

一个无证书签名方案的分析与改进

何俊杰*, 王娟, 祁传达

(信阳师范学院 数学与信息科学学院, 河南 信阳 464000)

(*通信作者电子邮箱 hejj99@163.com)

摘要:对郭玲玲等(郭玲玲, 林昌露, 张胜元. 针对一类无证书签名方案的攻击及改进. 计算机工程, 2012, 38(16): 134-137, 141)提出的无证书签名方案进行安全性分析, 结果表明方案不能抵抗公钥替换攻击。为此, 提出了一种改进方案。在随机预言机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的, 其安全性可归结为计算 Diffie-Hellman 问题。与其他基于双线性对的无证书签名方案相比, 改进方案具有较高的运算效率。

关键词:数字签名; 无证书签名; 双线性对; 公钥替换攻击; 随机预言机模型

中图分类号: TP309.2 **文献标志码:** A

Cryptanalysis and improvement of a certificateless signature scheme

HE Junjie*, WANG Juan, QI Chuanda

(College of Mathematics and Information Science, Xinyang Normal University, Xinyang Henan 464000, China)

Abstract: Security analysis of the certificateless signature scheme proposed by Guo L L, et al. (Guo L L, Lin C L, Zhang S Y. Attack and improvement for certificateless signature scheme. Computer Engineering, 2012, 38(16): 134-137, 141) showed that the scheme was insecure against public key replacement attack. An improved scheme which can resist public key replacement attack was proposed. The scheme was proved to be existentially unforgeable against adaptive chosen message and identity attacks in random oracle model, and the security was reduced to computational Diffie-Hellman assumption. Compared with other certificateless signature schemes based on bilinear pairing, the improved scheme has better computational efficiency.

Key words: digital signature; certificateless signature; bilinear pairing; public key replacement attack; random oracle model

0 引言

1984年, Shamir^[1]提出了基于身份公钥密码体制。在基于身份的密码体制中, 用户私钥由密钥生成中心(Key Generator Center, KGC)利用系统主密钥统一生成。基于身份公钥密码体制虽然较好地解决了传统公钥密码系统中公钥证书的存储和管理问题, 但却带来了新的安全隐患——密钥托管问题。KGC拥有系统主密钥, 可以生成所有用户的私钥, 恶意的KGC可以冒充任意一个用户进行加解密或签名活动。甚至在严重情况下, 如果系统主密钥泄露, 将会导致整个公钥体系崩溃。

Al-Riyami等^[2]在2003年的亚密会上提出了无证书的公钥密码体制模型。无证书公钥密码体制不需要公钥证书, 同时消除了基于身份公钥系统中的密钥托管问题^[3]。Al-Riyami等^[2]利用椭圆曲线上的双线性对构造了第一个无证书签名方案, 但Huang等^[4]指出该方案不能抵抗公钥替换攻击。随后, Zhang等^[5]和Huang等^[6]分别对无证书签名方案的安全模型做了讨论。2007年, Liu等^[7]提出了第一个具体的标准模型下可证明安全的无证书签名方案。2008年, 刘景伟等^[8]提出了一种高效的基于ID的无证书签名方案, 但吴晨煌等^[9]指出方案不能抵抗替换公钥攻击。2010年, He等^[10]提出了一个不使用对运算的无证书签名方案, 但Tian

等^[11]指出方案不能抵抗类型II敌手的攻击。最近, 夏峰等^[12]提出了公钥不可替换攻击无证书签名体制。2009年, 苏万力等^[13]基于双线性对设计了一个无证书签名方案, 但郭玲玲等^[14]分析证明了该方案无法抵抗公钥替换攻击, 同时提出一个改进方案, 并在随机预言机模型下证明了改进方案具有选择消息攻击下的存在不可伪造性。

本文对文献[14]所提出的改进方案进行安全性分析, 发现文献[14]方案的不可伪造性的证明是错误的, 方案并不能抵抗公钥替换攻击。针对这个安全缺陷, 本文提出了一种改进方案, 并对改进方案进行了安全性分析, 结果表明在随机预言机模型和计算Diffie-Hellman问题困难的假设下, 改进方案对两类敌手(可以替换公钥的不诚实用户和恶意但被动的KGC)的自适应选择消息和身份攻击是存在性不可伪造的。

