification
Lu et al.'s scheme	$ l + m $	$T_{\text{mtp}} + T_{\text{pmul}}$	$T_{\text{mtp}} + 2T_{\text{pair}}$
Fu-Wang's scheme	$ l + m $	$T_{\text{mtp}} + T_{\text{pmul}}$	$T_{\text{mtp}} + 2T_{\text{pair}}$
Our scheme	$ l + m $	$T_{\text{mtp}} + T_{\text{pmul}}$	$T_{\text{mtp}} + 2T_{\text{pair}}$

8 结论

本文对代理签名的形式化定义和安全模型进行了新的定义, 并对 Fu-Wang 的代理签名方案进行了安全性分析, 指出他们的方案存在伪造性攻击. 然后本文对其进行了改进, 改进方案能有效克服李发根等的攻击和伪造性攻击, 并且原始签名人和代理签名人之间不需要安全信道. 在新的安全模型下, 本文对改进方案进行了安全性证明并分析了改进方案的效率, 效率分析表明改进方案是高效的.

参考文献

- 1 Mambo M, Usuda K, Okamoto E. Proxy signatures: delegation of the power to sign messages. IEICE Trans Fundam Electron Commun Comput Sci, 1996, 79: 1338–1354
- 2 Jabri M A, Matsuoka S. Dealing with grid-computing authorization using identity-based certificateless proxy signature. In: Proceedings of 11th IEEE/ACM International Symposium on CCGrid, Newport Beach, 2011. 544–553
- 3 Cai X Q, Wang S Y. Cryptanalysis of efficient threshold proxy signature protocol for mobile agents. In: Proceedings of IEEE International Conference on Computer Science and Automation Engineering, Shanghai, 2011, 726–728
- 4 Zhang K. Threshold proxy signature schemes. In: Proceedings of Information Security Workshop, London, 1997. 191–197
- 5 Hwang S J, Shi C H. A simple multi-proxy signature scheme. In: Proceedings of the 10th National Conference on Information Security, Hualien, 2000. 134–138
- 6 Yi L J, Bai G Q, Xiao G Z. Proxy multi-signature scheme: a new type of proxy signature scheme. Electron Lett, 2000, 36: 527–528
- 7 Hwang S J, Chen C C. A new multi-proxy multi-signature scheme. Appl Math Comput, 2004, 147: 57–67
- 8 Li L H, Tzeng S F, Hwang M S. Generalization of proxy signature based on discrete logarithms. Comput Secur, 2003, 22: 245–255
- 9 Wang Z C, Qian H F, Li Z B. Hybrid proxy multisignature: a new type multi-party signature. Inform Sci, 2007, 177: 5638–5650
- 10 Singh H, Verma G K. ID-based proxy signature scheme with message recovery. J Syst Softw, 2012, 85: 209–214
- 11 Seo S H, Choi K Y, Hwang J Y, et al. Efficient certificateless proxy signature scheme with provable security. Inform Sci, 2012, 188: 322–337

