

一类无证书签名方案的构造方法

张 磊 张福泰

(南京师范大学数学与计算机科学学院 南京 210097)

摘 要 无证书密码体制(CL-PKC)是一类新型公钥密码体制,它保持了基于身份的密码体制(ID-PKC)不需要使用公钥证书的优点,又较好地解决了基于身份的公钥体制所固有的密钥托管问题.对无证书体制下安全高效的签名方案的设计方法的研究是受到高度关注的研究课题.文中给出了一类无证书签名方案的构造方法,并在一个很强的安全模型下对用该方法所构造的方案的安全性进行了证明.文中对新构造的方案与已有的一些同类方案的性能进行了比较.结果显示新方案在整体性能上有一定的优势.

关键词 无证书密码系统;计算 Diffie-Hellman 问题;双线性对;无证书签名;随机预言模型

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2009.00940

A Method to Construct a Class of Certificateless Signature Schemes

ZHANG Lei ZHANG Fu-Tai

(College of Mathematics and Computer Science, Nanjing Normal University, Nanjing 210097)

Abstract Certificateless public key cryptography (CL-PKC) is a new paradigm in public key cryptography. It effectively solves the inherent key escrow problem in identity based public key cryptography (ID-PKC) while keeps its certificate free property. Designing efficient and secure signature schemes in certificateless public key setting is an interesting research topic that attracts the attentions of many researchers. This paper proposes a new method to construct a class of certificateless signature schemes. The schemes constructed using the new method can be proven secure in a very strong security model. The overall performances of the authors' newly constructed schemes are better than that of the other certificateless signature schemes available in the literature.

Keywords certificateless public key cryptography; computational Diffie-Hellman problem; bilinear pairing; certificateless signature; random oracle model

1 引 言

在基于证书的传统公钥密码系统下,为了保证系统的安全性,用户的公钥由 CA 颁发的证书进行认证.然而在实际应用中证书的产生、管理、传输、验证等过程不仅复杂而且代价很高.为了简化证书管理过程,降低运行代价,Shamir^[1]在 1984 年首次

提出了基于身份的密码系统.在基于身份的密码系统中不再使用证书来认证用户的公钥,因为用户的公钥就是能唯一代表他身份的一个公开信息,比如说他的电话号码或者 email 地址.在该系统中,用户的私钥需要由一个可信中心(PKG)产生.正是由于这一点,基于身份的密码系统有一个与生俱来的缺陷,那就是密钥托管问题,即 PKG 知道任何用户的私钥.为了解决基于身份的密码系统中的密钥托管

问题, Al-Riyami 和 Paterson^[2] 在 2003 年提出了无证书的密码系统. 在无证书密码系统中用到一个第三方 KGC, 其作用是帮助用户生成自己的私钥. 但是 KGC 并不是生成用户的完整私钥, 而只是生成用户的部分私钥. 用户的完整私钥由用户自己随机选取的一个秘密值以及 KGC 帮他生成的部分私钥结合起来产生. 而用户的公钥由用户自己根据系统参数以及自己的秘密值进行一定运算生成.

数字签名是信息安全中的一个重要工具, 它提供真实性、不可否认性、数据完整性等安全服务. 相对于传统公钥体制和基于身份的公钥体制下的数字签名而言, 无证书签名优势在于: (1) 签名验证者在验证签名时无需像在传统公钥密码系统下那样验证签名者公钥的有效性; (2) 没有基于身份的密码系统中的密钥托管问题. 最早的无证书签名由 Al-Riyami 和 Paterson^[2] 提出, 然而他们对该方案没有给出形式化的安全性证明. 在 ACISP 2005 会议上, Huang 等人^[3] 指出了其中的缺陷, 那就是第 1 类攻击者可以任意伪造签名. 另外, Huang 等人提出了一个修改方案并定义了无证书签名的安全模型. 但该模型并不能完全捕获到第 1 类攻击者的行为, 一个典型的例子就是 Yap 等人的方案^[4]. 该方案在文献[3]中的模型下被证明是安全的, 但事实上, 对它的各种各样的攻击陆续被提出^[5-6]. 同时我们看到, 现有文献中有不少无证书签名方案^[7-9] 的安全性是在这个模型下证明的, 因而这些方案的真正安全性还有待于探讨. 在文献[10]中 Zhang 等人给出了一个改进的安全模型, 并给出了一个高效的签名方案. 文献[11]进一步提出了无证书签名的一个更强的安全模型.

