信息科学

改进的基于 ECDLP 的无证书部分盲签名机制

张雪峰 [1], 何俊杰 [2], 祁传达 [2]

(1. 信阳农林学院 计算机科学系, 河南 信阳 464000)
(2. 信阳师范学院 数学与信息科学学院, 河南 信阳 464000)

摘 要: 对邵国金等人 (四川大学学报 (工程科学版), 2012 年第 1 期) 提出的基于椭圆曲线离散对数难题 (ECDLP) 的无双线性对运算的部分盲签名方案进行安全性分析, 发现方案不能抵抗公钥替换攻击. 为此, 提出了一个改进方案. 在随机谕言模型下证明了改进方案对自适应选择消息和身份攻击是存在性不可伪造性的. 将所提方案与部分现有的无证书部分盲签名方案的计算性能进行了比较, 结果显示改进方案具有较高的运算效率.

关键词: 部分盲签名; 无证书密码体制; 椭圆曲线; 离散对数; 随机谕言模型

1982 年, Chuam[1] 首次提出盲签名的概念. 盲签名可以有效保护用户的隐私, 被大量应用于电子现金、电子投票和电子拍卖等场合. 1996 年, Abe 和 Fujisaki[2] 提出了部分盲签名的概念. 部分盲签名是在盲签名的基础上嵌入了签名者与用户事先协商好的公共信息, 增强了签名者对消息的可控性. 1984 年, Shamir[3] 提出了基于身份公钥密码体制, 很好的解决了传统公钥密码系统中公钥证书的存储和管理问题. 但在基于身份公钥密码体制中, 用户私钥由密钥生成中心 (KGC) 统一生成, 恶意的 KGC 可以生成任意一个用户的私钥, 进而冒充该用户进行签名或解密行为. 2003 年, Al-Riyami 和 Paterson[4] 提出了无证书的公钥密码体制模型, 既消除了基于身份的密码体制中的密钥托管问题, 还不需要使用公钥证书 [5].

2008 年, 荣维坚 [6] 提出了第一个无证书部分盲签名方案, 但余丹等 [7] 指出方案不满足部分盲性. 随后, 不少学者都提出了无证书的部分盲签名方案 [8−10]. 但现有的无证书部分盲签名方案几乎都使用了计算开销比较大的双线性对运算, 效率不高. 2012 年, 邵国金等人 [11] 基于椭圆曲线离散对数难题提出了一种无证书部分盲签名算法, 该算法不使用双线性对运算, 在计算性能方面具有明显的优势.

本文对文献 [11] 所提出的无证书部分盲签名方案进行安全性分析, 指出方案不能抵抗公钥替换攻击. 为此, 提出了一种改进方案. 在随机谕言模型和椭圆曲线离散对数问题困难的假设下, 证明了改进方案可以抵抗两类敌手 (可以替换公钥的不诚实用户和恶意但被动的

收稿日期: 2013-11-20
资助项目: 国家自然科学基金 (61272465); 河南省自然科学基金项目 (142300410320,142300410317); 河南省教育厅科学技术研究项目 (14B520046)

KGC) 的自适应选择消息和身份的存在性伪造攻击. 与部分现有的无证书部分盲签名方案相比, 改进方案具有较高的运算效率.

1 预备知识

1.1 椭圆曲线离散对数问题

椭圆曲线密码学建立在椭圆曲线离散对数问题 (ECDLP) 难解的假设上. 设 $E(F_p)$ 为阶为素数 p 的有限域 F_p 上的椭圆曲线. T, Q 是 $E(F_p)$ 上的点, 其中, T 的阶为素数 n, 并且 Q 是 T 的倍数点, 即存在 $a \in Z_n^*$, 满足等式 $Q = aT$, 那么椭圆曲线离散对数问题定义如下.

1) ECDLP(Discrete Logarithm Problem): 对任意未知的 $a \in Z_n^*$, 给定 T, aT, 计算 a.

2) ECDLP 假设: 对任意的概率多项式时间算法 $\mathcal{A}$ 解决 ECDLP 的优势:

$$Adv^{ECDLP}(\mathcal{A}) = \Pr[\mathcal{A}(T, aT) = a | a \in Z_n^*]$$

是可以忽略的.

