文章编号:1005-0523(2016)05-139-04

一种无双线性对的代理盲签名方案

左黎明,郭红丽,张婷婷,陈祚松

(华东交通大学理学院,江西 南昌 330013)

摘要:对林振宇等人提出的改进代理盲签名方案进行了安全性分析,指出其方案不能抵抗有恶意原始签名者参与的合谋攻击,在此基础上提出了一种改进的无双线性对的代理盲签名方案,证明了改进方案在随机预言机模型下是存在性不可伪造。

关键词:代理盲签名;无双线性对;合谋攻击;随机预言机;不可伪造性

中图分类号:TP309.2

文献标志码:A

DOI:10.16749/j.cnki.jecjtu.2016.05.021

代理签名是一类重要的签名,由 Mambo 等^[1]在 1996 年提出。在此之前 Chaum^[2]于 1982 年提出了盲签名的概念,盲签名具有盲性和不可追踪性。2000 年 Lin^[3]首次提出代理盲签名方案,该方案具有盲签名和代理签名的特点。2003 年谭作文^[4]提出了一种基于 Schnorr^[5]签名的代理盲签名方案,将代理签名应用到电子支付和电子选举等。2005 年 Awasthi^[6]基于 Mambo 方案提出一种新的代理盲签名方案。2005 年谷利泽等^[7]提出一种基于离散对数困难问题的代理盲签名方案,但 2010 年王国瞻等^[8]指出文献[7]存在漏洞,不满足不可伪造性和不可链接性,原始签名者通过构造代理私钥可以伪造一个新的签名方案,代理签名者通过签名和签名参数可追踪到代理盲签名。2015 年林振宇等^[9]指出文献[8]中的改进方案依旧存在漏洞,不满足不可伪造性和不可链接性。在研究文献[9]过程中,发现其改进方案值得商榷,存在代理公钥替换攻击漏洞。

1 对原始方案的攻击

预备知识、原方案具体过程详见文献[9],文献[10]中周明和王箭细致归纳和描述了代理盲签名方案的形式化定义、安全模型和 3 种类型敌手能力模型(类型 I 代表恶意原始签名者,类型 II 代表恶意代理签名者,类型 III 代表恶意用户),本文沿用文献[10]中的安全定义和敌手模型,限于篇幅本文也不再另行说明。

1.1 代理公钥替换攻击

恶意攻击者 Jack 与不诚实的原始签名人 A 进行串谋,冒充合法代理签名者进行 B 签名。随机选择 $v \in Z_q^*$, 计算 $y_p = g^v \cdot y_B^{-1}$, y_B 为 B 的公钥,Jack 将 y_p 作为 B 的代理公钥。假设签名接受者 Rose 是诚实的,从盲签名阶段开始,攻击过程如下:

(S1) Jack 随机选择 $v \in Z_q^*$, 计算 $r = g^v \bmod p$, 将 (r_A, r, m, Γ) 发送给签名接收者 Rose;

(S2) Rose 随机选择 $\alpha, \beta, \gamma \in Z_q^*$, 并计算 $r' = r^\alpha g^\beta (y_B y_p)^{-\gamma} \bmod p$, $e' = h(m \| r')$, $e = ((e' - \gamma) / \alpha) \bmod p$, Rose 将 e 发给了冒充者 Jack;

(S3) Jack 计算 $s = (k + ev) \bmod p$, 将 s 传给签名接收者 Rose;

(S4) Rose 接收到 s 后验证 $g^s = r (y_B y_p)^e \bmod p$, 若此式成立, 则计算 $s' = (\alpha s + \beta) \bmod q$, 签名接收者 Rose 接

收稿日期:2016-04-05

基金项目:国家自然科学基金项目(11361024, 11261019);江西省自然科学基金项目(20151BAB201002);江西省研究生创新项目(YC2015-S255)

