·安全技术· 文章编号: 1000-3428(2015)07-0171-06 文献标识码: A 中图分类号: TP309

一种不含双线性对的无证书盲签名方案

何俊杰[1],张雪峰[2],祁传达[1]

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

摘 要: 为简化传统公钥密码系统中的证书管理过程,消除基于身份公钥密码系统中的密钥托管隐患,提出一种新的无证书盲签名方案,在随机预言模型中对适应性选择消息及身份攻击是存在性不可伪造的,且方案安全性可以归约为离散对数问题的难解性。分析结果表明,与现有签名算法与验证算法相比,该方案由于没有使用耗时较多的双线性对运算和MapToPoint散列函数运算,在计算性能上具有明显优势。

关键词: 盲签名; 无证书密码体制; 椭圆曲线; 离散对数; 随机预言模型; 双线性对; 盲性

中文引用格式: 何俊杰,张雪峰,祁传达. 一种不含双线性对的无证书盲签名方案[J]. 计算机工程,2015,41(7):171-176.

英文引用格式: He Junjie, Zhang Xuefeng, Qi Chuanda. A Certificateless Blind Signature Scheme Without Bilinear Pairing[J]. Computer Engineering, 2015, 41(7): 171-176.

A Certificateless Blind Signature Scheme Without Bilinear Pairing

HE Junjie[1], ZHANG Xuefeng[2], QI Chuanda[1]

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

【Abstract】 In order to simplify the certificate management process in the traditional public key cryptosystem and eliminate the security vulnerability brought by the key escrow problem in the identity-based public key cryptosystem, a new certificateless blind signature scheme without pairings is proposed. The scheme is proved to be existentially unforgeable against adaptive chosen message and identity attacks in the random oracle model, and the security is reduced to the hardness of the discrete logarithm problem. Analysis results show that compared with the signature and verification algorithm of many other certificateless blind signature schemes, the proposed scheme has obvious advantages in computational efficiency because of no time-consuming bilinear pairing operation and inefficient MapToPoint hash function.

【Key words】 blind signature; certificateless cryptosystem; elliptic curve; discrete logarithm; random oracle model; bilinear pairing; blindness

DOI: 10.3969/j.issn.1000-3428.2015.07.033

1 概述

1984年,Shamir[1]提出了基于身份的公钥密码体制(ID-PKC)。在ID-PKC中,用户的公钥可以由公开的身份信息直接生成,不需要统一存储,从而简化了传统公钥密码系统中公钥证书的存储和管理问题。但是用户的私钥由密钥生成中心(Key Generation Center,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[2]提出了无证书的公钥密码体制(CL-PKC)。在CL-PKC中,用户私钥由KGC和用户共同生成,既消除了ID-PKC中的密钥托管问题,又不需要使用公钥证书。自无证书公钥密码体制提出以来,很多学者陆续设计了各种无证书签名方案。1982年,Chuam[3]提出盲签名的概念。盲签名能让签名者在不知道待签消息内容的情况下对消息进行签名,签名者也无法将最终公布的签名与自己保留的签名过程联系起来。盲签名可有效保护用户的隐私,被广泛应用于电子投票和电子现金等场合。

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(142300410320);河南省教育厅科学技术研究基金资助项目(14B520046);信阳师范学院青年基金资助项目(2013-QN-060)。

作者简介:何俊杰(1981-),男,讲师、硕士,主研方向:信息安全;张雪峰,讲师、硕士;祁传达,教授、博士。

收稿日期:2014-06-25 修回日期:2014-08-25 E-mail: hejj99@163.com

将盲签名技术和无证书公钥密码体制相结合，很多学者提出了无证书盲签名方案。2008 年，Zhang L 等人[4] 基于计算 Diffie-Hellman 问题(CDHP)提出了一个无证书盲签名方案。2010 年，Zhang J Z 等人[5] 基于 CDHP 和双线性对逆问题(BPIP)设计了一个可证安全的无证书盲签名方案，但文献[7]却利用公钥替换攻击证明了文献[6]方案是不安全的。2013 年，汤鹏志等人[7] 提出了一个无证书的部分盲签名方案方案，只在验证阶段使用了一次双线性对运算，但文献[8]指出不能抵抗篡改协商信息攻击。这些方案都使用了计算开销较高的双线性对运算，执行效率普遍不高。为了提高运算效率，很多学者开始关注不使用双线性对运算的无证书部分盲签名方案的构造。2011 年，薛冰等人[9] 基于离散对数问题(DLP)和 CDHP 假设构造了一个无需对运算的无证书部分盲签名方案。2012 年，邵国金等人[10] 基于椭圆曲线 DLP 问题提出了一种无证书部分盲签名算法，也没有使用双线性对操作。2014 年，Dong G 等人[11] 提出了一个新的不含对运算的无证书盲签名方案。这些方案由于没有使用双线性对操作，计算效率得到了很大的提升。

