

文章编号:1001-9081(2010)07-1809-03

有效的无证书签名方案

洪东招¹, 谢琪²

(1. 杭州师范大学理学院, 杭州 310036; 2. 杭州师范大学信息科学与工程学院, 杭州 310036)

(hongdzjm@sina.com)

摘要:为解决基于身份的密码体制的密钥托管问题以及传统公钥密码体制的公钥认证问题,通过修改 Barreto 等人提出的高效的基于身份的签名方案中的私钥和公钥的产生算法,提出了一个无证书签名方案。该方案在随机预言模型下是可证明安全的,而且也是高效的方案,只需要一个对运算。

关键词:无证书签名;双线性对;q-SDH 问题;Inv-CDH 问题;随机预言机

中图分类号:TP309 **文献标志码:**A

Efficient certificateless signature scheme

HONG Dong-zhao¹, XIE Qi²

(1. College of Science, Hangzhou Normal University, Hangzhou Zhejiang 310036, China;

2. School of Information Science and Engineering, Hangzhou Normal University, Hangzhou Zhejiang 310036, China)

Abstract: To solve the key escrow problem of ID-based cryptography and the public key authentication of traditional public key cryptosystem, a certificateless signature scheme revising the private and public generation algorithms in Barreto et al.'s efficient ID-based signature was proposed. The scheme is provably secure in the random oracle model, and is an efficient scheme. It only needs one pairing operation.

Key words: certificateless signature; bilinear pairings; q-Strong Diffie-Hellman Problem, q-SDHP (q-SDHP); Inverse Computational Diffie-Hellman Problem (Inv-CDHP); random oracle

0 引言

在基于证书的传统公钥密码系统下,需要权威的认证中心(Certificate Authority, CA)签发用户的公钥证书,而在实际应用中证书的撤销、存储、发布、验证等过程复杂并且代价高。为此,Shamir^[1]首次提出了基于身份的密码系统。在该密码系统中,用户使用能唯一代表他身份的一个公开信息(比如身份证号等)作为公钥,用户私钥不需认证。但在该系统中,用户私钥完全由可信的密钥产生中心(Key Generation Centre, KGC)产生,故存在着密钥托管问题。为了解决基于身份的密码系统的密钥托管问题,AL-Riyasni 等人^[2]首次提出无证书公钥密码系统。在此系统中,用户私钥由第三方 KGC 和用户共同产生,用户随机选取一个秘密值与 KGC 产生的部分私钥结合生成私钥,所以恶意的 KGC 不能获得用户的私钥。

自首次无证书签名方案^[2]提出以来,该方面的研究逐步得到发展,提出了一些新的方案。Yum 等人^[3]提出了无证书签名方案的一般模型, Li 等人^[4]和 Yap 等人^[5]提出了比较有效的无证书签名方案。但这些方案存在安全漏洞,如 Huan 等人^[6]指出文献^[2]的方案, Hu 等人^[7]指出文献^[3]的方案, Au 等人^[8]指出文献^[4]的方案, Park^[9]指出文献^[5]的方案易受恶意 KGC 攻击或公钥替换攻击。这样,研究可证明安全的无证书签名方案显得十分重要。最近, Du 等人^[10]和张玉磊等人^[11]分别基于 k 个叛逆者联合攻击(Collusion Attack Algorithm with k traitors, k-CAA)和 Inv-CDHP、q-SDHP 和 Inv-CDHP 的安全性假设提出了可证明安全的基于双线性对的高效无证书签名方案。Fan 等人^[12]指出 Du-Wen 方案^[10]无法

抵抗公钥替换攻击,且安全性证明存在缺陷。

另一方面,基于身份的方案中必须假设 KGC 是安全的,否则 KGC 知道所有用户的密钥,总可以假冒任何用户产生有效的签名。近来, Barreto 等人^[13]提出了一个高效的基于身份的签名方案(以下简称 Barreto 方案),优于现有的方案。但在无证书签名方案中,因为 KGC 不安全,因此 Barreto 方案不能在无证书公钥的环境中使用。本文通过修改 Barreto 方案中的私钥和公钥的产生算法,提出了一个无证书签名方案,并且在随机预言机模型下,证明了方案的安全性,其安全性依赖于 q-SDH 困难问题和 Inv-CDH 困难问题。效率分析表明提出的方案也是高效的方案。