1 数学基础

1.1 双线性对

设 $(G_1, +)$ 是一个阶为素数 q 的加法群, (G_2, \cdot) 是一个阶为 q 的乘法群, 假定在群 G_1 和 G_2 中的离散对数问题是难解的。称映射 $e: G_1 \times G_1 \rightarrow G_2$ 是一个双线性对, 如果满足下面三条性质:

1) 双线性性: 对于任何 $U, V \in G_1, a, b \in \mathbb{Z}_q^*$, 有 $e(aU, bV) = e(U, V)^{ab}$;

收稿日期: 2012-10-29; 修回日期: 2012-11-29。 基金项目: 国家自然科学基金资助项目(61272465); 河南省自然科学基金资助项目(102102210242, 122400450189); 河南省教育厅科学技术研究重点项目(12A520034)。

作者简介: 何俊杰(1981-), 男, 安徽庐江人, 讲师, 硕士, CCF会员, 主要研究方向: 信息安全; 王娟(1978-), 女, 河南唐河人, 副教授, 博士, 主要研究方向: 非线性系统; 祁传达(1964-), 男, 河南固始人, 教授, 博士, 主要研究方向: 密码理论。

2) 非退化性:存在 $U, V \in G_1$, 使得 $e(U, V) \neq 1$;

3) 可计算性:对于任何的 $U, V \in G_1$, 存在一个高效的算法来计算 $e(U, V)$ 的值。

群 G_1 一般可取有限域上超椭圆曲线或超奇异椭圆曲线, 双线性对则可以通过改进 Weil 配对或 Tate 配对来实现。

1.2 相关数学难题

下面考虑群 G 中的困难性问题与假设。设 P 是 G 的一个生成元。

1) 离散对数问题 (Discrete Logarithm Problem, DLP): 任取 $Q \in G$, 求满足 $Q = xP$ 的整数 $x \in \mathbb{Z}_q^*$ 。

2) 计算 Diffie-Hellman 问题 (Computational Diffie-Hellman Problem, CDHP): 任给 $aP, bP \in G (a, b \in \mathbb{Z}_q^*)$, 计算 abP 。

3) 判定 Diffie-Hellman 问题 (Decisional Diffie-Hellman Problem, DDHP): 任给 $aP, bP, cP \in G (a, b, c \in \mathbb{Z}_q^*)$, 判断 $c = ab \bmod p$ 是否成立。若等式成立, 则称 (P, aP, bP, cP) 是一个有效的 Diffie-Hellman 组。

如果在群 G 上, DDHP 容易但 CDHP 困难, 则 G 称为间隙 Diffie-Hellman 群 (Gap Diffie-Hellman Group, GDH 群)。本文中, 假定 G_1 是 GDH 群。

2 无证书签名方案的安全模型

无证书签名系统中有两类敌手, 即类型 I 敌手 A_I 与类型 II 敌手 A_{II} 。其中: 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; 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。

3 对文献[14]方案的安全性分析

3.1 方案回顾

1) 系统建立。产生系统参数和主密钥, KGC 做如下操作: 选取 2 个 q 阶加法循环群 G_1 和乘法循环群 G_2 , 任意选取 G_1 的一个生成元 P , 并且选取一个双线性对 $e: G_1 \times G_1 \rightarrow G_2$; 选取任意的 $s \in \mathbb{Z}_q^*$ 作为主密钥, 并且计算系统公钥 $P_{pub} = sP$; 选取 2 个加密哈希函数 $H_1: \{0, 1\}^* \times G_1 \rightarrow G_1$ 和 $H_2: \{0, 1\}^* \times \{0, 1\}^* \times G_1 \times G_1 \rightarrow \mathbb{Z}_q^*$ 。系统公开参数为 $\{G_1, G_2, q, e, P, P_{pub}, H_1, H_2\}$, 主密钥 s 由 KGC 保管。

2) 部分私钥提取。KGC 为用户 A 产生部分私钥 $D_A = sQ_A$, 其中 $Q_A = H_1(ID_A, P)$, 并通过安全信道将 D_A 传送给用户。