本文提出一种新的不含双线性对的无证书盲签名方案，并对该方案做了详细的安全性分析和效率比较。

2 预备知识

2.1 离散对数问题

设 p 是一个大素数，G 是 p 阶加法循环群，P 是 G 的一个生成元。

(1) 离散对数问题(DLP)：对任意的 $Q \in G$，计算 a，使得 $Q = aP$。

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

$$Adv^{\mathrm{DLP}}(\mathcal{A}) = \Pr[\mathcal{A}(P,Q) = a \mid Q = aP, a \in Z_p^*]$$

是可以忽略的。

2.2 无证书盲签名的安全模型

2.2.1 不可伪造性

无证书公钥密码系统中一般有 2 类攻击者。第Ⅰ类攻击者 $\mathcal{A}_{\mathrm{I}}$ 可以任意替换任何用户的公钥，但不能获得系统主密钥。这类攻击者主要用来模拟不诚实的用户。第Ⅱ类攻击者 $\mathcal{A}_{\mathrm{II}}$ 不能替换目标用户的公钥，但能够获取系统主密钥，当然也就可以产生所有用户的部分私钥。这类攻击者主要用来模拟恶意但被动的 KGC。

无证书盲签名方案的不可伪造性可用下面的挑战者 $\mathcal{C}$ 和攻击者 A_{I} 或 A_{II} 间的 2 个游戏来刻画。

游戏 1(适用于第 1 类攻击者 $\mathcal{A}_{\mathrm{I}}$)

系统初始化：$\mathcal{C}$ 运行系统建立算法，输入安全参数 k，输出系统主密钥 s 和公开参数 $params$。$\mathcal{C}$ 将系统主密钥 s 保密，将 $params$ 发送给 $\mathcal{A}_{\mathrm{I}}$。

攻击：$\mathcal{A}_{\mathrm{I}}$ 可以适应性地进行多项式有界次的询问：

(1) 秘密值询问：$\mathcal{A}_{\mathrm{I}}$ 输入身份 ID 进行秘密值询问，$\mathcal{C}$ 运行设置秘密值算法输出对应的秘密值 x_{ID}，并返回给 $\mathcal{A}_{\mathrm{I}}$。

(2) 公钥询问：$\mathcal{A}_{\mathrm{I}}$ 输入身份 ID 进行公钥询问，$\mathcal{C}$ 运行设置公钥算法输出公钥 pk_{ID}，并返回给 $\mathcal{A}_{\mathrm{I}}$。

(3) 部分私钥询问：$\mathcal{A}_{\mathrm{I}}$ 输入身份 ID 进行部分私钥询问，$\mathcal{C}$ 运行部分私钥提取算法输出部分私钥 D_{ID}，并返回给 $\mathcal{A}_{\mathrm{I}}$。

(4) 公钥替换询问：$\mathcal{A}_{\mathrm{I}}$ 输入身份 ID 和 $\mathrm{pk}_{\mathrm{ID}}^*$，要求替换原公钥 $\mathrm{pk}_{\mathrm{ID}}$，$\mathcal{C}$ 完成用户 ID 的公钥替换并记录。

(5) 签名询问：$\mathcal{A}_{\mathrm{I}}$ 输入身份 ID 和消息 m，$\mathcal{C}$ 用当前公钥(无论是否被替换)对应的私钥对 m 签名，并把签名结果返回给 $\mathcal{A}_{\mathrm{I}}$。

伪造：$\mathcal{A}_{\mathrm{I}}$ 输出一个四元组 $(m^*, \sigma^*, ID^*, pk^*)$。

如果四元组 $(m^*, \sigma^*, ID^*, pk^*)$ 可以通过签名验证且 $\mathcal{A}_{\mathrm{I}}$ 未询问过身份 ID^* 的部分私钥和身份为 ID^*、公钥为 pk^* 的用户对 m^* 的盲签名，则攻击者 $\mathcal{A}_{\mathrm{I}}$ 在游戏 1 中获胜。

游戏 2(适用于第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$)

系统初始化：$\mathcal{C}$ 运行系统建立算法，输入安全参数 k，输出系统主密钥 s 和公开参数 $params$。$\mathcal{C}$ 将 $params$ 和 s 都发送给 $\mathcal{A}_{\mathrm{II}}$。

攻击：$\mathcal{A}_{\mathrm{II}}$ 可以适应性地进行多项式有界次的秘密值询问、公钥询问、公钥替换询问和签名询问，具体与游戏 1 相同。

伪造：$\mathcal{A}_{\mathrm{II}}$ 输出一个四元组 $(m^*, \sigma^*, ID^*, pk^*)$。

如果四元组 $(m^*, \sigma^*, ID^*, pk^*)$ 可以通过签名验证，$\mathcal{A}_{\mathrm{II}}$ 未询问过身份 ID^* 的秘密值和身份为 ID^*、公钥为 pk^* 的用户对 m^* 的盲签名，且 $\mathcal{A}_{\mathrm{II}}$ 没有替换用户 ID^* 的公钥，则攻击者 $\mathcal{A}_{\mathrm{II}}$ 在游戏 2 中获胜。