1.2 无证书密码体制的攻击模型

无证书签名系统中有两类敌手, 即第 1 类敌手 $\mathcal{A}_I$ 与第 2 类敌手 $\mathcal{A}_{II}$. 其中, $\mathcal{A}_I$ 模拟不诚实的用户, 它可以任意替换用户的公钥, 但不知道系统主密钥; $\mathcal{A}_{II}$ 模拟恶意但被动的 KGC, 它知道系统的主密钥, 但是不能替换目标用户的公钥.

2 对文献 [11] 方案的公钥替换攻击

2.1 方案回顾

1) 系统建立. 系统参数 $params=\{E(F_p), T, P_0, H_1, H_2, H_3\}$, 其中, $E(F_p)$ 是椭圆曲线上的加法循环群, $P_0 = sT$ 是 KGC 的公钥, 对应的 $s \in Z_n^*$ 是 KGC 的主密钥; H_1, H_2, H_3 是安全的散列函数.

2) 密钥产生. 签名者 A 提交其身份 ID_A 给 KGC, KGC 随机选择 $y_A \in Z_n^*$, 计算 $Y_A = y_A T$, $q_A = H(ID_A, Y_A)$ 和 $d_A = y_A + sq_A$ 并返回 d_A 作为 A 的部分私钥, Y_A 作为 A 的部分公钥. A 随机选择 $x_A \in Z_n^*$ 作为私有秘密值, 计算 $X_A = x_A T$, 输出私钥 $S_A = (x_A, d_A)$ 和公钥 $P_A = (X_A, Y_A)$.

3) 签名发布. 用户向签名者 A 请求消息 m 的部分盲签名, c 是双方事先协商的公共信息, 用户和签名者交互执行如下协议:

① 签名 (阶段 1). 签名者 A 随机选择 $r \in Z_n^*$, 计算 $R = rT$, 并将 R 发送给用户;

② 盲化. 用户随机选择 $\alpha, \beta \in Z_n^*$, 计算 $z = H_3(c)$, $L = \alpha R + \alpha\beta zT$, $h = H_2(m, c, L)$ 和 $u = \alpha^{-1}h + \beta z$, 然后发送 u 给 A;

③ 签名 (阶段 2). 签名者 A 计算 $v = (r + u)/(x_A + d_A + z)$, 其中 $z = H_3(c)$, 将 v 返回给用户;

④ 去盲. 用户收到 v 后, 计算 $w = \alpha v$, 输出对 (m, c) 的部分盲签名 (L, w).

4) 签名验证. 验证者计算 $z = H_3(c)$, $q_A = H(ID_A, Y_A)$ 和 $h = H_2(m, c, L)$, 验证等式

$$L + hT = w(X_A + Y_A + q_A P_0 + zT)$$

是否成立, 若等式成立则接受签名, 否则拒绝.

2.2 公钥替换攻击

邵国金等人 [11] 在随机谕言模型下证明了方案能抵抗无证书签名的两类敌手的适应性选择消息和身份攻击下的存在性伪造. 但我们分析发现, 方案并不能抵抗公钥替换攻击.

敌手 $\mathcal{A}_I$ 可按如下操作伪造用户 ID_A 对任意消息 m 和公共信息 c 的部分盲签名:

1) 随机选择 $\delta \in Z_n^*$, 计算 $q_A = H(ID_A, Y_A)$, $X_A^* = \delta T - Y_A - q_A P_0$, 用 $P_A^* = (X_A^*, Y_A)$ 代替用户 A 的公钥;

2) 随机选择 $\tau \in Z_q^*$, 计算 $L^* = \tau T$, $z = H_3(c)$, $h^* = H_2(m, c, L^*)$ 和 $w^* = (\tau + h^*)(\delta + z)^{-1}$.

由于

$$w^*(X_A^* + Y_A + q_A P_0 + zT) = (\tau + h^*)(\delta + z)^{-1}(\delta T + zT) = (\tau + h^*)T = L^* + h^* T$$

说明 (L^*, w^*) 满足验证方程, 是敌手 $\mathcal{A}_I$ 假冒身份为 ID_A 的用户对消息 m 和公共信息 c 伪造的有效部分盲签名.

3 文献 [11] 方案的改进

为了抵抗敌手 $\mathcal{A}_I$ 的公钥替换攻击, 对文献 [11] 方案提出了一个改进算法. 改进方案的密钥产生算法与文献 [11] 方案相同. 在系统建立阶段, 增加安全的散列函数 $H_4 : E(F_p) \to Z_n^*$, 系统参数 $params$=$\{E(F_p), T, P_0, H_1, H_2, H_3, H_4\}$. 签名发布和验证算法描述如下.