3) 设置秘密值。用户 A 随机选择 $x_A \in \mathbb{Z}_q^*$ 作为秘密值。

4) 完全私钥生成。用户 A 产生自己的完全私钥 $S_A = (x_A, D_A)$ 。

5) 公钥生成。用户 A 产生自己的公钥 $PK_A = x_AP$ 。

6) 签名。用户 A 输入系统公开参数、身份 ID_A 、消息 $m \in \{0, 1\}^*$ 和私钥 $S_A = (x_A, D_A)$, 进行签名操作: 选取任意的 $r \in \mathbb{Z}_q^*$, 计算 $U = rP, h = H_2(m, ID_A, PK_A, U), V = D_A + (hx_A + r)Q_A$; 输出签名 $\sigma = (U, V)$ 。

7) 验证。验证者接收到用户 A 发送的消息 m 及签名 $\sigma = (U, V)$, 利用消息 m 、用户身份 ID_A 及用户的公钥 PK_A 进行验证操作: 计算 $Q_A = H_1(ID_A, P), h = H_2(m, ID_A, PK_A, U)$; 当且仅当等式 $e(V, P) = e(Q_A, P_{pub} + hPK_A + U)$ 成立时, 接受签名。

3.2 公钥替换攻击

郭玲玲等^[14]在随机预言机模型下使用预言重放技术^[15]

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攻击下的存在性伪造。但通过分析发现, 郭等对方案的不可伪造性的证明是错误的, 方案并不能抵抗公钥替换攻击。敌手 A_I 为了伪造身份为 ID_A 的用户对任意的消息 m 的签名, 可以进行如下操作:

1) 敌手 A_I 随机选取 $\delta \in \mathbb{Z}_q^*$, 计算 $PK_A^* = \delta P$, 用 $PK_A^* = \delta P$ 代替用户 A 的公钥;

2) 随机选取 $\tau \in \mathbb{Z}_q^*$, 计算 $U^* = \tau P - P_{pub}, h^* = H_2(m, ID_A, PK_A^*, U^*)$ 和 $V^* = (\delta h^* + \tau)Q_A$ 。

则 $\sigma^* = (U^*, V^*)$ 是敌手 A_I 假冒身份为 ID_A 的用户对消息 m 伪造的有效签名。事实上,

$$\begin{aligned} e(Q_A, P_{pub} + h^* PK_A^* + U^*) &= \\ e(Q_A, P_{pub} + h^* \delta P + \tau P - P_{pub}) &= \\ e(Q_A, (h^* \delta + \tau)P) &= \\ e((h^* \delta + \tau)Q_A, P) &= e(V^*, P) \end{aligned}$$

说明 $\sigma^* = (U^*, V^*)$ 满足验证方程, 是有效的签名。

4 对文献[14]方案的改进

为了抵抗敌手 A_I 的公钥替换攻击, 本文对文献[14]方案提出了一个改进措施。改进方案的部分私钥提取、设置秘密值、完全私钥生成和公钥生成算法与文献[14]方案相同, 见 3.1 节。系统建立、签名和验证算法描述如下:

1) 系统建立。KGC 选取 q 阶加法循环群 G_1 和 q 阶乘法循环群 G_2 , 任意选取 G_1 的一个生成元 P , 并选择双线性对 $e: G_1 \times G_1 \rightarrow G_2$; 随机选取 $s \in \mathbb{Z}_q^*$ 作为系统主密钥, 计算系统公钥 $P_{pub} = sP$; 选取 3 个安全的哈希函数 $H_1: \{0, 1\}^* \times G_1 \rightarrow G_1$ 、 $H_2: \{0, 1\}^* \times G_1 \times G_1 \rightarrow \mathbb{Z}_q^*$ 和 $H_3: \{0, 1\}^* \rightarrow G_1$ 。系统公开参数为 $\{G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3\}$, KGC 秘密保管主密钥 s 。

2) 签名。用户选取任意的 $r \in \mathbb{Z}_q^*$, 计算 $U = rP, h = H_2(m, ID_A, PK_A, U), V = D_A + (hx_A + r)H_3(ID_A)$, 输出签名 $\sigma = (U, V)$ 。

