文章编号:1001 - 9081(2009)05 - 1330 - 04

基于双线性对的高效无证书签名方案

张玉磊[1],王彩芬[1],张永洁[2],程文华[1],韩亚宁[1]
(1. 西北师范大学 数学与信息科学学院,兰州 730070; 2. 甘肃省卫生学校,兰州 730000)
(zylei79@163.com)

摘 要:为了避免身份密码系统中密钥托管问题,出现了无证书密码系统。基于双线性对提出了一个高效的无证书签名方案。在方案中,签名算法需要一个指数运算,验证算法仅需要一个对运算和一个指数运算。与许多已有方案相比,具有较高的效率。方案的安全性依赖于 q-SDH 困难问题和 Inv-CDH 困难问题,并在随机预言机模型下,证明能够抵抗适应性选择消息攻击下的存在性伪造。

关键词:双线性对;q-SDH 问题;Inv-CDH 问题;无证书签名
中图分类号: TP309.7;TP393.08 **文献标志码**:A

Efficient certificateless signature scheme based on bilinear parings

ZHANG Yu-lei[1], WANG Cai-fen[1], ZHANG Yong-jie[2], CHENG Wen-hua[1], HAN Ya-ning[1]
(1. *College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu* 730070, *China*;
2. *Gansu Province Health School, Lanzhou Gansu* 730000, *China*)

Abstract: Due to eliminating the inherent key escrow in identity-based cryptosystem, the certificateless public key cryptosystem came into being. A new efficient certificateless signature scheme based on bilinear pairing was put forward. The signing algorithm did not need any pairing computation but need one exponentiation computation, and the verification algorithm only needed one pairing and one exponentiation computation. The new scheme is more efficient than other exsiting schemes in terms of computation overhead. Furthermore, the security relies on the hardness of the q-Strong Diffie-Hellman (q-SDH) problem and Inverse-Compute Diffie-Hellman (Inv-CDH) problem. Under the random oracle model, the new scheme is proved to be secure against existential forgery on adaptively chosen message attack.

Key words: bilinear pairing; q-SDHP; Inv-CDHP; certificateless signature

0 引言

为了简化传统 PKI 证书管理,文献[1]提出了基于身份的公钥密码系统(ID-based Public Key Cryptography,ID-PKC)。但是,ID-PKC 引入了密钥托管问题,密钥生成中心(Key Generator Center, KGC)了解所有用户的私钥,恶意 KGC 可以伪造用户的私钥。为了解决 ID-PKC 密钥托管缺陷,文献[2]提出了无证书公钥密码系统(Certificateless Public Key Cryptography, CL-PKC)。CL-PKC 是传统 PKI 和 ID-PKC 的折中,既简化了传统 PKI 对公钥证书的需求,又解决了 ID-PKC 的密钥托管问题。在 CL-PKC 中,KGC 不能完全获得用户私钥,它根据用户的身份 ID 生成用户的部分私钥,用户将部分私钥和自己选择的秘密值组合生成用户真正私钥。CL-PKC 降低了系统公钥认证的开支,适合于低带宽、低功率的移动环境使用。

自 CL-PKC 提出之后,出现了许多无证书签名方案(Certificateless Signature, CLS)。文献[2]提出了第一个 CLS 方案,不久,文献[3]就指出该方案是不安全的,容易受到公钥替换攻击,并对其作了改进,给出了 CLS 方案的安全模型。文献[4]提出了无证书签名方案的一般构造,但文献[5]指出该构造是不安全的。文献[6]改进了文献[3]的安全模型,并给出一个可证明安全的无证书签名方案,但是,该方案需要 4 个对运算,效率比较低。文献[7]提出的方案(Gorantla-Saxena 方案)需要 3 个对运算,文献[8]提出的方案(Yap 方案)仅需要 2 个对运算,文献[9]提出了基于 q-SDH 困难问题的方案(Goya-Terada 方案),需要 1 个对运算和 2 个指数运算。这三个方案的效率都比较高,但都不安全。文献[10 - 12]分别指出文献[7 - 9]的方案存在公钥替换攻击。

本文利用双线性对技术,提出一个有效可证明安全的无证书签名方案。效率方面,签名算法只需要一个指数运算,不需要对运算;验证算法仅需要一个对运算和一个指数运算。同时,方案使用传统哈希函数代替一般无证书签名算法中使用的 Map-To-Point 哈希函数,提高了方案的效率。安全性方面,方案使用"绑定"技术[2],将用户公钥"绑定"到 H_2 哈希函数中,降低了公钥替换攻击的可能,提高了系统的安全性。同时,方案依赖于 q 强 Diffie-Hellman 困难问题(q-SDHP)和逆计算 Diffie-Hellman 困难问题(Inv-CDHP),并在随机预言机模型下,证明方案能够抵抗适应性选择消息攻击下的存在性伪造。

1 基础知识

1.1 双线性对

设 q 是大素数, G_1 和 G_2 是阶为 q 的加法循环群和乘法循

收稿日期:2008 - 11 - 28;**修回日期**:2009 - 02 - 14。 **基金项目**:教育部科学技术研究重点资助项目(208148);甘肃省教育厅重点资助项目(0801-01);西北师范大学青年教师科研基金资助项目(NWNU-QN-07-37)。