1 提出的方案

在 Du-Wen 和张玉磊等人的无证书签名方案中,因为公钥为 $PK = (P_{pub} + Q_{ID}P)$, 因此,在签名的产生中需要计算乘法逆元,会增加计算量;而且因为 Du-Wen 方案中的安全性假设为 k-CAA,这并不是一个普遍能接受的标准安全假设^[15],且方案存在安全缺陷^[12]。而 Barreto 方案是当前已有方案中十分高效的可证明安全的方案。因此,本文修改 Barreto 方案中私钥和公钥产生算法,形成新的无证书签名方案。具体过程如下。

系统设置:同 Barreto 方案。 k 是安全参数,PKG 选择双线性群群 (G_1, G_2, G_T) 的阶为素数 $p > 2^k$ 并且 Q 为群 G_2 的生成元, $P = \psi(Q) \in G_1$ 为 G_1 生成元, $e: G_1 \times G_2 \rightarrow G_T$ 是一个安全的双线性对映射。设 $g = e(P, Q)$, 随机选择 $s \in_R Z_p^*$ 作为系统主密钥,计算 $Q_{pub} = sP \in G_2$, 选择 2 个 Hash 函数: $H_1: \{0, 1\}^* \rightarrow Z_p^*$, $H_2: \{0, 1\}^* \times G_T \rightarrow Z_p^*$, 秘密保存主密钥 s , 公开参数 $params :=$

收稿日期:2009-12-28;修回日期:2010-02-08。

作者简介:洪东招(1982-),男,浙江苍南人,硕士研究生,主要研究方向:信息安全、现代密码学; 谢琪(1968-),男,浙江上虞人,教授,博士,主要研究方向:信息安全、现代密码学。

$\{G_1, G_2, G_T, P, Q, g, Q_{\text{pub}}, e, \psi, H_1, H_2\}$ 。

部分私钥提取: 已知 $ID \in (0, 1)^*$, PKG 计算 $Q_{\text{ID}} = H_1(ID)$, $d_{\text{ID}} = \frac{1}{s + Q_{\text{ID}}}P$ 通过安全信道发送 d_{ID} 给 ID 用户作为部分私钥。ID 用户验证等式: $e(d_{\text{ID}}, P_{\text{pub}} + Q_{\text{ID}}P) = g$ 。

设置秘密值: ID 用户随机选取 $r \in Z_p^*$, 把 r 作为用户自己的秘密值。

设置私钥: 已知系统参数, 用户部分私钥 d_{ID} , 秘密值 r , 输入用户私钥 $sk_{\text{ID}} = rd_{\text{ID}}$ 。

设置公钥: 输入系统参数, 用户的秘密值 r , 产生用户的公钥 $pk_{\text{ID}} = \frac{1}{r}(P_{\text{pub}} + Q_{\text{ID}}P)$ 。

签名: 同 Barreto 方案。选择随机值 $x \in_R Z_p^*$, 计算 $R = g^x \bmod p$, $h = H_2(m, R)$, $S = (x + h)sk_{\text{ID}}$ 。对 m 的签名就是 $\sigma = (S, R)$ 。

验证: 同 Barreto 方案。计算 $h = H_2(m, R)$, 接受签名并且返回 1, 当且仅当等式 $Ver(m, ID, pk_{\text{ID}}, \sigma) = 1 \Leftrightarrow e(S, pk_{\text{ID}})g^{-h} = R$ 成立。

方案验证的正确性为:

$$\begin{aligned} e(S, pk_{\text{ID}})g^{-h} &= e((x + h)rd_{\text{ID}}, pk_{\text{ID}})g^{-h} = \\ &= e((x + h)r \frac{1}{s + Q_{\text{ID}}}P, \frac{1}{r}(P_{\text{pub}} + Q_{\text{ID}}P))g^{-h} = \\ &= \frac{1}{r}(sP + Q_{\text{ID}}P)g^{-h} = e((x + h)P, P)g^{-h} = R \end{aligned}$$