本文研究在目前提出的最强的安全模型下, 高效无证书签名方案的设计. 我们提出了一类无证书签名方案的构造方法. 在这种构造方法下, 所得的签名方案结构简捷运行高效, 并在一定意义下性能优于现有的其它无证书签名方案. 我们的构造基于双线性映射. 其安全性基于一个经典的困难问题——计算 Diffie-Hellman 问题. 同时, 我们在随机预言模型下^[12], 利用文献[11]中的安全模型对所构造的签名方案的安全性进行了证明.

2 预 备

2.1 双线性映射及数学困难问题

假设 G_1 是一个阶为素数 q 的加法群, P 是它的一个生成元; G_2 是一个阶为 q 的乘法群. 若一个映射

$e: G_1 \times G_1 \rightarrow G_2$ 满足以下 3 条性质, 则我们称这个映射为双线性映射.

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

(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.

定义 1. 离散对数问题: 给定一个阶为 q 的循环群 G , 它的一个生成元 g 以及 $h \in G^*$, 找到一个值 $a \in \mathbb{Z}_q^*$ 使得 $h = g^a$.

定义 2. 计算 Diffie-Hellman (CDH) 问题. 给定一个阶为 q 的循环群 G , 它的一个生成元 g 以及 $g^a, g^b \in G_1^*$ (其中 $a, b \in \mathbb{Z}_q^*$ 且其值未知), 计算 g^{ab} .

2.2 无证书签名方案

一个无证书签名方案由系统参数生成、部分密钥生成、设置秘密值、设置私钥、设置公钥、签名以及验证 7 个算法组成. 通常, 前两个算法由 KGC 执行, 而其它算法由签名或验证用户执行. 以下是各个算法的描述.

系统参数生成: 输入安全参数 k , 输出系统主密钥 $master\text{-}key$ 和系统公开参数 $params$. 其中系统公开参数 $params$ 向系统中的全体用户公开, 而主密钥 $master\text{-}key$ 则由 KGC 秘密保存.

部分密钥生成: 输入系统参数 $params$ 、一个用户的身份 ID 和系统主密钥 $master\text{-}key$, KGC 为用户输出部分私钥 D_{ID} .

设置秘密值: 输入系统参数 $params$ 和用户身份 ID 、输出该用户的秘密值 x_{ID} .

设置私钥: 输入系统参数 $params$ 、一个用户的身份 ID 、该用户的秘密值 x_{ID} 和部分私钥 D_{ID} , 输出该用户的私钥 S_{ID} .

设置公钥: 输入系统参数 $params$ 、一个用户的身份 ID 、秘密值 x_{ID} 和部分私钥 D_{ID} , 输出该用户的公钥 P_{ID} .

签名: 输入系统参数 $params$ 、消息 M 、一个用户的身份 ID 、其公钥 P_{ID} 及私钥 S_{ID} , 输出该用户对消息 M 的签名 σ .

验证: 输入系统参数 $params$ 、一个消息 M 、一个签名 σ 、签名者的身份 ID 及公钥 P_{ID} , 当检验签名有效时, 输出 1; 否则, 输出 0.

2.3 安全模型

在无证书系统中有两类攻击者, 即第 1 类攻击者 A_1 与第 2 类攻击者 A_{II} . 第 1 类攻击者不知道系统主密钥, 但是可以任意替换用户的公钥. 第 2 类攻击者知道系统的主密钥, 但是不能替换目标用户的

公钥. 无证书签名方案的安全性可用下面的挑战者 C 和攻击者 A_I 或 A_{II} 间的两个游戏^[11]来定义.