3) 验证。验证者收到用户 A 发送的消息 m 及签名 $\sigma = (U, V)$ 后, 计算 $Q_A = H_1(ID_A, P), h = H_2(m, ID_A, PK_A, U)$; 验证等式 $e(V, P) = e(Q_A, P_{pub})e(H_3(ID_A), hPK_A + U)$ 是否成立, 若成立, 则接受签名; 否则签名无效。

可以验证, 改进的无证书签名方案是正确的。事实上,

$$\begin{aligned} e(V, P) &= e(D_A + (hx_A + r)H_3(ID_A), P) = \\ e(sQ_A, P)e((hx_A + r)H_3(ID_A), P) &= \\ e(Q_A, sP)e(H_3(ID_A), hx_AP + rP) &= \\ e(Q_A, P_{pub})e(H_3(ID_A), hPK_A + U) \end{aligned}$$

5 改进方案的分析

5.1 安全性分析

定理 1 在随机预言模型和 CDHP 困难的假设下, 改进的无证书签名方案对敌手 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 (挑战者) B 收到 G_1 中 CDHP 实例 (P, aP, bP) , 其中随机数 $a, b \in \mathbb{Z}_q^*$ 未知, 算法 B 调用敌手 A_I 为子程序计算 abP 。

系统设置 B 生成系统公开参数 $params$ 并发送给敌手 A_I , 其中系统公钥设置为 $P_{pub} = aP$, 即用 a 模拟系统主密钥。

询问 A_I 可以适应性地向 B 进行多项式有界次的询问。

简单起见,假设所有的询问都是互不相同的。 B 随机选取整数 $n(1 \leq n \leq q_K)$, 记 $ID_n = ID^*$ 。

1) 公钥询问: B 维护列表 L_K 响应 A_I 的公钥询问。 A_I 关于 $ID_i(1 \leq i \leq q_K)$ 的每次询问, B 首先检查列表 L_K 。如果在列表 L_K 中已经存在项 (ID_i, x_i, P_i) , 将 P_i 返回给 A_I 作为身份 ID_i 的公钥。否则, 也就是 A_I 从来没做过 ID_i 的公钥询问, 则随机选取 $x_i \in_R \mathbf{Z}_q^*$, 计算 $P_i = x_i P_0$ 。将 (ID_i, x_i, P_i) 添加到列表 L_K , 并将 P_i 返回给 A_I 。

2) H_1 询问: B 维护列表 L_1 响应 A_I 的 H_1 询问。 A_I 关于 $(ID_i, P)(1 \leq i \leq q_1)$ 的每次询问, B 首先检查列表 L_1 。如果在 L_1 中已经存在项 (ID_i, P, Q_i, c_i) , B 将 Q_i 返回给 A_I 作为 (ID_i, P) 的 H_1 哈希值。否则, 如果 $i = n$, 即 $ID_i = ID_n = ID^*$, 令 $Q_n = bP$; 如果 $i \neq n$, 随机选取 $c_i \in_R \mathbf{Z}_q^*$, 计算 $Q_i = c_i P_0$ 将 (ID_i, P, Q_i, c_i) 添加到 L_1 , 并将 $H_1(ID_i, P) = Q_i$ 返回给 A_I 。

3) H_2 询问: B 维护列表 L_2 响应 A_I 的 H_2 询问。 A_I 关于 $(m_i, ID_i, P_i, U_i)(1 \leq i \leq q_2)$ 的每次询问, B 首先检查列表 L_2 。如果在 L_2 中已经存在项 $(m_i, ID_i, P_i, U_i, h_i)$, B 将 h_i 返回给 A_I 作为 (m_i, ID_i, PK_i, U_i) 的 H_2 哈希值; 否则, 随机选取 $h_i \in_R \mathbf{Z}_q^*$, 将 $(m_i, ID_i, P_i, U_i, h_i)$ 添加到 L_2 , 并将 $H_2(m_i, ID_i, PK_i, U_i) = h_i$ 返回给 A_I 。

4) H_3 询问: B 维护列表 L_3 响应 A_I 的 H_3 询问。 A_I 关于 $ID_i(1 \leq i \leq q_3)$ 的每次询问, B 首先检查列表 L_3 。如果在 L_3 中已经存在项 (ID_i, d_i, R_i) , B 将 R_i 返回给 A_I 作为 ID_i 的 H_3 哈希值; 否则, 随机选取 $d_i \in_R \mathbf{Z}_q^*$, 计算 $R_i = d_i(aP)$, 将 (ID_i, d_i, R_i) 添加到 L_3 , 并将 $H_3(ID_i) = R_i$ 返回给 A_I 。