作者简介:左黎明(1981—),男,副教授,硕士,研究方向为信息安全,非线性系统。

受 $(m, (m_w \Gamma, r_A), (e', s'))$ 作为原始签名者 A 的代理盲签名;若不成立,则代理盲签名无效。

在签名验证过程中,根据文献[9]验证等式: $e' = h(m \parallel g^{s'}(y_{BY_p})^{-e'}) \bmod p$,可见上述攻击是有效的。证明过程如下:

$$\begin{aligned} h(m \parallel g^{s'}(y_{BY_p})^{-e'}) \bmod p &= h(m \parallel g^{\alpha s + \beta}(y_{BY_p})^{-e'}) \bmod p = h(m \parallel g^{\alpha(k+ev) + \beta}(y_B \cdot g^v \cdot y_B^{-1})^{-e'}) \bmod p = \\ h(m \parallel g^{k\alpha + \alpha ev + \beta} \cdot g^{-\alpha ev - \gamma v}) \bmod p &= h(m \parallel g^{k\alpha + \beta - w}) \bmod p = h(m \parallel r^\alpha g^\beta (g^v)^{-\gamma}) \bmod p = \\ h(m \parallel r^\alpha g^\beta (y_{BY_p})^{-\gamma}) \bmod p &= h(m \parallel r') \bmod p = e' \end{aligned}$$

注意到引发原方案漏洞的主要问题在于验证等式中没有使用原始签名人 A 的授权信息而是直接使用了代理公钥,在原始签名人 A 合谋的情况下代理公钥的生成和发布并不一定是权威的。事实上不难发现不诚实的签名接收者 Rose 与不诚实的原始签名人 A 进行串谋,可以通过替换代理公钥实现伪造合法代理签名者 B 的代理签名,攻击方法与上述攻击过程类似。

2 改进的代理盲签名方案

针对文献[9]的公钥替换攻击漏洞,本文提出一个改进的代理盲签名方案。

2.1 符号说明

设 A 为原始签名者, B 为代理签名者, R 是签名接收者。 p 和 q 为大素数,且满足 $q | (p-1)$,选择 Z_p 的 q 阶生成元 $g, 1 \leq g \leq p$,即 $g^q = 1 \pmod{p}$ 。选择抗碰撞的哈希函数 $h: \{0, 1\}^* \rightarrow Z_q^*$ 。设 A 的私钥为 x_A ,公钥为 $y_A = g^{x_A} \bmod p$, B 的私钥为 x_B ,公钥为 $y_B = g^{x_B} \bmod p$, m_w 为代理授权信息。

2.2 代理授权

原始签名者 A 随机选择 $k_A \in Z_q^*$,并计算 $r_A = g^{k_A} \bmod p$,计算 $s_A = x_A h(m_w, r_A) + k_A y_B \bmod q$, A 将 (r_A, s_A, m_w) 通过安全渠道秘密发送给代理签名者 B ,并在线公开 (r_A, g^{s_A}, m_w) 为代理签名者 B 的授权信息。代理签名者 B 收到 (r_A, s_A, m_w) 后,验证等式 $g^{s_A} = y_A^{h(m_w, r_A)} r_A^{y_B}$ 是否成立,若成立,则计算 $x_p = s_A + x_B \bmod q, y_p = g^{x_p} \bmod p$,将 x_p 作为代理私钥, y_p 作为代理公钥。

2.3 代理盲签名

(S1) B 随机选择 $k \in Z_q^*$,计算 $r = g^k \bmod p$,将 (r, y_p) 发送给 R ;

(S2) R 查询 B 的代理信息 (r_A, g^{s_A}, m_w) ,随机选择 $\alpha, \beta \in Z_q^*$ 计算: $r' = r g^\alpha y_p^\beta \bmod p, e' = h(m \parallel r'), e = e' + \beta \bmod q$,将 e 传给 B ;

(S3) B 计算: $s = k + x_p e \bmod q$,将 s 发送给 R ;

(S4) R 收到 s 后,验证等式: $g^s = r g^{s_A \beta} y_B^e \bmod p$,若成立,则计算 $s' = s + \alpha \bmod q$, R 接受 $(m, (r_A, g^{s_A}, m_w), (e', s'))$ 作为 A 的代理盲签名;若不成立,则拒绝该签名。

2.4 签名验证

验证者查询 B 的代理信息 (r_A, g^{s_A}, m_w) ,计算 $r' = g^{s'}(g^{s_A} \cdot y_B)^{-e'}$,验证等式: $e' = h(m \parallel r')$,若该等式成立,则代理盲签名 $(m, (r_A, g^{s_A}, m_w), (e', s'))$ 有效;否则签名无效。