2 安全性证明与效率比较

2.1 安全性证明

无证书签名方案中存在两类敌手^[14]: 第一类敌手 A_1 不能获知系统主密钥, 但可以替换任何用户的公钥; 第二类敌手 A_1 可获知系统主密钥, 但不能取代目标用户的公钥。本方案主要参考文献[11, 13]给出了安全性证明。

定理 1 在随机预言模型下, 如果 q-SDHP 假设是困难的, 那么本文方案对于第一类敌手 A_1 是自适应选择消息和身份攻击下存在性不可伪造的。

证明 令 Ω 是 q-SDHP 的解决者, 它接受 q-SDHP 的一个随机实例 $(P, aP, a^2P, \dots, a^qP) \in G_1^{q+1}$, 需要找到一个对 $(c, \frac{1}{c+a}P)$, 其中 $a, c, q \in Z_p^*$ 。 A_1 是第一类敌手。假设 A_1 能伪造签名成功, 证明 Ω 可利用 A_1 的能力, 解决给定的 q-SDHP。

系统参数的设置。在设置阶段, 建立一个生成元 $Q \in G$, 使得它知道 $q-1$ 对 $(\omega_i, \frac{1}{\omega_i + a}Q)$, 其中 $\omega_1, \dots, \omega_{q-1} \in_R Z_p^*$, 步骤如下所示^[13]:

1) 令 $\omega_1, \dots, \omega_{q-1} \in_R Z_p^*$, 展开函数 $f(x) = \prod_{i=1}^{q-1} (x + \omega_i)$ 得到 $c_0, c_1, \dots, c_{q-1} \in Z_p^*$, 那么有 $f(x) = \prod_{i=0}^{q-1} c_i x^i$;

2) 设生成元 $Q = \sum_{i=0}^{q-1} c_i (a^i P) = f(a)P \in G_1$, 那么公钥 $H_{\text{pub}} = \sum_{i=1}^{q-1} c_{i-1} (a^i P) = aQ$ 。

3) Ω 展开 $f_i(x) = \frac{f(x)}{x + \omega_i} = \sum_{i=0}^{q-2} d_i x^i$, 并且 $\sum_{i=0}^{q-2} d_i a^i P = f_i(a)P = \frac{f(a)}{\omega_i + a}P = \frac{1}{\omega_i + a}Q$, 从而计算出对 $(\omega_i, \frac{1}{\omega_i + a}Q)$ 。

Ω 设置系统主公钥 $H_{\text{pub}}, g' = e(Q, Q)$, a 为系统主密钥, Ω 为未知主密钥。系统参数 $param = (G_1, G_2, e, p, P, H_{\text{pub}}, g')$,

H_1, H_2), Ω 把上述所有参数给 A_1 。 Ω 随机选择一个挑战身份 $ID^* \in_R \{0, 1\}^*$, 挑战消息 M^* 。

Ω 把 H_1, H_2 作为随机预言机。 A_1 可以做 H_1, H_2 询问, 部分私钥、私钥、公钥、公钥替换、签名等询问。设 A_1 的每次询问都是不同的。 Ω 维护 L, L_1, L_2, L_3 等列表, 四个列表的格式依次如下 (ID_i, Q_i, D_i) , (ID_i, Q_i) , (M_i, R_i, h_i) 和 (ID_i, r_i, PK_i, c) 。所有列表初始为空。

H_1 询问。当收到 A_1 的询问 $H_1(ID_i)$, 如果 $ID_i = ID^*$, Ω 返回一个随机 $Q^* \in_R Z_p^*$ 且 $Q^* \notin \{\omega_1, \omega_2, \dots, \omega_{q_h}\}$, 其中 q_h 表示 H_1 询问的最大次数; 否则, Ω 回答 $Q_i \in \{\omega_1, \omega_2, \dots, \omega_{q_h}\}$ 并添加 (ID_i, Q_i) 到 L_1 列表中。

H_2 询问。当收到 A_1 的询问 $H_2(M_i, R_i)$, Ω 随机选择 $h_i \in_R Z_p^*$, 返回 h_i 并将添加 (M_i, R_i, h_i) 到 L_2 列表中。