5) 部分私钥询问: 对 A_I 关于 $ID_i(1 \leq i \leq q_E)$ 的部分私钥询问(假设已经做过关于 (ID_i, P) 的 H_1 询问, 否则先执行 H_1 询问), 如果 $ID_i = ID^*$, B 宣告失败, 算法终止; 否则, 即 $ID_i \neq ID^*$, B 从列表 L_1 中找出项 (ID_i, P, Q_i, c_i) , 计算 $D_i = c_i(aP)$, 将 D_i 返回给 A_I 。

6) 秘密值询问: 对 A_I 关于 $ID_i(1 \leq i \leq q_{SV})$ 的秘密值询问, B 首先检查列表 L_K 。如果在 L_K 中已经存在项 (ID_i, x_i, P_i) , B 将 x_i 返回给 A_I 作为 ID_i 的秘密值; 否则, 随机选取 $x_i \in_R \mathbf{Z}_q^*$, 将 (ID_i, x_i, P_i) 添加到 L_K , 并将 x_i 返回给 A_I 。

7) 公钥替换询问: 对 A_I 关于 $(ID_i, PK_i^*)(1 \leq i \leq q_{RP})$ 的公钥替换询问, B 首先检查列表 L_K 。如果在 L_K 中已经存在项 (ID_i, x_i, P_i) , 则令 $x_i = \perp, P_i = PK_i^*$; 否则将 (ID_i, \perp, PK_i^*) 添加到 L_K 。

8) 签名询问: B 维护列表 L_S 响应 A_I 的签名询问。 A_I 可以选择消息 m 和身份 ID , 对 (ID, m) 进行签名询问(假设已经做过关于 ID 的公钥询问和 H_3 询问及 (ID, P_{ID}) 的 H_1 询问, 否则先执行公钥询问、 H_1 询问和 H_3 询问)。

如果 $ID \neq ID^*$, B 从列表 L_K 中找出项 (ID, x_{ID}, P_{ID}) , 从列表 L_1 中找出项 (ID, P, Q_{ID}, c) , 从列表 L_3 中找出项 (ID, d, R) ; 任取 $h, u \in_R \mathbf{Z}_q^*$, 计算 $U = uP - hP_{ID}$, 如果 (m, ID, P_{ID}, U, h) 已经在列表 L_2 中, 则重新选取 h, u 并计算 U ; 计算 $V = (c + du)P_{pub}$; 将 (m, ID, P_{ID}, U, h) 加到列表 L_2 , 并将 $\sigma(ID, m) = (U, V)$ 返回给 A_I 。 B 所产生的签名是有效的。事实上,

$$\begin{aligned} e(V, P) &= e((c + du)P_{pub}, P) = \\ &= e(cP_{pub}, P)e(duP_{pub}, P) = \\ &= e(P_{pub}, cP)e(d(aP), uP) = \\ &= e(P_{pub}, Q_{ID})e(H_3(ID), U + hP_{ID}) \end{aligned}$$

如果 $ID = ID^*$, 即 $ID = ID_n$, B 首先在 L_1 中找到 $(ID, P,$

$Q_{ID^*}, c_n)$, 其中 $Q_{ID^*} = bP$, 从列表 L_K 中找出项 $(ID^*, x_{ID^*}, P_{ID^*})$, 从列表 L_3 中找出项 (ID^*, d_n, R_n) ; 任意选取 $\tau, h \in_R \mathbf{Z}_q^*$, 计算 $U = d_n^{-1}(\tau P - Q_{ID^*}) - hP_{ID^*}$, 如果 $(m, ID^*, P_{ID^*}, U, h)$ 已经在列表 L_2 中, 则重新选取 τ, h 并计算 U ; 计算 $V = \tau P_{pub}$; 将 $(m, ID^*, P_{ID^*}, U, h)$ 加到列表 L_2 中。并将 $\sigma(ID^*, m) = (U, V)$ 返回给 A_I 。 B 所产生的签名也是有效的。事实上,

$$\begin{aligned} e(Q_{ID^*}, P_{pub})e(H_3(ID^*), hP_{ID^*} + U) &= \\ e(Q_{ID^*}, P_{pub})e(d_n P_{pub}, d_n^{-1}(\tau P - Q_{ID^*})) &= \\ e(\tau P, P_{pub}) &= e(\tau P_{pub}, P) = e(V, P) \end{aligned}$$