等式的正确性在于 r' ,验证有效性如下:

$$r' = g^{s'}(g^{s_A} \cdot y_B)^{-e'} = g^{s+\alpha}(g^{s_A} \cdot y_B)^{-e'} = g^{s+\alpha}(y_p)^\beta = g^{k+\alpha} \cdot y_p^{\beta-e} = g^{k+\alpha}(y_p)^\beta = r g^\alpha y_p^\beta \bmod p$$

2.5 代理资格注销

原始签名者 A 发布公告含有 (r_A, g^{s_A}, m_w) 的签名均无效,并删除 B 的在线代理信息。

3 安全性分析

3.1 不可伪造性

以下证明在 DLP 困难假设和随机预言机模型下,本文方案针对类型 I 的敌手在适应性选择消息攻击下是不可伪造的,相关安全模型和敌手能力的细致描述参考文献[10]。

定理 假设存在挑战者 C 可以在多项式时间 t 内以一个不可忽略的概率 ε 伪造一个有效的签名,则存在敌手 A_u 在多项式时间 t_2 内以不可忽略概率优势 ε_2 解决 DLP。

证明 设挑战者 C 利用敌手 A_u 要解决的 DLP 困难问题中的一个实例为 $\bar{y}=g^{\bar{x}} \bmod p$, 游戏 G 中允许进行 $q_H=q_{H1}+q_{H2}$ 次哈希询问、 q_{SK} 次密钥询问、 q_p 次代理授密钥询问、 q_S 次签名询问。挑战者 C 掌握了系统参数 (p, g, h) 和原始签名人密钥 (x_A, y_A) , 分别建立表 $L_{H1}, L_{H2}, L_{SKB}, L_p, L_S$, 记录 A_u 询问结果, 初始各表为空。设 $i=k$ 时, 游戏参与者目标密钥对为 $(\bar{x}, \bar{y})$ 。

1) h 询问 1: C 接受 A_u 关于 (m_w, r_{Ai}) 的 h 询问, 查询 L_{H1} , 若 (m_w, r_{Ai}, h_{1i}) 在 L_{H1} 中, C 直接返回结果 $h(m_w, r_{Ai})$ 给 A_u ; 否则 C 随机选择 h_{1i} , 将 h_{1i} 作为 $h(m_w, r_{Ai})$ 值返回给 A_u , 并将 (m_w, r_{Ai}, h_{1i}) 添加到 L_{H1} 中。

2) h 询问 2: C 接受 A_u 关于 (m_i, r'_i) 的 h 询问, 查询 L_{H2} , 若 (m_i, r'_i, h_{2i}) 在 L_{H2} 中, C 直接返回结果 (m_i, r'_i) 给 A_u ; 否则 C 随机选择 h_{2i} , 将 h_{2i} 作为 $h(m_i, r'_i)$ 值返回给 A_u , 并将 (m_i, r'_i, h_{2i}) 添加到 L_{H2} 中。

3) 代理人密钥询问: ① 当 $i \neq k$ 时, C 在表 L_{SKB} 中搜索元组 (y_{Bi}, x_{Bi}) , 若 (y_{Bi}, x_{Bi}) 在表 L_{SKB} 中, 返回结果 (y_{Bi}, x_{Bi}) ; 否则 C 随机选取 $x_{Bi} \in Z_q^*$, 计算 $y_{Bi}=g^{x_{Bi}}$, 记录 (y_{Bi}, x_{Bi}) 在表 L_{SKB} 中, 并返回结果 (y_{Bi}, x_{Bi}) ; ② 当 $i=k$ 时, C 输出 $\perp$, 算法终止。