定义 1 一个无证书盲签名方案在适应性选择消息攻击下是存在不可伪造的，当且仅当，在多项式时间内，2 类攻击者 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 赢得以上 2 个游戏的概率是可以忽略的。

2.2.2 盲性

盲性不仅是指签名过程时签名者对消息的不可见，还包括签名者对签名的不可追踪性。无证书盲签名方案的盲性可用下面的游戏 3 来刻画。

游戏 3(盲性游戏)

系统初始化: $\mathcal{C}$ 运行系统建立算法,输入安全参数 k,输出系统公开参数 $params$。$\mathcal{C}$ 将 $params$ 发送给 $\mathcal{A}$。

挑战: $\mathcal{A}$ 选择 2 个严格区分的消息 m_0, m_1,并发送给 $\mathcal{C}$。$\mathcal{C}$ 随机选择 $b \in_R \{0,1\}$,将 m_b 发送给 u_0,将 m_{1-b} 发送给 u_1,其中 u_0, u_1 是 2 个诚实的用户。敌手 $\mathcal{A}$ 与用户 u_0, u_1 交互对消息 m_b, m_{1-b} 进行签名,最后得到签名 $\mathrm{sig}(m_b)$ 和 $\mathrm{sig}(m_{1-b})$,并将 $(m_b, \mathrm{sig}(m_b))$ 和 $(m_{1-b}, \mathrm{sig}(m_{1-b}))$ 发送给 $\mathcal{A}$。

猜测: $\mathcal{A}$ 执行多项式有界次的询问后,输出对 b 的猜测 b',如果 $b' = b$,则 $\mathcal{A}$ 赢得游戏。

敌手 $\mathcal{A}$ 赢得盲性游戏的优势定义为:

$$Adv(\mathcal{A}) = |2\Pr(b' = b) - 1|$$

定义 2 称一个盲签名方案具有盲性,指的是不存在多项式时间内的攻击者能以不可忽略的优势赢得盲性游戏。

3 新的无证书盲签名方案

无证书盲签名方案过程如下:

(1) 系统建立

给定安全参数 1^k,KGC 选取 p 阶加法循环群 G,其中 p 为素数,任取 G 的一个生成元 P; 随机选择 $s \in Z_p^*$ 作为系统主密钥,计算系统公钥 $P_{\mathrm{pub}} = sP$; 选取 3 个安全的散列函数: $H_1: \{0,1\}^* \times G \to Z_p^*$, $H_2: \{0,1\}^* \times G \to Z_p^*$ 和 $H_3: G \to Z_p^*$; 系统参数为 $Params = \{G_1, p, P, P_{\mathrm{pub}}, H_1, H_2, H_3\}$,在系统内公开; 系统主密钥 s 由 KGC 秘密保存。

(2) 部分私钥提取

签名者 A 提交其身份 ID_A 给 KGC,KGC 选择随机数 $y_A \in Z_p^*$,计算 $Y_A = y_A P, q_A = H_1(ID_A, Y_A)$ 和 $d_A = y_A + sq_A \bmod p$ 并返回 d_A 作为 A 的部分私钥,Y_A 作为 A 的部分公钥。

(3) 设置秘密值

签名者 A 秘密选取 $x_A \in_R Z_p^*$,将 x_A 作为用户 A 的秘密值秘密保管。

(4) 设置公钥

签名者 A 计算 $X_A = x_A P$,输出公钥 $P_A = (X_A, Y_A)$。

(5) 设置私钥

签名者 A 输出其私钥 $S_A = (x_A, d_A)$。

(6) 签名发布

设 m 是待签名的消息,c 是双方事先共同协商的公共信息,用户和签名者 A 进行如下交互:

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

盲化: 用户选择随机数 $\alpha, \beta \in Z_p^*$,计算 $S = \alpha R + \alpha\beta P, h = H_2(m, S)$ 和 $u = (\alpha^{-1} h + \beta) \bmod p$,然后发送 u 给 A。

签名(阶段 2): 签名者 A 计算 $z_A = H_3(X_A)$ 和 $v = (r + u)(x_A + z_A d_A)^{-1} \bmod p$,将 v 发送给用户。

去盲: 用户收到 v 后,计算 $w = \alpha v$,获得消息 m 的盲签名 (S, w)。

(7) 验证

验证者收到消息 m 的盲签名 (S, w) 后,计算 $z_A = H_3(X_A)$, $q_A = H(ID_A, Y_A)$ 和 $h = H_2(m, S)$,验证: $S + hP = w(X_A + z_A Y_A + z_A q_A P_{\mathrm{pub}})$ 是否成立。如果等式成立,则盲签名有效,否则,盲签名无效。