3.1 签名发布

用户请求签名者 A 对消息 m 进行部分盲签名, c 是双方事先协商的公共信息, 用户和签名者 A 进行如下交互:

1) 签名 (阶段 1): 签名者 A 选择随机数 $r \in Z_n^*$, 计算 $R = rT$, 并将 R 发送给用户;

2) 盲化: 用户随机选择 $\alpha, \beta \in Z_n^*$, 计算 $z = H_3(c)$, $L = \alpha R + \alpha\beta zT$, $h = H_2(m, c, L)$ 和 $u = \alpha^{-1}h + \beta z$, 然后发送 u 给 A;

3) 签名 (阶段 2): 签名者 A 计算 $z = H_3(c)$, $t_A = H_4(X_A)$ 和 $v = (r + u)/(x_A + t_A d_A + z)$, 将 v 返回给用户;

4) 去盲: 用户收到 v 后, 计算 $w = \alpha v$, 输出对 (m, c) 的部分盲签名 (L, w).

3.2 签名验证

验证者计算 $z = H_3(c)$, $t_A = H_4(X_A)$, $q_A = H(ID_A, Y_A)$ 和 $h = H_2(m, c, L)$, 验证等式

$$L + hT = w(X_A + t_A Y_A + t_A q_A P_0 + zT)$$

是否成立. 若等式成立则接受签名, 否则拒绝.

4 改进方案的分析

4.1 正确性证明

因为,

$$\begin{aligned}
&w(X_A + t_A Y_A + t_A q_A P_0 + zT) = \alpha v\,(x_A + t_A(y_A + q_A s) + z)T = \\
&\alpha(r + u)(x_A + t_A d_A + z)^{-1}\,(x_A + t_A d_A + z)\,T = \alpha(r + \alpha^{-1}h + \beta z)T = \\
&\alpha r T + (h + \alpha\beta z)T = \alpha R + \alpha\beta zT + hT = L + hT,
\end{aligned}$$

说明 (m,c,L,w) 满足验证等式, 是有效的部分盲签名, 即改进名方案是正确的.

4.2 安全性分析

1) 不可伪造性

定理 1 在随机谕言模型和 ECDLP 困难的假设下, 改进方案对敌手 $\mathcal{A}_I$ 的自适应选择消息和身份攻击是存在性不可伪造的.

证明 设算法 $\mathcal{C}$ 是解决 ECDLP 的挑战者, 即给定 (T,aT), $a\in Z_n^*$ 未知, 目标是计算 a.

假设存在敌手 $\mathcal{A}_I$ 以不可忽略的概率成功伪造盲签名, 则 $\mathcal{C}$ 可以调用敌手 $\mathcal{A}_I$ 作为子程序进而计算出 a. 具体过程如下:

系统设置. 算法 $\mathcal{C}$ 生成系统参数 $params$=$\{E(F_p), T, P_0, H_1, H_2, H_3, H_4\}$, 其中系统公钥设置为 $P_0=aT$, 即用 a 模拟系统主密钥, 但 $\mathcal{C}$ 不知道 a 的值. 将 $params$ 发送给攻击者 $\mathcal{A}_I$.

询问. $\mathcal{A}_I$ 可以适应性地向 $\mathcal{C}$ 进行多项式有界次的询问. 简单起见, 假设每次询问都是互不相同的. $\mathcal{C}$ 随机选择整数 $N(1\le N\le q_K)$, 记 $ID_N=ID^*$.

①H_1 询问: $\mathcal{C}$ 维持表 L_1 记录并响应 $\mathcal{A}_I$ 的 H_1 询问. $\mathcal{A}_I$ 关于 $(ID_i,*)(1\le i\le q_1)$ 的每次 H_1 询问, $\mathcal{C}$ 首先查看表 L_1. 如果 L_1 中含有项 (ID_i, Y_i, d_i, q_i), 将 q_i 返回给 $\mathcal{A}_I$ 作为 (ID_i,Y_i) 的 H_1 散列值. 否则, 如果 $ID_i=ID^*$, 令 $d_i=\perp$; 随机选择 $y_i,d_i\in Z_n^*$, 计算 $Y_i=y_iT$; 如果 $ID_i\neq ID^*$, 随机选择 $d_i,q_i\in Z_n^*$, 计算 $Y_i=d_iT-q_i(aT)$. 将 (ID_i, Y_i, d_i, q_i) 添加到 L_1, 并将 $H_1(ID_i,Y_i)=q_i$ 返回给 $\mathcal{A}_I$.