部分私钥询问。当收到 A_1 身份 ID_i 的部分私钥询问, Ω 从 L_1 列表找到 (ID_i, Q_i) , 返回 $D_i = (\frac{1}{a + Q_i})Q$ 并将添加 (ID_i, Q_i, D_i) 到 L 列表中。

公钥询问。当收到 A_1 关于身份 ID_i 的公钥询问, 如果 L_3 列表包含 (ID_i, r_i, PK_i, c) , 那么 Ω 返回 PK_i 给 A_1 ; 否则 Ω 随机选择 $r^* \in_R Z_p^*$, 如果 $ID_i = ID^*$, 计算 $PK^* = \frac{1}{r^*}(H_{\text{pub}} + Q^*Q)$, 返回 PK^* 给 A_1 , 并将添加 $(ID^*, r^*, PK^*, 1)$ 到 L_3 列表中; 否则, Ω 从 L_1 列表中找到 (ID_i, Q_i) , 随机选择 $r_i \in_R Z_p^*$, 计算 $PK_i = \frac{1}{r_i}(H_{\text{pub}} + Q_iQ)$ 。返回 PK_i 给 A_1 并将 $(ID_i, r_i, PK_i, 0)$ 添加到 L_3 列表中。

私钥询问。当收到 A_1 身份 ID_i 的私钥询问, Ω 从 L 列表找到 ID_i 的部分私钥 D_i , 从 L_3 列表找到 ID_i 的秘密值 r_i , 返回给 A_1 私钥 $SK_i = r_i D_i$ 。

公钥替换询问。当收到 A_1 关于身份 ID_i 的公钥替换询问, A_1 选取 PK_i' , 那么 Ω 更新 L 列表中 PK_i 为 PK_i' 。

签名询问。若 A_1 做 (M_i, PK_i, ID_i, R_i) 签名询问, 其中 M_i 表示消息, PK_i 表示由 A_1 选择的公钥, ID_i 表示身份, 假设 $ID_i \neq ID^*$ 。 Ω 按如下步骤新建签名:

若 $c = 1$, 随机选取 $x_i \in_R Z_p^*$, 计算 $R_i = g^{x_i}$, 从 L_2 中找到 h_i , 计算 $S_i = (x_i + h_i)SK_i = (x_i + h_i) \frac{r_i}{a + Q_i}Q$, 则签名 $\sigma = (S_i, R_i)$, Ω 返回 σ 给 A_1 。

若 $c = 0$, Ω 可从 A_1 获得 r_i' , 选取 $x_i \in_R Z_p^*$, 计算 $R_i = g^{x_i}$, 计算 $S_i = (x_i + h_i)SK_i = (x_i + h_i) \frac{r_i'}{a + Q_i}Q$, Ω 返回 σ 给 A_1 。

最后使用分叉技术^[16]: 假设 A_1 成功伪造一个签名 $\sigma = (S, R)$, 那么 Ω 可以重放 A_1 的攻击能力, 重新排列 H_2 询问的回答, 获得另外一个伪造签名 $\sigma' = (S', R)$ 。由于 σ, σ' , 其中 $h' \neq h$ 满足下列等式:

$$\begin{aligned} e(S, PK^*)g'^{-h} &= \\ e(S', PK^*)g'^{-h'}, e(S, PK^*)e(S', PK^*)^{-1} &= g'^{h-h'} \\ e(S - S', PK^*) &= g'^{h-h'}, e((S - S') \frac{1}{r^*}(a + Q^*), Q) = \\ &= e((h - h')Q, Q) \end{aligned}$$

从而得到等式: $\frac{1}{r^*}(S - S')(h - h')^{-1} = \frac{1}{(a + Q^*)}Q$ 。最后成功输出一个对 $(Q^*, \frac{1}{a + Q^*}Q)$ 。那么 Ω 可以利用 A_1 的能力解决 q-SDHP。