游戏 1(适用于第 1 类攻击者):

初始化: C 运行系统参数生成算法, 输入安全参数 k , 输出系统主密钥 $master\text{-}key$ 和系统参数 $params$. C 将 $params$ 发送给 A_I , 而对主密钥 $master\text{-}key$ 严格保密.

攻击: A_I 可以适应性地进行公钥询问、部份私钥询问、秘密值询问、公钥替换询问以及签名询问, C 模拟签名方案中的相应算法分别做出回答.

伪造: 最后 A_I 输出一个四元组 $(M^*, \sigma^*, ID^*, P^*)$. 我们说 A_I 赢得了这个游戏, 当且仅当:

1. σ^* 是公钥为 P^* 、身份为 ID^* 的用户对消息 M^* 的一个有效签名.
2. A_I 没有询问过身份为 ID^* 的用户的部分私钥.
3. A_I 没有询问过身份为 ID^* 、公钥为 P^* 的用户对 M^* 的签名.

游戏 2(适用于第 2 类攻击者).

初始化: C 运行系统参数生成算法, 输出系统主密钥 $master\text{-}key$ 和系统参数 $params$. C 将 $master\text{-}key$ 和 $params$ 发送给 A_{II} .

攻击: A_{II} 可以适应性地进行公钥询问、秘密值询问、公钥替换询问以及签名询问, C 模拟签名方案中的相应算法分别做出回答.

伪造: 最后 A_{II} 输出一个四元组 $(M^*, \sigma^*, ID^*, P^*)$. 我们说 A_{II} 赢得了这个游戏, 当且仅当:

1. σ^* 是公钥为 P^* 、身份为 ID^* 的用户对消息 M^* 的一个有效签名.
2. A_{II} 没有询问过身份为 ID^* 的用户的秘密值且 A_{II} 没有替换用户 ID^* 的公钥.
3. A_{II} 没有询问过身份为 ID^* 、公钥为 P^* 的用户对 M^* 的签名.

定义 3. 一个无证书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, 任何计算能力多项式受限的攻击者赢得以上两个游戏的概率是可忽略的.

在下文中, 我们说一个签名方案是安全的, 即指它在适应性选择消息攻击下是存在不可伪造的.

3 一类无证书签名方案的构造方法

系统参数生成: 输入一个安全参数 k , KGC 选定满足 2.1 节所述性质的 e, G_1, G_2, P , 并在 Z_q^* 中随机选取系统主密钥 $master\text{-}key = s$, 记 $P_0 = sP$, 选择 Hash 函数 $H_1, H_2: \{0, 1\}^* \rightarrow G_1, H_3: \{0, 1\}^* \rightarrow Z_q^*$, 设置系统参数 $params = \{e, G_1, G_2, P, P_0, H_1, H_2, H_3\}$.

部分私钥生成: KGC 利用系统主密钥帮用户

生成部分私钥. 当输入一个用户的身份 ID , KGC 计算并输出该用户的部分私钥 $D_{ID} = sH_1(ID)$.

设置秘密值: 用户(其身份为 ID) 在 Z_q^* 中随机选取一个值 x 作为其秘密值.

设置公钥: 秘密值为 x 的用户(其身份为 ID) 设置其公钥为 $P_{ID} = xP$.

设置私钥: 身份为 ID 的用户设置其私钥为 $S_{ID} = xU + D_{ID}$, 其中 $U = H_2(ID, P_{ID})$, x 为该用户的秘密值, D_{ID} 为其部分私钥, P_{ID} 为其公钥.

签名: 假设签名者的身份为 ID , 公钥为 $P_{ID} = xP$, 私钥为 $S_{ID} = xU + D_{ID}$. 当输入一个消息 M , 该签名者按以下方式对消息 M 进行签名:

1. 选取 $r \in Z_q^*$, 计算 $R = e(X, P)^r$. 其中 $X \in G_1$ 是一个可以公开计算的值(我们可以令 $X = P, P_0, H_1(ID)$ 等).
2. 计算 $h = H_3(M, ID, R, P_{ID})$, $V = rX + hS_{ID}$.
3. 输出签名 $\sigma = (h, V)$.