②H_2 询问: $\mathcal{C}$ 维持表 L_2 记录并响应 $\mathcal{A}_I$ 的 H_2 询问. $\mathcal{A}_I$ 关于 (m_i,c_i,L_i) $(1\le i\le q_2)$ 的每次 H_2 询问, $\mathcal{C}$ 首先查看表 L_2. 如果 L_2 中含有项 (m_i,c_i,L_i,h_i), $\mathcal{C}$ 将 h_i 返回给 $\mathcal{A}_I$ 作为 (m_i,c_i,L_i) 的 H_2 散列值; 否则, 随机选择 $h_i\in Z_n^*$, 将 (m_i,c_i,L_i,h_i) 添加到 L_2, 并将 $H_2(m_i,c_i,L_i)=h_i$ 返回给 $\mathcal{A}_I$.

③ H_3 询问: $\mathcal{C}$ 维持表 L_3 记录并响应 $\mathcal{A}_I$ 的 H_3 询问. $\mathcal{A}_I$ 关于 c_i $(1\le i\le q_3)$ 的每次 H_3 询问, $\mathcal{C}$ 首先查看表 L_3. 如果 L_3 中含有项 (c_i,z_i), $\mathcal{C}$ 将 z_i 返回给 $\mathcal{A}_I$ 作为 c_i 的 H_3 散列值; 否则, 随机选择 $z_i\in Z_n^*$, 将 (c_i,z_i) 添加到 L_3, 并将 $H_3(c_i)=z_i$ 返回给 $\mathcal{A}_I$.

④ H_4 询问: $\mathcal{C}$ 维持表 L_4 记录并响应 $\mathcal{A}_I$ 的 H_4 询问. $\mathcal{A}_I$ 关于 X_i $(1\le i\le q_4)$ 的每次 H_4 询问, C 首先查看表 L_4. 如果 L_4 中含有项 (X_i,t_i), $\mathcal{C}$ 将 t_i 返回给 $\mathcal{A}_I$ 作为 X_i 的 H_4 散列值; 否则, 随机选择 $t_i\in Z_n^*$, 将 (X_i,t_i) 添加到 L_4, 并将 $H_4(X_i)=t_i$ 返回给 $\mathcal{A}_I$.

⑤ 公钥询问: $\mathcal{C}$ 维持表 L_{PK} 记录并响应 $\mathcal{A}_I$ 的公钥询问. $\mathcal{A}_I$ 关于 ID_i $(1\le i\le q_{PK})$ 的每次公钥询问, $\mathcal{C}$ 首先查看表 L_{PK}. 如果表 L_{PK} 中含有项 (ID_i,Y_i,X_i,x_i), $\mathcal{C}$ 将 $P_i=(Y_i,X_i)$ 返回给 $\mathcal{A}_I$ 作为身份 ID_i 的公钥. 否则, 也就是 $\mathcal{A}_I$ 从来没做过 ID_i 的公钥询问, 则随机选择 $x_i\in_R Z_n^*$, 计算 $X_i=x_iT$; 并查询 L_1, 取得 Y_i. $\mathcal{C}$ 将 (ID_i,Y_i,X_i,x_i) 添加到表 L_{PK}, 并将 $P_i=(Y_i,X_i)$ 返回给 $\mathcal{A}_I$.

⑥ 部分私钥询问: 对 $\mathcal{A}_I$ 关于 ID_i $(1\le i\le q_E)$ 的部分私钥询问 (假设已经做过关于 $(ID_i,*)$ 的 H_1 询问, 否则先执行 H_1 询问), 如果 $ID_i=ID^*$, $\mathcal{C}$ 宣告失败, 算法终止; 如果 $ID_i\neq ID^*$, $\mathcal{C}$ 从表 L_1 中找出项 (ID_i, Y_i, d_i, q_i), 将 d_i 返回给 $\mathcal{A}_I$.

⑦ 秘密值询问: 对 $\mathcal{A}_I$ 关于 ID_i $(1\le i\le q_{SV})$ 的秘密值询问, $\mathcal{C}$ 首先查看表 L_{PK}. 如果 L_{PK} 中含有项 (ID_i,Y_i,X_i,x_i), $\mathcal{C}$ 将 x_i 返回给 $\mathcal{A}_I$ 作为 ID_i 的秘密值; 否则, $\mathcal{C}$ 首先执行对 ID_i 的公钥询问, 并将 x_i 返回给 $\mathcal{A}_I$.