因为:

$$\begin{aligned} w(X_A + z_A Y_A + z_A q_A P_{\mathrm{pub}}) &= \\ \alpha v(x_A + z_A(y_A + q_A s))P &= \\ \alpha(r + u)(x_A + z_A d_A)^{-1}(x_A + z_A d_A)P &= \\ \alpha(r + \alpha^{-1} h + \beta)P &= \\ \alpha r P + (h + \alpha\beta)P &= \\ \alpha R + \alpha\beta P + hP &= S + hP \end{aligned}$$

即 (m, S, w) 满足验证等式,是有效的盲签名。所以,所提方案是正确的。

4 安全性分析

4.1 不可伪造性

定理 1 在随机预言模型下,所提方案对敌手 $\mathcal{A}_{\mathrm{I}}$ 的自适应选择消息和身份攻击是存在性不可伪造的,其安全性依赖于群 G 中的 DLP 的难解性。

证明: 设算法 $\mathcal{C}$ 是解决 DLP 的挑战者,即给定 (P, aP),其中 $a \in Z_p^*$ 未知,目标是计算 a。下面证明,如果存在敌手 $\mathcal{A}_{\mathrm{I}}$ 以不可忽略的概率成功伪造盲签名,则挑战者 $\mathcal{C}$ 可以计算出 a。

(1) 系统设置

算法 $\mathcal{C}$ 生成系统参数 $params = \{G_1, p, P, P_{\mathrm{pub}}, H_1, H_2, H_3\}$,其中,系统公钥设置为 $P_0 = aP$,即用 a 模拟系统主密钥,但 $\mathcal{C}$ 不知道 a 的值。$\mathcal{C}$ 将 $params$ 发送给敌手 A_I。

(2) 询问

$\mathcal{A}_{\mathrm{I}}$ 适应性地向 $\mathcal{C}$ 进行多项式有界次的询问。$\mathcal{C}$ 选择随机数整数 $n(1 \leqslant n \leqslant q_{PK})$,记 $ID_n = ID^*$。

1) H_1 询问: $\mathcal{C}$ 维持列表 L_1 记录并响应 A_I 的 H_1 询问。$\mathcal{A}_{\mathrm{I}}$ 关于 $(ID_i, *)$ $(1 \leqslant i \leqslant q_1)$ 的每次 H_1 询问,$\mathcal{C}$ 首先查找表 L_1,如果 L_1 中含有项 (ID_i, Y_i, d_i, q_i),则将 q_i 返回给 $\mathcal{A}_{\mathrm{I}}$ 作为 (ID_i, Y_i) 的 H_1 散列值。否则,如果 $ID_i = ID^*$,令 $d_i = \perp$; 选择随机数 $y_i, d_i \in Z_p^*$,计算 $Y_i = y_i P$; 如果 $ID_i \neq ID^*$,选择随机数 $d_i, q_i \in Z_p^*$,计算 $Y_i = d_i P - q_i(aP)$。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 $\mathcal{A}_{\mathrm{I}}$。

2) H_2 询问: $\mathcal{C}$ 维持列表 L_2 记录并响应 A_I 的 H_2 询问。A_I 关于 (m_i, S_i) $(1 \leqslant i \leqslant q_2)$ 的每次 H_2 询问,$\mathcal{C}$ 首先查看列表 L_2。如果 L_2 中含有项 (m_i, S_i, h_i),

则将 h_i 返回给$\mathcal{A}_{\mathrm{I}}$作为(m_i,S_i)的 H_2 散列值;否则,选择随机数 $h_i\in Z_p^*$,将(m_i,S_i,h_i)添加到 L_2,并将 $H_2(m_i,S_i)=h_i$ 返回给$\mathcal{A}_{\mathrm{I}}$。

3) H_3 询问:$\mathcal{C}$维持列表 L_3 记录并响应$\mathcal{A}_{\mathrm{I}}$的 H_3 询问。$\mathcal{A}_{\mathrm{I}}$关于 $X_i(1\leqslant i\leqslant q_3)$的每次 H_3 询问,$\mathcal{C}$首先查看列表 L_3。如果 L_3 中含有项(X_i,z_i),则将 z_i 返回给$\mathcal{A}_{\mathrm{I}}$作为 X_i 的 H_3 散列值;否则,选择随机数 $z_i\in Z_p^*$,将(X_i,z_i)添加到 L_3,并将 $H_3(X_i)=z_i$ 返回给$\mathcal{A}_{\mathrm{I}}$。