定理 2 在随机预言模型下, 如果 Inv-CDHP 假设是困难

的,那么本文方案对于第二类敌手 A_{II} 是自适应选择消息和身份攻击下存在性不可伪造的。

证明 假设 A_{II} 能伪造签名成功,证明 Ω 可利用 A_{II} 的能力,解决给定的 Inv-CDHP。令 Ω 是一个 Inv-CDHP 的解决者,接受 Inv-CDHP 的一个随机实例,已知 cP , 不知道 $c \in Z_p^*$, 求 $c^{-1}P$ 。

系统参数的设置: Ω 选择系统主密钥 $s \in_R Z_p^*$, 计算 $P_{pub} = sP, Y = yP$, 系统参数 $param = (G_1, G_2, e, p, P, P_{pub}, g, H_1, H_2)$ 。 Ω 把上述参数及系统主密钥 s 给 A_{II} 。

Ω 把 H_1, H_2 作为随机预言机。 A_{II} 可以做 H_1, H_2 询问,私钥、公钥、签名等询问。设 A_{II} 的每次询问都是不同的, H_1, H_2 询问与定理 1 中的询问相同。

私钥询问。当收到 A_{II} 身份 ID_i 的私钥询问, Ω 从 L_1 列表找到 Q_i , 从 L_3 列表找到 r_i , 计算 $SK_i = r_i D_i = r_i \frac{1}{s + Q_i} P$, 返回 SK_i 给 A_{II} 并将添加 (ID_i, r_i, D_i, SK_i) 到 L_4 列表中。

公钥询问。当收到 A_{II} 身份 ID_i 的公钥询问,如果 L_3 列表包含 (ID_i, r_i, PK_i, Q_i) , Ω 返回 PK_i 给 A_{II} ; 否则 Ω 随机选择 $r^* \in_R Z_p^*$, 如果 $ID_i = ID^*$ 计算 $PK^* = sY + Q^* Y$ 返回 PK^* 给 A_{II} 并将添加 (ID^*, \perp, PK^*, Q^*) 到 L_3 列表中; 否则, Ω 从 L_1 列表中找到 (ID_i, Q_i) , 随机选择 $r_i \in_R Z_p^*$, 计算 $PK_i = \frac{1}{r_i}(P_{pub} + Q_i P)$, 返回 PK_i 给 A_{II} 并将 (ID_i, r_i, PK_i, Q_i) 添加到 L_3 列表中。

签名询问。若 A_{II} 做 (M_i, PK_i, ID_i, R_i) 签名询问,其中 M_i 表示消息, PK_i 表示由 A_{II} 选择的公钥, ID_i 表示身份, Ω 按如下步骤新建签名: 假设 $ID_i \neq ID^*$ 。随机选取 $x_i \in_R Z_p^*, h_i$, 计算 $S_i = (x_i + h_i)SK_i, R_i = e(S_i, PK_i)g^{-h_i}$, 则签名 $\sigma = (S_i, R_i)$, Ω 返回 σ 给 A_{II} 。

最后使用分叉技术^[16]: 假设 A_{II} 成功伪造一个签名 $\sigma = (S, R)$, 那么 Ω 可以重放 A_{II} 的攻击能力, 重新排列 H_2 询问的回答, 获得另外一个伪造签名 $\sigma' = (S', R)$ 。由于 σ, σ' , 其中 $h' \neq h$ 满足下列等式:

$$\begin{aligned} e(S, PK^*)g^{-h} &= \\ e(S', PK^*)g^{-h'}, e(S, PK^*)e(S', PK^*)^{-1} &= g^{h-h'} \\ e(S - S', PK^*) &= g^{h-h'}, e((S - S')(s + Q^*)Y, P) = \\ &= e((h - h')P, P) \end{aligned}$$

从而得到等式: $(S - S')(s + Q^*)(h - h')^{-1} = \frac{1}{y}Q$ 。即 Ω 可以解决 Inv-CDHP 问题。

2.2 效率比较

因为 Du-Wen 方案^[10]与张玉磊等人^[11]的方案是已有方案中效率比较高的方案, 因此提出的方案只与这 2 个方案进行比较。根据计算复杂性理论, 因为除签名的产生与验证以外的过程在预先完成, 因此无证书签名方案的效率主要考虑签名的产生与验证的计算量, 而其他计算量与 Hash 函数的计算量 T_h 、求乘法逆元计算量 T_i 、模幂乘运算量 T_e 和双线性对的计算量 T_p 相比可以忽略不计, 因此本文主要比较这些计算量, 具体如表 1 所示。