⑧ 公钥替换询问：对 $\mathcal{A}_I$ 关于 (ID_i, P_i^*) $(1 \le i \le q_{RP})$ 的公钥替换询问, 其中 $P_i^* = (Y_i^*, X_i^*)$, $\mathcal{C}$ 首先查看表 L_{PK}. 如果 L_{PK} 中含有项 (ID_i, Y_i, X_i, x_i), 则令 $x_i = \perp$, $Y_i = Y_i^*$, $X_i = X_i^*$; 否则将 $(ID_i, Y_i, X_i, \perp)$ 添加到 L_{PK}.

⑨ 签名询问：$\mathcal{C}$ 维持表 L_S 记录并响应 $\mathcal{A}_I$ 的签名询问. $\mathcal{A}_I$ 可以选择消息 m 和身份 ID, 对 (ID, m, c) 进行签名询问, 假设已经做过关于 ID 的公钥询问, 关于 c 的 H_3 询问, 关于 X_{ID} 的 H_4 询问及关于 (ID, Y_{ID}) 的 H_1 询问, 否则先执行公钥询问、H_1 询问、H_3 询问和 H_4 询问. $\mathcal{C}$ 从表 L_{PK} 中找出项 $(ID, Y_{ID}, X_{ID}, x_{ID})$, 从表 L_1 中找出项 $(ID, Y_{ID}, d_{ID}, q_{ID})$, 从表 L_3 中找出项 (c, z), 从表 L_4 中找出项 (X_{ID}, t_{ID}). 任意选择 $h, w \in Z_n^*$, 计算

$$L = w(X_{ID} + t_{ID}Y_{ID} + t_{ID}q_{ID}P_0 + zT) - hT$$

如果 (m, c, L, h) 已经在表 L_2 中, 则重新选择 h, w 并计算 L; 将 (m, c, L, h) 加到表 L_2, 并将 (L, w) 作为身份 ID 对 (m, c) 的部分盲签名返回给 $\mathcal{A}_I$.

伪造. 如果算法 $\mathcal{C}$ 没有终止, 则 $\mathcal{A}_I$ 在没有做过 ID^* 的部分私钥询问及 (ID^*, m, c) 的签名询问的情况下, 以一个不可忽略的概率输出身份为 ID^* 的用户对消息 m 的有效部分盲签名 (ID^*, m, c, L, w). 根据 Forking 引理 [12], 通过对 $\mathcal{A}_I$ 的 H_2 询问和 H_4 询问进行散列重放, $\mathcal{C}$ 可以获得消息 m 的三个有效部分盲签名 $(ID^*, m, c, L, w_i, h_i, t_i)$, $i = 1, 2, 3$, 其中 t_1, t_2, t_3 互不相同. 于是

$$L + h_iT = w_i\left(X_{ID^*} + t_i(Y_{ID^*} + q_{ID^*}P_0) + zT\right),\ i = 1, 2, 3$$

其中, $Y_i = y_iT$. 这 3 个等式可以看成是关于 L, X_{ID^*} 和 P_0 的线性方程组：

$$L - w_iX_{ID^*} - w_it_iq_{ID^*}P_0 = (w_it_iy_i + w_iz - h_i)T,\ i = 1, 2, 3$$

可以解出

$$P_0 = \frac{(w_1 - w_2)(b_3 - b_1) - (w_1 - w_3)(b_2 - b_1)}{(w_1 - w_2)(a_3 - a_1) - (w_1 - w_3)(a_2 - a_1)}T$$

其中, $a_i = w_it_iq_{ID^*}$, $b_i = w_it_iy_i + w_iz - h_i$, 于是,

$$a = \frac{(w_1 - w_2)(b_3 - b_1) - (w_1 - w_3)(b_2 - b_1)}{(w_1 - w_2)(a_3 - a_1) - (w_1 - w_3)(a_2 - a_1)}$$

即为 ECDLP 的解.

所以, 在 ECDLP 问题困难的假设下, 改进方案对敌手 $\mathcal{A}_I$ 的自适应选择消息和身份攻击是存在性不可伪造的.

定理 2 在随机谕言模型和 ECDLP 困难的假设下, 改进方案对敌手 $\mathcal{A}_{II}$ 的自适应选择消息和身份攻击是存在性不可伪造的.