4) 公钥询问:$\mathcal{C}$维持列表 L_{PK}记录并响应$\mathcal{A}_{\mathrm{I}}$的公钥询问。$\mathcal{A}_{\mathrm{I}}$关于 $ID_i(1\leqslant i\leqslant q_{PK})$的每次公钥询问,$\mathcal{C}$首先查看列表 L_{PK}。如果 L_{PK}中含有项(ID_i,Y_i,X_i,x_i),则将 $P_i=(Y_i,X_i)$作为用户 ID_i 的公钥并返回给$\mathcal{A}_{\mathrm{I}}$。否则,说明$\mathcal{A}_{\mathrm{I}}$未对 ID_i 进行过公钥询问,则选择随机数 $x_i\in_R Z_p^*$,计算 $X_i=x_iP$;查询 L_1,获得 Y_i;将(ID_i,Y_i,X_i,x_i)添加到列表 L_{PK},并将$P_i=(Y_i,X_i)$返回给$\mathcal{A}_{\mathrm{I}}$。

5) 部分私钥询问:对$\mathcal{A}_{\mathrm{I}}$关于 $ID_i(1\leqslant i\leqslant q_E)$的部分私钥询问,如果 $ID_i=ID^*$,$\mathcal{C}$宣告失败,算法终止;如果 $ID_i\neq ID^*$,$\mathcal{C}$从列表 L_1 中找出项(ID_i,Y_i,d_i,q_i),将 d_i 返回给$\mathcal{A}_{\mathrm{I}}$。如果 L_1 中不存在项(ID_i,Y_i,d_i,q_i),说明未做过关于$(ID_i,*)$的 H_1 询问,则先执行 H_1 询问。

6) 秘密值询问:对$\mathcal{A}_{\mathrm{I}}$关于 $ID_i(1\leqslant i\leqslant q_{SV})$的秘密值询问,$\mathcal{C}$首先查找表 L_{PK}。如果 L_{PK}中含有项(ID_i,Y_i,X_i,x_i),则将 x_i 返回给$\mathcal{A}_{\mathrm{I}}$作为身份为 ID_i 的用户的秘密值;否则,$\mathcal{C}$首先执行对 ID_i 的公钥询问,并将 x_i 返回给$\mathcal{A}_{\mathrm{I}}$。

7) 公钥替换询问:对关于$(ID_i,P_i^*=(Y_i^*,X_i^*))$$(1\leqslant i\leqslant q_{RP})$的公钥替换询问,$\mathcal{C}$首先查找表 L_{PK}。如果在 L_{PK}中已经含有项(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}。

8) 签名询问:$\mathcal{C}$维持列表 L_S 记录并响应$\mathcal{A}_{\mathrm{I}}$的签名询问。A_I 选择身份 ID 和消息 m,向$\mathcal{C}$ 询问(ID,m)的签名。假设已经执行过关于 ID 的公钥询问,关于(ID,Y_{ID})的 H_1 询问和关于 X_{ID}的 H_3 询问,否则先进行这些询问。$\mathcal{C}$ 从列表 L_{PK}中找出项$(ID,Y_{ID},X_{ID},x_{ID})$,从列表 L_1 中找出项$(ID,Y_{ID},d_{ID},q_{ID})$,从列表 L_3 中找出项(X_{ID},z_{ID})。

$\mathcal{C}$任意选取 $h,w\in Z_n^*$,计算 $S=w(X_{ID}+z_{ID}Y_{ID}+z_{ID}q_{ID}P_{pub})-hP$,如果$(m,S,h)$已经含于列表 L_2 中,则重新选择 h,w 并计算 S;将(m,S,h)加到列表 L_2,并将(S,w)作为身份 ID 对消息 m 的盲签名返回给 A_I。

(3) 伪造

如果算法$\mathcal{C}$没有停止,则$\mathcal{A}_{\mathrm{I}}$在没有进行过(ID^*,m)的签名询问及 ID^* 的部分私钥询问的情况下,以不可忽略的概率输出身份为 ID^* 的用户对消息 m 的合法盲签名(ID^*,m,S,w)。根据 *Forking* 引理[12],通过对$\mathcal{A}_{\mathrm{I}}$的 H_2 询问和 H_3 询问进行重放,$\mathcal{C}$可以得到(ID^*,m)的 3 个有效盲签名(ID^*,m,S,w_i,h_i,z_i),$i=1,2,3$,其中 z_1,z_2,z_3 互不相同。于是:

$$S+h_iP=w_i(X_{ID^*}+z_i(Y_{ID^*}+q_{ID^*}P_{\mathrm{pub}}))$$
$$i=1,2,3$$

其中,$Y_i=y_iP$。这 3 个等式可以看成是关于 S,X_{ID^*}和 P_{pub}的线性方程组:

$$S-w_iX_{ID^*}-w_iz_iq_{ID^*}P_{\mathrm{Pub}}=(w_iz_iy_i-h_i)P$$
$$i=1,2,3$$

可以解出:

$$P_{\mathrm{pub}}=\frac{(w_1-w_2)(b_3-b_1)-(w_1-w_3)(b_2-b_1)}{(w_1-w_2)(a_3-a_1)-(w_1-w_3)(a_2-a_1)}P$$