验证: 验证者按如下方式验证身份为 ID , 公钥为 P_{ID} 的用户对消息 M 的签名 σ 的有效性:

1. 计算 $U = H_2(ID, P_{ID})$, $Q_{ID} = H_1(ID)$, $R = e(V, P)(e(U, P_{ID})e(Q_{ID}, P_0))^{-h}$.
2. 检验等式 $h \stackrel{?}{=} H_3(M, ID, R, P_{ID})$ 是否成立. 若成立, 则输出 1; 否则输出 0.

4 安全性证明

定理 1. 在随机预言模型下, 若群 G_1 中的 CDH 问题是困难的, 那么用上述方法构造的无证书签名方案对于第 1 类攻击者是安全的.

证明. 假设 C 想解决 G_1 中的 CDH 问题, 其输入为 (aP, bP) , 他需要计算出 abP . 假设 A_I 是第 1 类攻击者, 他能以不可忽略的概率攻破我们的签名方案. 我们看 C 如何利用 A_I 来解决 CDH 问题.

首先, C 设置 $P_0 = aP$, 选择系统参数 $params = \{e, G_1, G_2, P, P_0, H_1, H_2, H_3\}$. 然后 C 将系统参数给 A_I . 这里我们将 Hash 函数 H_1, H_2, H_3 看成随机预言机. 并且为了简单起见, 我们假设以下 A_I 的询问都是不同的.

H_1 询问: C 维护一个列表 H_1^{list} , 开始时, 该列表被初始化为一个空表, 其每一项的格式为 $(ID, \alpha, Q_{ID}, D_{ID})$. 假设 A_I 最多能做 q_{H_1} 次 H_1 询问, C 在 $[1, q_{H_1}]$ 中随机选取一个值 J . 当 C 收到 A_I 对 $H_1(ID_i)$ 的询问时, 若这不是第 J 次询问, C 随机选择 $\alpha_i \in Z_q^*$, 计算 $Q_i = \alpha_i P, D_i = \alpha_i P_0$, 将 $(ID_i, \alpha_i, Q_i, D_i)$ 加入到 H_1^{list} 并将 Q_i 返回给 A_I ; 否则, C 设置 $\alpha_j = D_j = \perp, Q_j = bP$, 将 $(ID_j, \alpha_j, Q_j, D_j)$ 加入到 H_1^{list}

并将 Q_i 返回给 A_1 .

H_2 询问: C 维护一个列表 H_2^{list} , 其每一项的格式为 (ID, P_{ID}, β, U) . 最初, 该列表是空的. 当 A_1 询问 $H_2(ID_i, P_i)$ 时, C 随机选择 $\beta_i \in Z_q^*$, 计算 $U_i = \beta_i P$, 将 $(ID_i, P_i, \beta_i, U_i)$ 加入到 H_2^{list} 并将 U_i 返回给 A_1 .

H_3 询问: C 维护一个列表 H_3^{list} , 其格式为 (M, ID, R, P_{ID}, h) . 最初, 这个列表被初始化为一个空表. 当 A_1 询问 $H_3(M_i, ID_i, R_i, P_i)$ 时, C 随机选择 $h_i \in Z_q^*$, 将 $(M_i, ID_i, R_i, P_i, h_i)$ 加入到 H_3^{list} 并将 h_i 返回给 A_1 .

部分私钥询问: 若 $ID_i = ID_j$, C 终止; 否则检索 H_1^{list} 找到 $(ID_i, \alpha_i, Q_i, D_i)$ 这一项, 将 D_i 返回给 A_1 , 当 $H_1(ID_i)$ 没有询问过时, C 首先做 $H_1(ID_i)$ 操作.

公钥询问: C 维护一个列表 K^{list} , 其每一项的格式为 (ID, x, P_{ID}) . 这个列表起初是空的. 当 C 接收到 A_1 对身份 ID_i 的公钥询问时, C 首先检索 K^{list} . 若 K^{list} 中有一项 (ID_i, x_i, P_i) , 则 C 返回 P_i 作为回答; 否则, C 随机选择 $x_i \in Z_q^*$, 计算 $P_i = x_i P$, 返回 P_i 作为回答并将 (ID_i, x_i, P_i) 加入到 K^{list} .