伪造 如果算法 B 没有终止, 则 A_I 在没有做过 (ID^*, m^*) 的签名询问和部分私钥询问的条件下, 以一个不可忽略的概率对一个输入消息 m^* 输出一个身份 ID^* 对应的有效签名 (U, V) 。根据 Forking 引理^[15-16], 通过对 A_I 哈希重放, B 可以获得对消息 m 的两个有效签名 (ID^*, m^*, U, h, V) 和 (ID^*, m^*, U, h', V') , 其中 $U = rP, h \neq h'$ 。因为有效签名满足 $V = D_{ID^*} + (hx_{ID^*} + r)H_3(ID^*)$, 所以:

$$\begin{aligned} V &= D_{ID^*} + (hx_{ID^*} + r)H_3(ID^*) \\ V' &= D_{ID^*} + (h'x_{ID^*} + r)H_3(ID^*) \end{aligned}$$

于是

$$\begin{aligned} hh'x_{ID^*}H_3(ID^*) &= h'(V - D_{ID^*} - rH_3(ID^*)) = \\ &= h(V' - D_{ID^*} - rH_3(ID^*)) \end{aligned}$$

所以

$$D_{ID^*} = (h' - h)^{-1}(h'V - hV' + (h - h')rH_3(ID^*))$$

而 $D_{ID^*} = aQ_{ID^*} = aH(ID^*, P_{ID^*}) = abP$, 即为 CDHP 的解。所以, 在 CDHP 困难的假设下, 改进方案对敌手 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 在随机预言模型和 CDH 困难的假设下, 改进的无证书签名方案对敌手 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(挑战者) C 收到 G_1 中 CDHP 实例 (P, aP, bP) , 其中随机数 $a, b \in \mathbf{Z}_q^*$ 未知, 算法 C 调用 A_{II} 为子程序计算 abP 。

系统设置 C 随机选择 $s \in \mathbf{Z}_q^*$ 作为系统主密钥, 生成系统公共参数 $params$, 其中 $P_{pub} = sP$, 将 $params$ 和 s 发送给敌手 A_{II} 。

询问 A_{II} 可以适应性地向 B 进行多项式有界次的询问。其中 H_2 询问和 H_3 询问与定理1相同。简单起见, 假设所有的询问都是互不相同的。 B 随机选取整数 $n(1 \leq n \leq q_K)$, 记 $ID_n = ID^*$ 。

1) 公钥询问: C 维护列表 L_K 响应 A_{II} 的公钥询问。 A_{II} 关于 $ID_i(1 \leq i \leq q_K)$ 的每次询问, B 首先检查列表 L_K 。如果在列表 L_K 中已经存在项 (ID_i, x_i, P_i) , 将 P_i 返回给 A_I 作为身份 ID_i 的公钥。否则, 如果 $i = n$, 即 $ID_i = ID_n = ID^*$, 令 $x_n = \perp, P_n = bP$, 即用 $x_{ID^*} = b$ (未知) 模拟用户 ID^* 的秘密值; 如果 $i \neq n$, 随机选取 $x_i \in_R \mathbf{Z}_q^*$, 计算 $P_i = x_i P_0$ 。将 (ID_i, x_i, P_i) 添加到 L_K , 并将 P_i 返回给 A_{II} 。

2) H_1 询问: C 维护列表 L_1 响应 A_{II} 的 H_1 询问。 A_{II} 关于 $(ID_i, P)(1 \leq i \leq q_1)$ 的每次询问, C 首先检查列表 L_1 。如果在 L_1 中已经存在项 (ID_i, P, Q_i, c_i) , B 将 Q_i 返回给 A_{II} 作为 (ID_i, P) 的 H_1 哈希值。否则, 随机选取 $c_i \in_R \mathbf{Z}_q^*$, 计算 $Q_i = c_i P_0$ 。将 (ID_i, P, Q_i, c_i) 添加到 L_1 , 并将 $H_1(ID_i, P) = Q_i$ 返回给 A_{II} 。