证明 设算法 $\mathcal{C}$ 是解决 ECDLP 的挑战者, 即给定 (T, aT), $a \in Z_n^*$ 未知, 目标是计算 a.

假设存在敌手 $\mathcal{A}_{II}$ 以不可忽略的概率成功伪造盲签名, 则 $\mathcal{C}$ 可以调用敌手 $\mathcal{A}_{II}$ 作为子程序进而计算出 a. 具体过程如下：

系统设置. $\mathcal{C}$ 选择随机数 $s \in Z_n^*$ 作为系统主密钥, 生成系统参数 $params$={$E(F_p)$, T, P_0, H_1, H_2, H_3, H_4}, 其中系统公钥 $P_0 = sT$, 将 $params$ 和 s 发送给敌手 $\mathcal{A}_{II}$.

询问. $\mathcal{A}_{II}$ 可以适应性地向 $\mathcal{C}$ 进行多项式有界次的询问. 简单起见, 假设每次询问都是互不相同的. $\mathcal{C}$ 随机选择整数 $N(1 \le N \le q_K)$, 记 $ID_N = ID^*$.

① H_2 询问、H_3 询问、H_4 询问和签名询问与定理 1 相同.

② H_1 询问：$\mathcal{C}$ 维持表 L_1 记录并响应 $\mathcal{A}_{II}$ 的 H_1 询问. $\mathcal{A}_{II}$ 关于 $(ID_i, *)(1 \le i \le q_1)$ 的每次 H_1 询问, $\mathcal{C}$ 首先查看表 L_1. 如果 L_1 中含有项 (ID_i, Y_i, d_i, q_i), $\mathcal{C}$ 将 q_i 返回给 $\mathcal{A}_{II}$ 作为 (ID_i, Y_i) 的 H_1 散列值. 否则, 随机选择 $y_i, d_i \in Z_n^*$, 计算 $Y_i = y_i T$. 将 (ID_i, Y_i, d_i, q_i) 添加到 L_1, 并将 $H_1(ID_i, Y_i) = q_i$ 返回给 $\mathcal{A}_{II}$.

③ 公钥询问：$\mathcal{C}$ 维持表 L_{PK} 记录并响应 $\mathcal{A}_{II}$ 的公钥询问. $\mathcal{A}_{II}$ 关于 ID_i $(1 \le i \le q_K)$ 的每次公钥询问, $\mathcal{C}$ 首先查看表 L_{PK}. 如果表 L_{PK} 中含有项 (ID_i, Y_i, X_i, x_i), 将 $P_i = (X_i, Y_i)$ 返回给 $\mathcal{A}_{II}$ 作为身份 ID_i 的公钥. 否则, 如果 $i = N$, 即 $ID_i = ID_N = ID^*$, 令 $x_{ID^*} = x_N = \perp$, $X_{ID^*} = X_N = aP$, 即用 a(未知) 模拟用户 ID^* 的秘密值; 如果 $i \ne N$, 随机选择 $x_i \in_R Z_n^*$, 计算 $X_i = x_i P$. 查询表 L_1, 取得 Y_i. $\mathcal{C}$ 将 (ID_i, X_i, Y_i, x_i) 添加到 L_{PK}, 并将 $PK_i = (X_i, Y_i)$ 返回给 $\mathcal{A}_{II}$.

④ 部分私钥询问：对 $\mathcal{A}_{II}$ 关于 ID_i $(1 \le i \le q_E)$ 的部分私钥询问 (假设已经做过关于 $(ID_i, *)$ 的 H_1 询问, 否则先执行 H_1 询问), $\mathcal{C}$ 从表 L_1 中找出项 (ID_i, Y_i, d_i, q_i), 将 d_i 返回给 $\mathcal{A}_{II}$.

⑤ 秘密值询问：对 $\mathcal{A}_{II}$ 关于 ID_i $(1 \le i \le q_{SV})$ 的秘密值询问 (假设已经做过关于 ID_i 的公钥询问, 否则先执行公钥询问), 如果 $ID_i = ID^*$, $\mathcal{C}$ 宣告失败, 算法终止; 否则, 即 $ID_i \ne ID^*$, $\mathcal{C}$ 从表 L_{PK} 中找出项 (ID_i, Y_i, X_i, x_i), 将 x_i 返回给 $\mathcal{A}_{II}$.