公钥替换询问: 当 C 接收到 A_1 的一个关于身份为 ID_i 的用户的公钥替换询问 (ID_i, P'_i) 时, C 检索 K^{list} 找到 (ID_i, x_i, P_i) 并设置 $x_i = \perp$, $P_i = P'_i$.

秘密值询问: 当 C 接收到 A_1 对身份为 ID_i 的用户的秘密值询问时, C 检索 K^{list} 找到 (ID_i, x_i, P_i) . 若 $x_i = \perp$, 表明关于身份 ID_i 的公钥已经被替换, 因此 C 无法正确回答 A_1 的秘密值询问, C 只能返回 \perp ; 否则 C 返回 x_i .

签名询问: 当 A_1 向 C 请求身份为 ID_i , 公钥为 P_i 的用户对一个消息 M_i 的签名时, C 按照如下步骤回答:

1. 随机选择 $h_i \in Z_q^*$, $V_i \in G_1$.
2. 计算 $R_i = e(V_i, P)(e(U_i, P_i)e(Q_i, P_0))^{-h_i}$, 其中 $U_i = H_2(ID_i, P_i)$, $Q_i = H_1(ID_i)$.
3. 设置 $H_3(M_i, ID_i, R_i, P_i) = h_i$.
4. 返回 (h_i, V_i) .

最后, A_1 输出一个伪造 $(M^*, \sigma^* = (h, V), ID^*, P^*)$. 若 $ID^* \neq ID_j$, C 终止; 否则, 根据 Forking Lemma^[13], C 选择不同的 Hash 函数 H'_3 并再次利用 A_1 的能力, 它可以得到另一个伪造 $(M^*, \sigma'^* = (h', V'), ID^*, P^*)$. 从而 C 得到了两个有效的伪造, 并且它们满足 $R = e(V, P)(e(U, P^*)e(Q, P_0))^{-h}$ 与 $R = e(V', P)(e(U, P^*)e(Q, P_0))^{-h'}$. 其中 $U = H_2(ID^*, P^*) = \beta P$, 并以 (ID^*, P^*, β, U) 的形式存在于 H_2^{list} 中, $Q = H_1(ID^*) = bP$.

这样就有 $e(V, P)(e(U, P^*)e(Q, P_0))^{-h} = e(V', P)(e(U, P^*)e(Q, P_0))^{-h'}$. 因此, C 可以计算出 CDH 问题的解 $abP = (h - h')^{-1}(V - V') - \beta P^*$.
证毕.

定理 2. 在随机预言模型下, 若群 G_1 中的 CDH 问题是困难的, 那么我们的无证书签名方案对于第 2 类攻击者是安全的.

证明. 假设 C 是一个 CDH 困难问题的解决者, 其困难问题的输入为 (aP, bP) , 他的目标是计算 abP . 假设 A_{II} 是第 2 类攻击者, 他能攻破我们的签名方案. 以下我们看 C 如何利用 A_{II} 来解决 CDH 问题.

首先, C 选择系统主密钥 $s \in Z_q^*$, 计算 $P_0 = sP$, 选择系统参数 $params = \{e, G_1, G_2, P, P_0, H_1, H_2, H_3\}$. 然后 C 将系统参数与主密钥给 A_{II} . 这里我们将 Hash 函数 H_2, H_3 看成随机预言机. 并且为了简单起见, 我们假设以下 A_{II} 的询问都是不同的.

公钥询问: C 维护一个列表 K^{list} , 其每一项的格式为 (ID, x, P_{ID}) . 这个列表被初始化为一个空表. 假设 A_{II} 最多能做 q_K 次公钥询问, C 在 $[1, q_K]$ 中随机选取一个值 J . 当 C 接收到 A_{II} 的一个关于身份为 ID_i 的用户的公钥询问时, C 首先检索 K^{list} . 若 K^{list} 中有一项 (ID_i, x_i, P_i) , 则 C 返回 P_i 作为回答; 否则, 若 $ID_i \neq ID_J$, C 随机选择 $x_i \in Z_q^*$, 设置 $P_i = x_i P$; 而当 $ID_i = ID_J$ 时, 设置 $x_i = \perp$, $P_i = aP$. 最后, C 返回 P_i 作为回答并将 (ID_i, x_i, P_i) 加入到 K^{list} .