3) 秘密值询问: 对 A_{II} 关于 $ID_i(1 \leq i \leq q_{SV})$ 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 $ID_i = ID^*$, C 宣告失败,算法终止;否则,即 $ID_i \neq ID^*$, C 从列表 L_K 中找出项 (ID_i, x_i, P_i) , 将 x_i 返回给 A_{II} 。

4) 签名询问: C 维护列表 L_S 响应 A_{II} 的签名询问。 A_{II} 可以选择消息 m 和身份 ID , 对 (ID, m) 进行签名询问(假设已经做过关于 ID 的公钥询问和 H_3 询问及 (ID, P_{ID}) 的 H_1 询问, 否则先执行公钥询问、 H_1 询问和 H_3 询问)。如果 $ID \neq ID^*$, C 可获得 ID 的部分私钥 D_{ID} 和秘密值 x_{ID} , 然后简单地运行签名算法即可生成签名。如果 $ID = ID^*$, 即 $ID = ID_n$, C 首先在 L_1 中找到 (ID^*, P, Q_{ID^*}, c_n) , 从列表 L_K 中找出项 (ID^*, \perp, P_{ID^*}) , 从列表 L_3 中找出项 (ID^*, d_n, R_n) ; 任意选取 $\tau, h \in_R \mathbb{Z}_q^*$, 计算 $U = \tau P - hP_{ID^*}$, 如果 $(m, ID^*, P_{ID^*}, U, h)$ 已经在列表 L_2 中, 则重新选取 τ, h 并计算 U ; 计算 $V = sQ_{ID^*} + \tau R_n$; 将 $(m, ID^*, P_{ID^*}, U, h)$ 加到列表 L_2 中, 并将 $\sigma(ID, m) = (U, V)$ 返回给 A_{II} 。 C 所产生的签名是有效的。事实上,

$$e(Q_{ID^*}, P_{pub})e(H_3(ID^*), hP_{ID^*} + U) = e(Q_{ID^*}, sP)e(R_n, \tau P) = e(P, sQ_{ID^*} + \tau R_n) = e(V, P)$$

伪造 如果算法 C 没有终止, 则 A_{II} 在未做过 (ID^*, m^*) 的签名询问和秘密值询问的条件下, 以一个不可忽略的概率对一个输入消息 m^* 输出一个身份 ID^* 对应的有效签名 (U, V) 。根据 Forking 引理^[15-16], 通过对 A_{II} 哈希重放, C 可以获得对消息 m 的两个有效签名 (ID^*, m^*, U, h, V) 和 (ID^*, m^*, U, h', V') , 其中 $U = rP, h \neq h'$ 。由

$$V = D_{ID^*} + (hx_{ID^*} + r)H_3(ID^*) \\ V' = D_{ID^*} + (h'x_{ID^*} + r)H_3(ID^*)$$

得 $D_{ID^*} = V - (hx_{ID^*} + r)H_3(ID^*) = V' - (h'x_{ID^*} + r)H_3(ID^*)$, 所以 $x_{ID^*}H_3(ID^*) = (h' - h)^{-1}(V - V')$ 。而 $x_{ID^*}H_3(ID^*) = bd_n(aP) = d_n(abP)$, 则 $abP = d_n^{-1}(h' - h)^{-1}(V - V')$ 为 CDHP 的解。

所以, 在 CDHP 困难的假设下, 改进方案对敌手 A_{II} 的自适应选择消息和身份攻击也是存在性不可伪造的。

5.2 性能分析

将改进的新方案与已有的无证书签名方案^[2,5-6,14]进行计算性能方面的比较。重点考虑计算消耗比较大的运算, 主要包括双线性对运算、群 G_1 中的标量乘运算、群 G_2 中的幂乘运算和 MapToPoint 哈希运算, 分别用 P, M, E 和 H 表示。具体比较数据如表 1 所示, 其中括号中的数据是预运算量。