- 12 Li J G, Xu L Z, Zhang Y C. Provably secure certificate-based proxy signature schemes. *J Comput*, 2009, 4: 444–452
- 13 Tiwari N, Padhye S. New proxy signature scheme with message recovery using verifiable self-certified public keys. In: *Proceedings of 2nd International Conference on Computer and Communication Technology*, Allahabad, 2011. 539–544
- 14 He J, Li X M, Li L J, et al. A new forward-secure proxy signature scheme. In: *Proceedings of the International Forum on Information Technology and Applications*, Kunming, 2010. 30–33
- 15 Fan K, Wang Y, Li H. A new proxy blind signature scheme. *Int J Grid Utility Comput*, 2012, 3: 38–42
- 16 Dai J Z, Yang X H, Dong J X. Designated-receiver proxy signature scheme for electronic commerce. In: *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, 2003. 384–389
- 17 Boldyreva A, Palacio A, Warinschi B. Secure proxy signature schemes for delegation of signing rights. *J Cryptol*, 2012, 25: 57–115
- 18 Herranz J, Saez G. Revisiting Fully Distributed Proxy Signature Schemes. In: *Progress in Cryptology-INDOCRYPT 2004*, LNCS 3348. Berlin: Springer, 2005. 356–370
- 19 Malkin T, Obana S, Yung M. The hierarchy of key evolving signatures and a characterization of proxy signatures. In: *Advances in Cryptology-Eurocrypt 2004*, LNCS 3027. Berlin: Springer, 2004. 306–322
- 20 Wang Q, Cao Z F. Security arguments for partial delegation with warrant proxy signature schemes. *IACR Cryptol ePrint Arch*, 2004, 2004: 315
- 21 Schuldt J C N, Matsuura K, Paterson K G. Proxy Signatures Secure Against Proxy Key Exposure. In: *Public Key Cryptography*, LNCS 4939. Berlin: Springer, 2008. 141–161
- 22 Ristenpart T, Yilek S. The Power of Proofs-of-Possession: Secureing Multiparty Signatures Against Rogue-Key Attacks. In: *Advances in Cryptology-EUROCRYPT 2007*, LNCS 4515. Berlin: Springer, 2007. 228–245
- 23 Wu W, Mu Y, Susilo W, et al. Identity-Based Proxy Signature from Pairings. In: *Autonomic and Trusted Computing*, LNCS 4610. Berlin: Springer, 2007. 22–31
- 24 Zhang L, Zhang F T, Wu Q H. Delegation of signing rights using certificateless proxy signatures. *Inform Sci*, 2012, 184: 298–309
- 25 Cao F, Cao Z F. Security Model of Proxy-Multi Signature Schemes. In: *Cryptology and Network Security*, LNCS 4301. Berlin: Springer, 2006. 144–152
- 26 Lee N Y, Hwang T, Wang C H. On Zhang's nonrepudiable proxy signature schemes. In: *Proceedings of ACISP 1998*, LNCS 1438. Berlin: Springer, 1998. 415–422
- 27 Li F G, Shirase M, Takagi T. Cryptanalysis of efficient proxy signature schemes for mobile communication. *Sci China Inf Sci*, 2010, 53: 2016–2021
- 28 Lu R X, Dong X L, Cao Z F. Designing efficient proxy signature schemes for mobile communication. *Sci China Ser F-Inf Sci*, 2008, 51: 183–195
- 29 Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing. In: *Advances in Cryptology-ASIACRYPT 2001*, LNCS 2248. Berlin: Springer, 2001. 514–532
- 30 Fu X T, Wang C. Improved proxy signature schemes for mobile communication. *J Huazhong Univ Sci Tech*, 2012, 40: 72–75 [傅晓彤, 汪婵. 改进的适用于移动通信的代理签名方案. *华中科技大学学报*, 2012, 40: 72–75]
- 31 Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. *J Cryptol*, 2000, 13: 361–396
- 32 Chen L, Cheng Z, Smart N P. Identity-based key agreement protocols from pairings. *Int J Inf Secur*, 2007, 6: 213–241

Further improvement of Fu-Wang's proxy signature schemes

ZHOU CaiXue^{1*} & LI FaGen²

1 *School of Information Science and Technology, University of Jiujiang, Jiujiang 332005, China;*

2 *School of Computer Science and Engineering, University of Electronic Science and Technology, Chengdu 611731, China*

*E-mail: charlesjjjx@126.com

Abstract In a proxy signature scheme, an original signer can authorize a designated person as his proxy signer and then the proxy signer is able to sign messages on behalf of the original signer. In this paper, we define the new formal definition and security model of proxy signature, and then point out that Fu-Wang's proxy signature schemes are insecure and that the original signer, the proxy signer and the third party attacker can all forge a proxy signature of their schemes, and then by using the methods of binding public key in hash function and padding a special string before message in generating standard signature, proxy-designation and proxy signature and, we further improve their schemes, and give out the security proof in the new security model and analyze the performance of the improved schemes. The result shows the improved schemes are secure and of high efficiency.

Keywords proxy signature, proxy aggregate signature, forgery attack, bilinear pairing, security model

ZHOU CaiXue was born in 1966. He received his B.S. degree (1988) in Computer Science Department from Fudan University, Shanghai and M.S. degree (1991) in Space College of Beijing University of Aeronautics and Astronautics, Beijing. He is an Associate Professor in the School of Information Science and Technology, University of Jiujiang, Jiujiang, China since 2007. He is a member of the CCF (China Computer

Federation). His research interests include applied cryptography, security of computer networks.

LI FaGen was born in 1979. He received his Ph.D. (2007) in School of Communication Engineering from Xi'dian University Xi'an. From 2008 to 2009 he was a Postdoctoral Fellow at Future University-Hakodate, Japan. He is an Associate Professor in the School of Computer Science and Engineering, University Electronic Science and Technology, Chengdu since 2009.

He is a member of the CACR (Chinese Association for Cryptologic Research). His research interests include applied cryptography, security of information science.