H_2 询问: C 维护一个列表 H_2^{list} , 其格式为 (ID, P_{ID}, β, U) . 该列表起初是空的. 当 C 收到 A_{II} 对 $H_2(ID_i, P_i)$ 的询问时, C 首先判定 ID_i 是否等于 ID_J . 若 $ID_i \neq ID_J$, C 随机选择 $\beta_i \in Z_q^*$, 计算 $U_i = \beta_i P$; 否则设置 $\beta_i = \perp$, $U_i = bP$. 最后 C 将 $(ID_i, P_i, \beta_i, U_i)$ 加入到 H_2^{list} 并将 U_i 返回给 A_{II} .

H_3 询问: C 维护一个列表 H_3^{list} , 其格式为 (M, ID, R, P_{ID}, h) . 这个列表被初始化为一个空表. 当 A_{II} 询问 $H_3(M_i, ID_i, R_i, P_i)$ 时, C 随机选择 $h_i \in Z_q^*$, 将 $(M_i, ID_i, R_i, P_i, h_i)$ 加入到 H_3^{list} 并将 h_i 返回给 A_{II} .

秘密值询问: 当 C 接收到 A_{II} 的关于身份为 ID_i 的用户的秘密值询问时, 若 $ID_i = ID_J$, C 终止; 否则, C 首先生成该用户的公钥, 然后检索 K^{list} 找到 (ID_i, x_i, P_i) . 若 $x_i = \perp$, 表明关于身份 ID_i 的公钥已经被替换, 因此 C 无法正确回答 A_{II} 的秘密值询问, C 返回 \perp ; 否则 C 返回 x_i .

公钥替换询问: 当 C 接收到 A_{II} 的一个关于身份为 ID_i 的用户的公钥替换询问 (ID_i, P'_i) 时, 若 $ID_i = ID_J$, C 终止; 否则, C 检索 K^{list} 找到 $(ID_i, x_i,$

$P_i)$ 并设置 $x_i = \perp, P_i = P'_i$.

签名询问: 当 A_{II} 向 C 请求身份为 ID_i , 公钥为 P_i 的用户对消息 M_i 在的签名时, C 按照如下步骤回答该询问:

1. 随机选择 $h_i \in Z_q^*, V_i \in G_1$.
2. 计算 $R_i = e(V_i, P)(e(U_i, P_i)e(Q_i, P_0))^{-h_i}$, 其中 $U_i = H_2(ID_i, P_i), Q_i = H_1(ID_i)$.
3. 设置 $H_3(M_i, ID_i, R_i, P_i) = h_i$.
4. 返回 (h_i, V_i) .

最后, A_{II} 输出一个伪造 $(M^*, \sigma^* = (h, V), ID^*, P^*)$. 若 $ID^* \neq ID_j, C$ 终止; 否则, 根据 Forking Lemma, C 选择不同的 Hash 函数 H'_3 并再次利用 A_{II} 的能力, 它可以得到另一个伪造 $(M^*, \sigma^{*'} = (h', V'), ID^*, P^*)$. 从而 C 得到了两个有效的伪造, 并且它们满足 $R = e(V, P)(e(U, P^*)e(Q, P_0))^{-h}$ 与 $R = e(V', P)(e(U, P^*)e(Q, P_0))^{-h'}$. 其中 $P^* = aP, U = H_2(ID^*, P^*) = bP$, 并以 (ID^*, P^*, \perp, bP) 的形式存在于 H_2^{list} 中.

于是就有等式 $e(V, P)(e(U, P^*)e(Q, P_0))^{-h} = e(V', P)(e(U, P^*)e(Q, P_0))^{-h'}$. 由我们设置可知,

$$e(V - V', P)(e(bP, aP)e(Q, sP))^{-h} = (e(bP, aP)e(Q, sP))^{-h'},$$

因此, C 可以计算出 CDH 问题的解 $abP = (h - h')^{-1}(V - V') - sQ$.
证毕.