伪造. 如果算法 $\mathcal{C}$ 没有终止, 则 $\mathcal{A}_{II}$ 在未做过 ID^* 的秘密值询问及 (ID^*, m, c) 的签名询问的情况下, 以一个不可忽略的概率输出身份为 ID^* 的用户对消息 m 和公共信息 c 的部分盲签名 (ID^*, m, c, L, w). 根据 Forking 引理 [12], 通过对 $\mathcal{A}_{II}$ 的 H_2 询问施行散列重放, $\mathcal{C}$ 可以获得 (ID^*, m, c) 的两个有效部分盲签名 $(ID^*, m, c, L, w_i, h_i)$, $i = 1, 2$, 其中 $h_1 \ne h_2$. 于是

$$L + h_i T = w_i \left(X_{ID^*} + t_{ID^*}(Y_{ID^*} + q_{ID^*} P_0) + zT\right), \ i = 1, 2$$

两式相减, 可解得

$$X_{ID^*} = (w_1 - w_2)^{-1}(h_1 - h_2)T - (t_{ID^*}(Y_{ID^*} + q_{ID^*} P_0) + zT)$$

其中, $X_{ID^*} = aT$, $Y_{ID^*} + q_{ID^*} P_0 = d_{ID^*} T$, 所以

$$a = (w_1 - w_2)^{-1}(h_1 - h_2) - (t_{ID^*} d_{ID^*} + z)$$

即为 ECDLP 的解.

所以, 在 ECDLP 问题困难的假设下, 改进方案对敌手 $\mathcal{A}_{II}$ 的自适应选择消息和身份攻击是存在性不可伪造的.

2) 盲性

定理 3 改进的无证书部分盲签名方案满足盲性.

证明 下面证明在任意一组签名发布交互过程中签名者私自保存的中间变量和任意一个合法的盲签名之间一定存在盲化因子.

对于任意一个公布的合法部分盲签名 (ID, m, c, L, w) 和任意一组签名者私自保存的签名发布交互过程中的中间变量 (r, R, u, v), 其中 $R = rT$. 考虑以下三个关系式

$$L = \alpha R + \alpha\beta z T \tag{1}$$

$$u = \alpha^{-1} h + \beta z \tag{2}$$

$$w = \alpha v \tag{3}$$

其中 α, $\beta \in Z_n^*$, $h = H_2(m, c, L)$, $z = H_3(c)$.

由式 (3) 可知存在唯一的 $\alpha \in Z_n^*$, 即 $\alpha = wv^{-1}$. 由式 (2) 知存在唯一的 $\beta \in Z_n^*$, 即 $\beta = (u - \alpha^{-1}h)z^{-1}$.

因 (ID, m, c, L, w) 是一个有效的部分盲签名, 所以满足验证等式

$$L + hT = w(X_A + t_A Y_A + t_A q_A P_0 + zT)$$

其中, $t_A = H_4(X_A)$. 另一方面, 签名发布协议执行过程中的中间变量 (r, R, u, v) 满足 $v = (r + u)/(x_A + t_A d_A + z)$, 于是

$$\begin{aligned} \alpha R + \alpha\beta z T =& \alpha r T + (\alpha u - h)T = \alpha(r + u)T - hT \\ =& wv^{-1}(r + u)T - hT = w(x_A + t_A d_A + z)T - hT \\ =& w\left(X_A + t_A(Y_A + q_A P_0) + zT\right) - hT = L \end{aligned}$$

表明由 (2), (3) 式确定的 α, β 满足 (1) 式.

所以, 在任意一组中间变量和任意一个盲签名之间一定可以确定一组盲化因子 $\alpha, \beta \in Z_q^*$. 换句话说, 即使具有无穷的计算能力, 签名者也无法将某个有效盲签名与其某一次签名发布过程相联系, 当然也就无法追踪用户. 所以改进方案满足盲性要求.

4.2 性能分析

将改进方案与其他无证书部分盲签名方案 [6-11] 进行性能比较. 各方案中主要涉及到的运算有群 G(或 $E(F_p)$) 中的标量乘运算, 群 G_T 中的幂乘运算, MapToPoint 散列运算, Z_n^* 中的求逆运算, 以及双线性对运算, 分别用 M, E, H, I, P 表示. 其中, 双线性对的运算效率要明显低于其他运算. 各个方案在签名和验证阶段所使用的各种运算的次数如表 1 所示. 可以看出, 改进方案在克服公钥替换攻击的同时, 仅仅比文献 [11] 方案增加了一次群 G 中的标量乘运算. 由于没有使用双线性对运算, 所以计算性能要明显优于文献 [6-10] 方案.