4) 代理密钥询问: 假设已经做过关于 (m_w, r_{Ai}) 的 h 询问, 否则先做关于 (m_w, r_{Ai}) 的 h 询问 1 和密钥询问。 C 从表 L_p 搜索元组 $(r_{Ai}, s_{Ai}, m_w, x_{Bi}, k_{Ai}, x_{pi}, y_{pi})$, 若 $(r_{Ai}, s_{Ai}, m_w, x_{Bi}, k_{Ai}, x_{pi}, y_{pi})$ 在表 L_p 中, 返回结果 (x_{pi}, y_{pi}) , 否则: ① 当 $i \neq k$ 时, 随机选择 $k_{Ai} \in Z_q^*$, 计算 $s_{Ai}=x_{Ai}h_{1i}+k_{Ai}y_{Bi} \bmod q$, $x_{pi}=s_{Ai}+x_{Bi}$, $y_{pi}=g^{x_{pi}}$, 并添加 $(r_{Ai}, s_{Ai}, m_w, x_{Bi}, k_{Ai}, x_{pi}, y_{pi})$ 到表 L_p 中, 并结果返回 (x_{pi}, y_{pi}) ; ② 当 $i=k$ 时, C 输出 $\perp$, 算法终止。

5) 签名询问: A_u 可以对挑战者 C 进行签名询问。假设已经做过关于 m_i 的 h 询问, 否则先执行关于 m_i 的 h 询问。 C 从表 L_S 中寻找 m_i 的签名, 如果元组 $(m_i, (r_{Ai}, g^{s_{Ai}}, m_w), (e', s'))$ 在表 L_S 中, 则返回 $(m_i, (r_{Ai}, g^{s_{Ai}}, m_w), (e', s'))$ 给攻击者。否则: ① 当 $i \neq k$ 时, 挑战者 C 获取代理密钥 (x_{pi}, y_{pi}) , 通过正常运行本文的代理盲签名方案得到一个签名 $(m_i, (r_{Ai}, g^{s_{Ai}}, m_w), (e', s'))$ 来回答 A_u , 并记录在表 L_S ; ② 当 $i=k$ 时, 选择 $v \in Z_q^*$, $k \in Z_q^*$, $\alpha, \beta \in Z_q^*$ 计算: $\bar{y}_p=g^v \cdot \bar{y}^{-1}$, $r=g^k \bmod p$, $r'=rg^{\alpha}y_p^{\beta} \bmod p$, $e'=\beta$, $e=e'$, $s=k+e \pmod{q}$, $s'=s+\alpha \bmod q$, 挑战者 C 将 $(m_i, (r_{Ai}, g^{s_{Ai}}, m_w), (e', s'))$ 作为代理盲签名发送给攻击者 A_u , 并记录在表 L_S 。事实上, 此签名的有效性可由下式保证:

$$r'=g^{e'}(g^{s_{Ai}}\bar{y})^{-e'}=g^{s+\alpha}(g^{s_{Ai}}g^{\bar{x}})^{-\beta}=g^{s+\alpha}g^{-s_{Ai}\bar{x}-\beta}=g^{k+\beta+s_{Ai}\bar{x}+\alpha}g^{-s_{Ai}\bar{x}-\beta}=g^{k+\alpha}(y_p)^{\beta}=rg^{\alpha}y_p^{\beta} \bmod p$$

假设游戏没有终止, 在执行完多项式有界次询问后, A_u 可以在多项式时间 t 内以一个不可忽略的概率 ε 产生一个关于消息 m 的有效签名。根据分叉引理, 通过有限次的哈希重放, 可以输出关于目标密钥对 $(\bar{x}, \bar{y})$ 和消息 m 的两个有效签名 $(m, (r_A, g^A, m_w), (e_1', s_1'))$ 和 $(m, (r_A, g^A, m_w), (e_2', s_2'))$, 由本文方案中等式 $s=s'-\alpha \bmod q$, $e=e'-\beta \bmod q$, $s=k+x_p \bmod q$, $x_p=s_A+\bar{x} \bmod q$, 可以得到: $s_1'=k+(s_A+\bar{x})(e_1'+\beta)+\alpha \bmod q$, $s_2'=k+(s_A+\bar{x})(e_2'+\beta)+\alpha \bmod q$, $s_2'-s_1'=(e_2'-e_1')(s_A+\bar{x})$, 则 $\bar{x}=(s_2'-s_1')(e_2'-e_1')^{-1}-s_A$ 。 C 将 $\bar{x}=(s_2'-s_1')(e_2'-e_1')^{-1}-s_A$ 作为 DLP 的解。