5 效率分析及应用

下面, 我们将在计算和通信效率方面, 把用本文的方法所构造的方案与一些目前能在文献[11]中模型下证明是安全的方案以及几个效率比较高, 但是安全性未能有效证明的方案进行比较. 我们用 P 表示一个双线性对运算, S 表示群 G_1 中的标量乘运算, E 表示群 G_2 中的幂运算, H 表示一个 Hash 到群 G_1 的运算. 用 P_1 表示 G_1 中的一个点的长度, 用 P_2 表示 G_2 中的一个点的长度, 用 Z_1 表示 Z_q^* 中的一个点的长度. 比较结果如表 1 所示.

表 1 与其它方案的比较

方案	签名	验证(预计算)	签名长度	公钥长度	安全性
文献[7]中方案 1	2S	2P, 2S, 1H(2P, 2S)	$2P_1$	$1P_1$	未知
文献[7]中方案 2	1S, 1E	1P, 2S, 1E(1P, 1E)	$1P_1, 1P_2$	$1P_1$	未知
文献[10]中方案	3S, 2H	4P, 3H(3P, 2H)	$2P_1$	$1P_1$	安全
文献[14]中方案 1	1S, 1H	3P, 1H(2P, 1H)	$1P_1$	$1P_1$	未知
文献[14]中方案 2	3S, 1E	2P, 2S, 1E, 1H(1P, 2S, 1E)	$2Z_1, 1P_1$	$1P_1$	安全
文献[15]中方案	1S, 2E	1P, 1S, 2E(1P, 2E)	$2Z_1, 1P_1$	$1P_2$	安全
本文的方案	2S, 1E	3P, 1H(1P, 1E)	$1Z_1, 1P_1$	$1P_1$	安全

从表 1 中可以看出, 在签名阶段我们的方案未涉及到双线性对计算, 并且在效率上与其它方案相差无几. 在验证阶段, 当不考虑预计算时我们的方案比文献[10]中方案效率高一点, 而与文献[14]中方案 1 效率基本相同. 与文献[7, 15]中方案及文献[14]中方案 2 相比虽然效率略低, 但我们方案的签名长度是文献[14]中方案 2 及文献[15]中方案的 $2/3$, 与文献[7]中方案比我们的签名方案有较高的安全级别. 当考虑预计算时, 本文签名方案的验证算法比文献[10, 14-15]中方案及文献[7]中方案 1 效率更高, 而与文献[7]中方案 2 相比效率基本相同, 但签名长度则相对较短.

在有些情况下, 我们的方案可以进行预计算. 比如验证者若经常接收某个签名者的签名并进行验证, 那么他可以预计算 $Q_{ID}, U, e(U, P_{ID})e(Q_{ID}, P_0)$ 并储存这些值, 从而大大减少实际计算代价. 此外在安全要求较高, 签名长度要求较短的环境中我们的方案也有相对优势. 因此, 我们的方案可用于带宽受限的 Ad Hoc 网络以及需要频繁传递和验证签名的

电子商务和电子政务等领域以提供完整性、真实性和不可否认性等安全服务.

6 总 结

我们提出了一类无证书签名方案的构造方法, 用这种方法构造的方案的安全性基于计算 Diffie-Hellman 问题的困难性. 在考虑预计算的情况下, 我们的方案效率很高, 总共只需计算 1 个双线性对, 明显优于其它现有方案. 我们方案的安全性证明是基于文献[11]中的安全模型, 它是无证书签名方案的一个很强的安全模型. 因此, 我们的方案可在适合使用无证书密码体制的场合用以提供真实性、完整性和不可否认性等安全服务.