其中,$a_i=w_iz_iq_{ID^*}$;$b_i=w_iz_iy_i-h_i$,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 DLP 的解。

所以,如果 DLP 困难,则所提方案可以抵抗敌手$\mathcal{A}_{\mathrm{I}}$的自适应选择消息和身份下的存在性伪造攻击。

定理 2 在随机预言模型下,所提方案对敌手$\mathcal{A}_{\mathrm{II}}$的自适应选择消息和身份攻击是存在性不可伪造的,其安全性依赖于群 G 中的 *DLP* 的难解性。。

证明: 设算法$\mathcal{C}$是解决 DLP 的挑战者,即给定(P,aP),其中,$a\in Z_p^*$ 未知,目标是计算 a。下面证明如果存在敌手$\mathcal{A}_{\mathrm{II}}$以不可忽略的概率成功伪造盲签名,则挑战者$\mathcal{C}$可以计算出 a。

(1) 系统设置

$\mathcal{C}$选择随机数 $s\in Z_p^*$ 作为系统主密钥,生成系统公开参数 $params=\{G_1,p,P,P_{\mathrm{pub}},H_1,H_2,H_3\}$,其中,系统公钥 $P_{\mathrm{pub}}=sP$。将 $params$ 和 s 发送给敌手$\mathcal{A}_{\mathrm{II}}$。

(2) 询问

$\mathcal{A}_{\mathrm{II}}$适应性地向$\mathcal{C}$进行多项式有界次的询问。$\mathcal{C}$随机选择整数 $n(1\leqslant n\leqslant q_{PK})$,记 $ID_n=ID^*$。H_2 询问、H_3 询问以及签名询问与定理 1 相同。

1) H_1 询问:$\mathcal{A}_{\mathrm{II}}$关于$(ID_i,*)$$(1\leqslant i\leqslant q_1)$的每次 H_1 询问,$\mathcal{C}$首先查找表 L_1。如果 L_1 中含有项(ID_i,Y_i,d_i,q_i),则将 q_i 返回给$\mathcal{A}_{\mathrm{II}}$作为$(ID_i,Y_i)$的 H_1 散列值。否则,选择随机数 $y_i,d_i\in Z_n^*$,计算 $Y_i=y_iP$。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$\mathcal{A}_{\mathrm{II}}$。

2) 公钥询问:$\mathcal{A}_{\mathrm{II}}$关于 $ID_i(1\leqslant i\leqslant q_K)$的每次公钥询问,$\mathcal{C}$首先查找表 L_{PK}。如果 L_{PK}中含有项$(ID_i,$

$Y_i, X_i, x_i)$，则将 $P_i = (X_i, Y_i)$ 返回给 A_{II} 作为身份为 ID_i 的用户的公钥。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 $i \neq n$，选择随机数 $x_i \in_R Z_p^*$，计算 $X_i = x_i P$。查询列表 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 A_{II}。

3）部分私钥询问：对 $\mathcal{A}_{\text{II}}$ 关于 $ID_i (1 \leqslant i \leqslant q_E)$ 的部分私钥询问，$\mathcal{C}$ 从列表 L_1 中找出项 (ID_i, Y_i, d_i, q_i)，将 d_i 返回给 A_I。如果没做过关于 $(ID_i, *)$ 的 H_1 询问，则先执行 H_1 询问。

4）秘密值询问：对 $\mathcal{A}_{\text{II}}$ 关于 $ID_i (1 \leqslant i \leqslant q_{SV})$ 的秘密值询问，如果 $ID_i = ID^*$，$\mathcal{C}$ 挑战失败，算法终止；否则，即 $ID_i \neq ID^*$，$\mathcal{C}$ 从列表 L_{PK} 中找出项 (ID_i, Y_i, X_i, x_i)，将 x_i 返回给 $\mathcal{A}_{\text{II}}$。如果没做过关于 ID_i 的公钥询问，则先执行公钥询问。

（3）伪造

如果算法 $\mathcal{C}$ 没有停止，则 $\mathcal{A}_{\text{II}}$ 在没有进行过 (ID^*, m) 的签名询问和 ID^* 的秘密值询问的情况下，以不可忽略的概率输出用户 ID^* 对消息 m 的盲签名 (ID^*, m, S, w)。对 $\mathcal{A}_{\text{II}}$ 的 H_2 询问进行重放，根据 *Forking* 引理[12]，$\mathcal{C}$ 可获得 (ID^*, m) 的 2 个有效盲签名 (ID^*, m, R, w_i, h_i)，$i = 1, 2$，其中 $h_1 \neq h_2$。于是：

$$S + h_i P = w_i (X_{ID^*} + z_{ID^*} (Y_{ID^*} + q_{ID^*} P_{\text{pub}}))$$
$$i = 1, 2$$