游戏不终止的概率至少为 $\frac{1}{q_{sk}q_{pk}}$, 成功分叉的概率不小于 $\frac{1}{10^6q_h^2}$, 则 C 成功解决 DLP 的优势 $\varepsilon_2 \geq \frac{1}{10^6q_h^2q_{sk}q_{pk}}\varepsilon_1$, 需要的时间 $t_2 \leq \frac{2}{\varepsilon_2}(t_{H1}+t_{H2}+t_{SKB}+t_p+t_s+t_1)$, 其中 t_{H1} 和 t_{H2} 分别为两次哈希询问时间、 t_{SKB} 为密钥询问时间、 t_p 为代理密钥询问时间、 t_s 为签名询问时间。由上述过程可知 C 可以在多项式时间 t_2 内以不可忽略的概率 ε_2 解决 DLP, 但这与 DLP 的困难性矛盾, 所以在随机预言机模型和 DLP 困难性的假设下, 本文方案是随机预言机模型下不可伪造的。

3.2 效率分析

在盲签名阶段, 为了修补原始方案漏洞, 本文方案比原始方案增加了 2 个乘运算和 1 个指数运算, 其他阶段与原始签名的计算复杂度相同。

4 结语

代理盲签名是电子金融应用中一种非常重要的签名形式, 适用于实时性要求比较高, 需要采用多台签名服务器分担主签名服务器的负担的场合^[11](比如铁路网上售票系统)。本文在对文献[9]提出的代理盲签名方案分析时发现原方案存在一些值得商榷的安全缺陷, 导致不能抵抗代理公钥替换攻击。随后提出了一种

改进的代理盲签名方案,针对类型 I 敌手,改进方案能够被证明在随机预言机模型下是存在不可伪造的。本文方案没有使用实现困难且效率低下的双线性对运算,易于实现。

参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures for delegating signing operation[C]//Proc of 3rd ACM Conference on Computer and Communications Security, New Delhi: ACM Press, 1996: 48-57.
- [2] CHAUM D. Blind signatures for untraceable payments[C]//Proceedings of CRYPTO'82, New York: Plenum Press, 1983: 199-203.
- [3] LIN W D, JAN J K. A security personal learning tools using a proxy blind signature scheme[C]//Proc of International Conference on Chinese Language Computing, Illinois, USA: ICCLC Bess, 2000: 273-277.
- [4] TAN Z W, LIU Z J, TANG C M. A proxy blind signature schemes based on DLP[J]. Journal of Software, 2003, 14(11): 1931-1935.
- [5] SCHNORR C. Efficient identification and signature for smart cards[C]//Proceedings of CRYPTO 89, LNCS 435, Berlin: Springer, 1990: 239-252.
- [6] AWASTHI A K, LAL S. Proxy blind signature scheme[J]. JFCR Transaction on Cryptology, 2005, 2(1): 5-11.
- [7] 谷利泽, 张胜, 杨义先. 代理盲签名方案及其在电子货币中的应用[J]. 计算机工程, 2005, 31(16): 11-13.
- [8] 王国瞻, 亢保元, 成林. 一个代理盲签名方案的分析[J]. 计算机工程, 2010, 36(3): 134-135.
- [9] 林振宇, 贺亚威, 候整风. 改进的代理盲签名方案[J]. 合肥工业大学学报, 2015, 38(1): 40-43.
- [10] 周明, 王箭. 一个可证安全的高效的代理盲签名方案[J]. 计算机工程与科学, 2015, 37(9): 1643-1651.
- [11] 汤鹏志, 陈仁群, 左黎明. 一种基于椭圆曲线的门限部分盲签名方案[J]. 华东交通大学学报, 2014, 31(6): 96-102.

An Improved Proxy Blind Signature Scheme without Nilinear Pairing

Zuo Liming, Guo Hongli, Zhang Tingting, Chen Zuosong

(School of Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: The cryptanalysis of an improved proxy blind signature scheme without bilinear pairing proposed by Lin et al. pointed out that the scheme couldn't resist conspiracy attack which was made by the participant malicious original signer. Therefore, an improved proxy blind signature scheme without bilinear was put forward and proved to be existentially unforgeable against malicious original signers in random oracle model.

Key words: proxy blind signature; no bilinear pairing; collusion attacks; random oracle; unforgeability

(责任编辑 刘棉玲)