参 考 文 献

[1] Shamir A. Identity based cryptosystems and signature schemes//Proceedings of the Crypto'84. California, USA, 1984: 47-53

- [2] Al-Riyami S, Paterson K. Certificateless public key cryptography//Proceedings of the Asiacrypt 2003. Taipei, China, 2003; 452-473
- [3] Huang X, Susilo W, Mu Y, Zhang F. On the security of a certificateless signature scheme//Proceedings of the CANS 2005. Xiamen, China, 2005; 13-25
- [4] Yap W, Heng S, Goi B. An efficient certificateless signature scheme//Proceedings of the EUC Workshops 2006. Seoul, Korea, 2006; 322-331
- [5] Park J. An attack on the certificateless signature scheme from EUC Workshops 2006. Cryptology ePrint Archive, Report 2006/442, 2006
- [6] Zhang Z, Feng D. Key replacement attack on a certificateless signature scheme. Cryptology ePrint Archive, Report 2006/453, 2006
- [7] Choi K, Park J, Hwang J, Lee D. Efficient certificateless signature schemes//Proceedings of the ACNS 2007. Zhuhai, China, 2007; 443-458
- [8] Castro R, Dahab R. Two notes on the security of certificateless signatures//Proceedings of the ProvSec 2007. Wollongong, Australia, 2007; 85-102
- [9] Zhang J, Mao J. Security analysis of two signature schemes and their improved schemes//Proceedings of the ICCSA 2007. Kuala Lumpur, Malaysia, 2007; 589-602
- [10] Zhang Z, Wong D, Xu J, Feng D. Certificateless public-key signature: security model and efficient construction//Proceedings of the ACNS 2006. Singapore, 2006; 293-308
- [11] Hu B, Wong D, Zhang Z, Deng X. Key replacement attack against a generic construction of certificateless signature//Proceedings of the ACISP 2006. Melbourne, Australia, 2006; 235-246
- [12] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols//Proceedings of the CCCS'93. Virginia, USA, 1993; 62-73
- [13] Pointcheval D, Stern J. Security proofs for signature schemes//Proceedings of the EUROCRYPT'96. Saragossa, Spain, 1996; 387-398
- [14] Huang X, Mu Y, Susilo W, Wong D, Wu W. Certificateless signature revisited//Proceedings of the ACISP 2007. Townsville, Australia, 2007; 308-322
- [15] Zhang L, Zhang F, Zhang F. New efficient certificateless signature scheme//Proceedings of the EUC Workshops 2007. Taipei, China, 2007; 692-703



ZHANG Lei, born in 1982, Ph. D. candidate. His research interests include cryptography and information security.

ZHANG Fu-Tai, born in 1965, professor, Ph. D. supervisor. His research interests include information security, network security and cryptography.

Background

This paper investigates efficient constructions of signature schemes in Certificateless public key setting. Digital signature is one of the most important primitives in public key cryptography. It provides authenticity, integrity and non-repudiation to many kinds of applications. In traditional public key cryptosystems, the management of certificates is usually complex and costly. Shamir introduced Identity-based public key cryptography to remove this requirement. However, key escrow problem is inherent in Identity-based public key cryptography. Certificateless public key cryptography is a new paradigm which was first introduced by Al-Riyami and Paterson in 2003. Their main purpose is to solve the key escrow problem in Identity-based public key cryptography, while keeping the implicit certification property of Identity-based public key cryptography.

Recently, a number of certificateless signature schemes have been presented. The first one was presented by Al-Riyami and Paterson without formal security analysis. Later, Huang et al. pointed out a security drawback of this scheme

and proposed a secure one. They also defined the security model of certificateless signature schemes. An improved security model was presented by Zhang et al. and an even stronger one was put forward by Hu et al. With respect to the efficiency, most of the previous secure CLS schemes involve a relatively large amount of pairing computation and exponentiation in the process of signing and verification.

In this paper, the authors show a new method to construct a class of certificateless signature schemes. This kind of schemes can be proven secure in a very strong security model. In addition, the constructed schemes have a better overall performance when compared with some other provably secure certificateless signature schemes available. The research is supported by the National Natural Science Foundation of China (No. 60673070) and the Natural Science Foundation of Jiangsu Province (No. BK2006217). The projects focus on the study of secure and efficient encryption schemes, signature schemes and key agreement protocols in certificateless setting.