表 1 各种方案的计算性能比较

方案	签名		验证	总运算量
	(签名者)	(用户)		
文献 [6] 方案	$2M$	$3M$+$1I$	$4P$+$1M$	$4P$+$6M$+$1I$
文献 [7] 方案	$1P$+$1M$+$1E$	$1P$+$1M$+$2E$	$2P$+$2E$	$4P$+$2M$+$5E$
文献 [8] 方案	$3M$	$2P$+$3M$+$1E$	$3P$+$1E$	$5P$+$6M$+$2E$
文献 [9] 方案	$1M$+$1E$	$1M$+$2E$	$1P$+$1M$+$1E$	$1P$+$3M$+$4E$
文献 [10] 方案	$1P$+$1H$+$4M$+$1E$	$2P$+$1H$+$3M$+$1E$	$2P$+$2H$+$1M$+$1E$	$5P$+$4H$+$8M$+$3E$
文献 [11] 方案	$1M$+$1I$	$2M$+$1I$	$4M$	$7M$+$2I$
本文方案	$1M$+$1I$	$2M$+$1I$	$5M$	$8M$+$2I$

5 结束语

对邵国金等人 [11] 提出的基于椭圆曲线离散对数问题的无双线性对运算的部分盲签名方案进行了安全性分析, 结果显示方案不能抵抗公钥替换攻击. 对其进行了改进, 并对改进方

案进行了详细的安全性分析. 分析结果表明, 改进方案能够有效抵抗公钥替换攻击. 由于方案没有使用双线性对运算, 所以计算性能具有明显的优势.

参考文献

[1] Chaum D. Blind signatures for untraceable payments[C]// Advances in Cryptology-CRYPTO' 82. New York: Plenum Press, 1983, 199-203.

[2] Abe M, Fujisaki E. How to date blind signatures[C]// Advances in Cryptology-ASIACRYPTO'96. LNCS 1163, Berlin: Springer- Verlag, 1996: 244-251.

[3] Shamir A. Identity-based cryptosystems and signature schemes[C] //Advances in Cryptology-CRYPTO'84. Berlin: Springer-Verlag, 1984, 47-53.

[4] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]//Advances in Cryptology–ASIACRYPT' 03, LNCS 2894. Berlin: Springer-Verlag, 2003, 452-473.

[5] 张福泰, 孙银霞, 张磊, 等. 无证书公钥密码体制研究 [J]. 软件学报, 2011, 22(6): 1316-1332.

[6] 荣维坚. 无证书部分盲签名方案 [J]. 漳州师范学院学报 (自然科学版). 2008, 21(4): 44-47.

[7] 余丹, 杨晓元, 黄大威. 新的无证书部分盲签名方案 [J]. 计算机应用研究. 2010, 27(11): 4319-4321.

[8] Zhang L, Zhang F, Qin B, et al. Provably-secure electronic cash based on certificateless partially-blind signatures[J]. Electronic Commerce Research and Applications, 2011, 5(10): 545-552.

[9] 汤鹏志, 李晓雄, 左黎明, 等. 高效安全无证书部分盲签名 [J]. 计算机工程与设计. 2013, 34(2): 439-446.

[10] Liu J, Zhang Z, Sun R, et al. Certificateless Partially Blind Signature[C]//Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on. IEEE, 2012: 128-133.

[11] 邵国金, 薛冰, 陈明. 基于椭圆曲线 DLP 问题的无证书部分盲签名机制 [J]. 四川大学学报 (工程科学版), 2012, 44(1): 112-117.

[12] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361–396.

Cryptanalysis and Improvement of an Identity-Based Signature Algorithm Without Certificate

ZHANG Xue-feng[1], HE Jun-jie[2], QI Chuan-da[2]

(1. Department of Computer Science, Xinyang Agricultural College, Xinyang 464000, China)
(2. College of Mathematics and Information Science, Xinyang Normal University, Xinyang 464000, China)

Abstract: Security analysis of the certificateless partially blind signature scheme based on the elliptic curve discrete logarithm problem which is proposed by Shao G J et al. shows that the scheme is insecure against public key replacement attack. An improved scheme was proposed. The improved scheme was proved to be existentially unforgeable against adaptive chosen message and identity attacks in random oracle model. Efficiency analysis results show that the improved scheme has better computational efficiency.

Keywords: partially blind signature; certificateless cryptography; elliptic curve; discrete logarithm; random oracle model