两式相减可得：

$$X_{ID^*} = (w_1 - w_2)^{-1} (h_1 - h_2) P - z_{ID^*} (Y_{ID^*} + q_{ID^*} P_{\text{pub}})$$

其中，$X_{ID^*} = aP$，$Y_{ID^*} + q_{ID^*} P_{\text{pub}} = d_{ID^*} P$，所以，$a = (w_1 - w_2)^{-1} (h_1 - h_2) - z_{ID^*} d_{ID^*}$ 即为 *DLP* 的解。

如果 DLP 困难，则所提方案可以抵抗敌手 $\mathcal{A}_{\text{II}}$ 的自适应选择消息和身份下的存在性伪造攻击。

4.2　方案盲性

定理 3　所提的无证书盲签名方案满足盲性。

证明：对于任意一个公布的合法盲签名 (ID, m, S, 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，$R = rT$。考查以下 3 个关系式：

$$S = \alpha R + \alpha\beta P \quad (1)$$
$$u = \alpha^{-1} h + \beta \quad (2)$$
$$w = \alpha v \quad (3)$$

其中，$\alpha, \beta \in Z_p^*$；$h = H_2(m, S)$。

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

由于 (ID, m, S, w) 是合法的盲签名，因此满足：

$$L + hP = w(X_A + z_A Y_A + z_A q_A P_{\text{pub}})$$

其中，$z_A = H_3(X_A)$。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 $v = \dfrac{(r+u)}{(x_A + z_A d_A)}$，于是：

$$\begin{aligned}\alpha R + \alpha\beta P &= \alpha r P + (\alpha u - h) P = \\ &\alpha (r + u) P - hP = \\ &wv^{-1} (r + u) P - hP = \\ &w(x_A + z_A d_A) P - hP = \\ &w(X_A + z_A (Y_A + q_A P_{\text{pub}})) - hT = S\end{aligned}$$

表明由式（2）、式（3）确定的 α, β 满足式（1）。

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 $\alpha, \beta \in Z_q^*$ 而不会产生矛盾。换句话说，即便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，所提的无证书盲签名方案满足盲性要求。

5　效率分析

将本文方案与其他无证书盲签名方案[4-5,11,13-14]进行计算效率比较。各方案中主要涉及到的运算如表 1 所示，其中，各运算间的效率比较数据来自文献[15]，G_T 为与 G 同阶的乘法循环群，存在 $G \times G$ 到 G_T 的双线性对。可以看出，双线性对的运算效率要明显低于其他运算。各方案在签名发布和验证阶段所使用的各种运算的次数如表 2 所示。可以看出，所提方案在计算性能上具有明显优势。

表 1　各种运算的效率比较

运算	缩写	运算效率
Z_p^* 中的模乘运算	m	–
群 G 中的标量乘运算	M	$1M \approx 29m$
双线性对运算	P	$1P \approx 3M \approx 87m$
群 G_T 中的幂乘运算	E	$1E \approx 1M \approx 29m$
MapToPoint 散列运算	H	$1H \approx 1M \approx 29m$
Z_p^* 中的求逆运算	I	$1I \approx 11.6m$
普通散列运算	h	可以忽略

表 2　各种方案的计算性能比较

方案	签名发布	验证	总运算量
文献[4]方案	$4M + 3E + 1H$	$3P + 1E + 2H + 1I$	$3P + 4M + 4E + 2H + 1I \approx 562.6m$
文献[5]方案	$2M + 3E + 2I$	$1P + 1M + 1E$	$1P + 3M + 4E + 2I \approx 313.2m$
文献[11]方案	$5M + 1I$	$4M$	$9M + 1I \approx 272.6m$
文献[13]方案	$3E + 4M$	$1P + 1E + 1M$	$1P + 4E + 5M \approx 348m$
文献[14]方案	$8M$	$3P$	$3P + 8M \approx 493m$
本文方案	$3M + 2I$	$4M$	$7M + 2I \approx 226.0m$

6 结束语

本文基于无证书公钥密码体制提出一种不含双线性对运算的盲签名方案。在随机预言模型下，证明了该方案对无证书公钥密码系统 2 类敌手的自适应性选择消息及身份攻击都是存在不可伪造的。由于没有使用计算效率低下的双线性对运算，因此本文方案在计算性能上相较于其他无证书盲签名方案具有明显优势。

参考文献

[1] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]//Proceedings of Advances in Cryptology-CRYPTO'84. Berlin, Germany: Springer-Verlag, 1984: 47-53.

[2] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography [C]//Proceedings of Cryptology-ASIACRYPT'03. Berlin, Germany: Springer-Verlag, 2003: 452-473.

[3] Chaum D. Blind Signatures for Untraceable Payments [C]//Proceedings of Advances in Cryptology-CRYPTO'82. New York, USA: Plenum Press, 1983: 199-203.