表 1 本文无证书签名方案与已有相似方案的性能比较

方案	签名(预计算)	验证阶段(预计算)
文献[2]方案	$2M + 1E(1P)$	$4P + 1M + 1E$
文献[5]方案	$2M$	$2P + 2M + 1H(2P + 2M)$
文献[6]方案 1	$1M + 1H$	$3P + 1H(2P + 1H)$
文献[6]方案 2	$3M + 1E$	$2P + 2M + 1E + 1H(1P + 2M + 1E)$
文献[14]方案	$2M$	$2P + 1M(1H)$
本文方案	$2M(1H)$	$2P + 1M(1P + 2H)$

具体到本文方案, 签名和验证过程中的哈希运算 $Q_A = H_1(ID_A, P), H_3(ID_A)$ 和对运算 $e(Q_A, P_{pub})$ 都可以预先计算, 在实际签名实施过程中并不会增加运算量。

可以看出, 本文方案在克服公钥替换攻击的同时并没有比郭等无证书签名方案^[14]增加运算量, 而且比文献^[2,5-6]中的方案或多或少都减少了运算量。

6 结语

本文对郭玲玲等^[14]提出的无证书签名方案进行了安全

性分析, 指出方案不能抵抗公钥替换攻击。针对郭等方案的安全缺陷, 提出了一种改进方案, 并对新方案进行了详细的安全性分析。新方案能够有效抵抗两类敌手的自适应选择消息和身份的伪造攻击; 同时, 新方案中使用了较多的预运算, 使得方案具有较高的执行效率。

参考文献:

- [1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology - Crypto'84. New York: Springer-Verlag, 1984: 47-53.
- [2] 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.
- [3] 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.
- [4] HUANG X Y, SUSILO W, MU Y, et al. On the security of certificateless signature schemes from Asiacrypt 2003 [C]// CANS 2005: Cryptology and Network Security, LNCS 3810. Berlin: Springer-Verlag, 2005: 13-25.
- [5] ZHANG Z F, WONG D S, XU J, et al. Certificateless public-key signature: Security model and efficient construction [C]// ACNS 2006: Applied Cryptography and Network Security, LNCS 3989. Berlin: Springer-Verlag, 2006: 293-308.
- [6] HUANG X Y, MU Y, SUSILO W, et al. Certificateless signature revisited [C]// Information Security and Privacy, ACISP 2007, LNCS 4586. Berlin: Springer-Verlag, 2007: 308-322.
- [7] LIU J K, AU M H, SUSILO W. Self-generated-certificate public key cryptography and certificateless signature/ encryption scheme in the standard model [C]// Proceedings of the 2007 ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2007: 273-283.
- [8] 刘景伟, 孙蓉, 马文平. 高效的基于 ID 的无证书签名方案 [J]. 通信学报, 2008, 29(2): 87-94.
- [9] 吴晨煌, 梁红梅, 陈智雄, 等. 一个高效的基于 ID 的无证书签名方案的安全性分析及改进 [J]. 漳州师范学院学报: 自然科学版, 2009, 22(1): 26-29.
- [10] HE D B, CHEN J H, ZHANG R. Efficient and provably-secure certificateless signature scheme without bilinear pairings [EB/OL]. (2010-02-20) [2012-10-15]. <http://eprint.iacr.org/2010/632.pdf>.
- [11] TIAN M M, HUANG L S. Cryptanalysis of a certificateless signature scheme without pairings [J/OL]. International Journal of Communication Systems, 2012, 1-7. doi: 10.1002/dac.2310. [2012-10-15]. <http://onlinelibrary.wiley.com/doi/10.1002/dac.2310/full>.
- [12] 夏峰, 杨波. 公钥不可替换无证书签名方案 [J]. 计算机科学, 2012, 39(8): 92-95.
- [13] 苏万力, 李晖, 张跃宇, 等. 一种有效的无证书签名方案 [J]. 江苏大学学报, 2009, 30(4): 401-404.
- [14] 郭玲玲, 林昌露, 张胜元. 针对一类无证书签名方案的攻击及改进 [J]. 计算机工程, 2012, 38(16): 134-137, 141.
- [15] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures [J]. Journal of Cryptology, 2000, 13(3): 361-396.
- [16] RAFAEL C, RICARDO D. Two notes on the security of certificateless signatures [C]// Proceedings of First International Conference on Provable Security. Berlin: Springer-Verlag, 2007: 85-102.