表 1 效率比较

方案	签名产生	签名验证	合计
文献[10]方案	$T_h + T_i$	$T_h + T_p$	$2T_h + T_i + T_p$
文献[11]方案	$T_h + T_i + T_e$	$2T_h + T_p + T_e$	$3T_h + T_i + T_p + 2T_e$
本文方案	$T_h + T_e$	$T_h + T_p + T_e$	$2T_h + T_p + 2T_e$

因此, 由表 1 可知提出的方案也是高效的方案, 优于文献

[11] 方案。

3 结语

基于身份的签名方案与无证书签名方案关注 KGC 是否安全。修改 Barreto 方案中的私钥和公钥的产生算法而提出的一个无证书签名方案, 在随机预言机模型下是可证明安全的, 而且只需要一个对运算, 不需要计算乘法逆元。

参考文献:

- [1] SHAMIR A. Identity-based cryptosystems and signature schemes[C] // Advances in Cryptology-CRYPTO' 84, LNCS 196. Berlin: Springer-Verlag, 1985: 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] YUM D H, LEE P J. Generic construction of certificateless signature[C] // ACISP 2004: Australasian Conference on Information Security and Privacy, LNCS 3108. Berlin: Springer-Verlag, 2004: 200 - 211.
- [4] LI X, CHEN K, SUN L. Certificateless signature and proxy signature schemes from bilinear pairings[J]. Lithuanian Mathematical Journal, 2005, 45(1): 76 - 83.
- [5] YAP W S, HENG S H, GOI B M. An efficient certificateless signature scheme[C] // EUCWorkshops 2006: Emerging Directions in Embedded and Ubiquitous Computing, LNCS 4097. Berlin: Springer-Verlag, 2006: 322 - 331.
- [6] 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.
- [7] HU B C, WONG D S, ZHANG Z F, et al. Key replacement attack against a generic construction of certificateless signature[C] // ACISP2006: Australasian Conference on Information Security and Privacy, LNCS 4058. Berlin: Springer-Verlag, 2006: 235 - 246.
- [8] AU M H, CHEN J, LIU J K, et al. Malicious KGC attacks in certificateless cryptography[C] // ASIACCS 2007: The 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2007: 302 - 311.
- [9] PARK J H. An attack on the certificateless signature scheme from EUC Workshops 2006: Cryptology ePrint Archive, Report 2006/442 [EB/OL]. [2009 - 10 - 31]. <http://eprint.iacr.org/2006/442.pdf>.
- [10] DU H Z, WEN Q Y. Efficient and provably-secure certificateless short signature scheme from bilinear pairings[J]. Computer Standards and Interfaces, 2009, 31(2): 390 - 394.
- [11] 张玉磊, 王彩芬, 张永洁, 等. 基于双线性对的高效无证书签名方案[J]. 计算机应用, 2009, 29(5): 1330 - 1333.
- [12] FAN C I, HSU R H, HO P H. Cryptanalysis on Du-Wen certificateless short signature scheme[EB/OL]. [2009 - 11 - 12]. <http://jwis2009.nsysu.edu.tw/location/paper/Cryptanalysis%20on%20Du-Wen%20Certificateless%20Short%20Signature%20Scheme.pdf>.
- [13] BARRETO P S L M, LITERT B, MCCULLAGH N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C] // Advances in Cryptology-ASIACRYPT 2005, LNCS 3788. Berlin: Springer-Verlag, 2005: 515 - 532.
- [14] ZHANG Z F, WONG S D, XU J, et al. Certificateless public-key signature: security model and efficient construction[C] // ACNS 2006: 4th International Conference on Applied Cryptography and Network Security, LNCS 3989. Berlin: Springer-Verlag, 2006: 293 - 308.
- [15] WANG B, SONG Z X. A non-interactive deniable authentication scheme based on designated verifier proofs[EB/OL]. [2009 - 10 - 20]. <http://eprint.iacr.org/2008/159.pdf>.
- [16] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361 - 396.