[4] Zhang L, Zhang F T. Certificateless Signature and Blind Signature [J]. Journal of Electronics, 2008, 25(5): 629-635.

[5] Zhang J H, Gao S N. Efficient Provable Certificateless Blind Signature Scheme [C]//Proceedings of 2010 International Conference on Networking. Washton D. C., USA IEEE Press, 2010: 292-297.

[6] Wu C H, Guo R J, Chen Z X. Public Key Replacement Attack on Two Certificateless Blind Signature Schemes [J]. Journal of Information and Computational Science, 2013, 10(5): 1391-1398.

[7] 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.

[8] 何俊杰，张 帆，邵 辉. 对一个无证书部分盲签名方案的分析与改进 [J]. 信阳师范学院学报：自然科学版，2014，(2)：170-175.

[9] 薛 冰，景伟娜. 无对运算的无证书部分盲签名 [J]. 计算机应用，2011，31(11)：2990-2993.

[10] 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，2012，41(2)：112-117.

[11] Dong G, Gao F, Shi W, et al. An Efficient Certificateless Blind Signature Scheme Without Bilinear Pairing [J]. Anais da Academia Brasileira de Ciências, 2014, 86(2): 1003-1011.

[12] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures [J]. Journal of Cryptology, 2000, 13(3): 361-396.

[13] 黄茹芬，农 强，黄振杰. 一个高效的无证书盲签名方案 [J]. 计算机工程，2013，39(2)：130-136.

[14] 何俊杰，张 帆，祁传达. 新的无可信私钥生成中心的盲签名方案 [J]. 计算机应用，2013，33(4)：1061-1064.

[15] Islam S K H, Biswas G P. A Pairing-free Identity-based Authenticated Group Key Agreement Protocol for Imbalanced Mobile Networks [J]. Annals of Telecommunications-annales Des Télécommunications, 2012, 67(11/12): 547-558.

编辑 索书志

(上接第 170 页)

[6] Lewko A B, Okamoto T, Sahai A, et al. Fully Secure Functional Encryption: Attribute-based Encryption and (Hierarchical) Inner Product Encryption [C]//Proceedings of EUROCRYPT'10. Nice, France: Springer, 2010: 62-91.

[7] Allison B. Lewko and Brent Waters. New Proof Methods for Attribute-based Encryption: Achieving Full Security Through Selective Techniques [C]//Proceedings of CRYPTO'12. Santa Barbara, USA: Springer, 2012: 180-198.

[8] Cheung L, Newport C C. Provably Secure Ciphertext Policy ABE [C]//Proceedings of ACM Conference on Computer and Communications Security. Alexandria, USA: ACM Press, 2007: 456-465.

[9] Garg S, Gentry C, Halevi S, et al. Attribute-based Encryption for Circuits from Multilinear Maps [C]//Proceedings of CRYPTO'13. Santa Barbara, USA: Springer, 2013: 479-499.

[10] Herranz J, Laguillaumie F, R`afols C. Constant Size Ciphertexts in Threshold Attribute-based Encryption [C]//Proceedings of Public Key Cryptography Conference. Paris, France: Springer, 2010: 19-34.

[11] Attrapadung M, Libert B, de Panafieu E. Expressive Key-policy Attribute-based Encryption with Constant-size Ciphertexts [C]//Proceedings of Public Key Cryptography Conference. Taormina, Italy: Springer: 90-108.

[12] Yu Shucheng, Ren Kui, Lou Wenjing, et al. Defending Against Key Abuse Attacks in Kp-abe Enabled Broadcast Systems [C]//Proceedings of Security and Privacy in Communication Networks Conference. Athens, Greece: Springer, 2009: 311-329.

[13] Wang Yongtao, Chen Kefei, et al. Attribute-based Traitor Tracing [J]. Journal of Information Science and Engineering, 2011, 27(1): 181-195.

[14] Liu Zhen, Cao Zhenfu, Wong D S. White-box Traceable Ciphertext-policy Attribute-based Encryption Supporting any Monotone Access Structures [J]. IEEE Transactions on Information Forensics and Security 2013, 8(1): 76-88.

[15] Liu Zhen, Cao Zhenfu, Wong D S. Blackbox Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay [C]//Proceedings of ACM Conference on Computer and Communications Security. Berlin, Germany: ACM Press, 2013: 475-486.

[16] 马海英，曾国荪. 可追踪并撤销叛徒的属性基加密方案 [J]. 计算机学报，2012，35(9)：1845-1855.

[17] 冯登国，陈 成. 属性加密学研究 [J]. 密码学报，2014，1(1)：1-12.

[18] Liber B, Vergnaud D. Towards Practical Black-box Accountable Authority IBE: Weak Black-box Traceability with Short Cipher Texts and Private Keys [J]. IEEE Transactions on Information Theory, 2011, 57(10): 7189-7204.

编辑 索书志