作者简介:张玉磊(1979 -),男,甘肃白银人,讲师,硕士研究生,主要研究方向:信息安全、现代密码学; 王彩芬(1963 -),女,河北安国人,教授,博士,主要研究方向:信息安全、电子商务协议; 张永洁(1978 -),女,甘肃武都人,讲师,硕士研究生,主要研究方向:信息安全; 程文华(1985 -),女,甘肃泾川人,硕士研究生,主要研究方向:信息安全; 韩亚宁(1985 -),女,甘肃环县人,硕士研究生,主要研究方向:信息安全。

环群。G_1 是GDH群,$P \in G_1$ 是 G_1 的生成元。设 a、b 是 Z_q^* 中的元素,假设在群 G_1、G_2 中的离散对数问题是难解的。一个双线性对是一个映射 $e:G_1 \times G_1 \to G_2$,满足下列性质:

双线性　$e(aP,bQ) = e(P,Q)^{ab}$;

非退化性　存在 P、$Q \in G_1$,使得 $e(P,Q) \neq 1$;

可计算性　对所有的 P、$Q \in G_1$,存在有效算法可以计算 $e(P,Q)$。

1.2 相关困难问题

定义 1　q 强 Diffie-Hellman 问题(q-SDHP)。在群 G_1 上,对于 $a,q \in Z_q^*$,$p \in G_1$,给定 $q+1$ 元组 $(P,aP,a^2P,\cdots,a^qP)$,计算一个对 $\left(c,\frac{1}{a+c}P\right)$,其中,$c \in Z_q^*$。

定义 2　算法 A 解 q-SDHP 成功的概率。$\Pr\left[A(P,ap,a^2P,\cdots,a^qP \mid a \in Z_q^*, P \in G_1) = \left(c,\frac{1}{c+a}P\right)\right] \geqslant \varepsilon$,称算法 A 以 ε 的优势解 q 强 Diffie-Hellman 问题。

定义 3　逆计算 Diffie-Hellman 问题(Inv-CDHP)。在群 G_1 上,对于未知的 $a \in Z_q^*$,$P \in G_1$,给定 P,aP,计算 $\frac{1}{a}P$。

假设 1　q 强 Diffie-Hellman 问题是不可解的。如果没有算法能在 t_1 时间内,以 ε_1 的优势解 G_1 上的 q 强 Diffie-Hellman 问题,则 q 强 Diffie-Hellman 问题是不可解的。

假设 2　逆计算 Diffie-Hellman 问题是不可解的。如果没有算法能在 t_2 时间内,以 ε_2 的优势解 G_1 上的逆计算 Diffie-Hellman 问题,则逆计算 Diffie-Hellman 问题是不可解的。

2 无证书签名方案的定义及敌手模型

2.1 无证书签名方案

一个无证书签名方案一般由七个算法组成[2]。

1)系统建立(Setup)算法,是一个概率算法。KGC 输入安全参数 k,输出系统主密钥 s 和系统参数 $Params$。

2)用户部分私钥生成(Partial-Private-Key-Extract)算法,是一个确定性算法。KGC 输入用户的身份标识符 ID、系统参数 $Params$ 和主密钥 s,输出用户部分私钥 D_{ID},并将 D_{ID} 通过秘密信道发送给用户。

3)秘密值生成(Set-Secret-Value)算法。用户输入系统参数 $Params$,输出一个秘密值 x。

4)用户私钥生成(Set-Private-Key)算法,是一个确定性算法。输入 ID、部分私钥 D_{ID}、秘密值 x 及系统参数 $Params$,输出用户的完整私钥 S_{ID}。

5)用户公钥生成(Set-Public-Key)算法,是一个确定性算法。输入系统参数 $Params$、用户身份 ID 及秘密值 x,输出用户公钥 P_{ID}。

6)签名(Sign)算法,是一个概率算法。输入消息 $m \in M$、用户身份 ID、私钥 S_{ID} 及系统参数 $Params$,输出用户对 m 的签名 σ。

7)验证(Verify)算法,是一个确定性算法。输入消息 m、签名 σ、用户身份 ID、公钥 P_{ID} 及 $Params$,若签名正确输出"真",否则输出"假"。

2.2 无证书签名方案的敌手模型

在无证书签名方案中,由于没有公钥证书,必须考虑两类具有不同能力的敌手:Type Ⅰ敌手 $A_Ⅰ$ 和 Type Ⅱ敌手 $A_Ⅱ$。$A_Ⅰ$ 不能获得系统主密钥,但它可以用自己选择的值替换任意用户的公钥,它刻画的是一般用户攻击者;$A_Ⅱ$ 能够获得系统主密钥,但不允许实现公钥替换攻击,它刻画的是一个恶意KGC。

3 一个有效的签名方案

在许多无证书签名方案中,都使用了 Map-To-Point 的哈希函数,将身份信息映射到椭圆曲线的某个点上。但是,这一类哈希函数的计算效率比较低。本文方案使用传统密码哈希函数代替 Map-To-Point 哈希函数,提高无证书签名方案的效率。

本文提出的无证书签名方案同样包括七个算法。

1)系统建立算法。给定安全参数 k,KGC 执行以下步骤:①定义群 G_1 和 G_2(阶均为素数 q),双线性对 $e:G_1 \times G_1 \to G_2$,选择生成元 $P \in G_1$;② 选择 $s \in Z_q^*$,计算 $P_{pub} = sP$ 和 $g = e(P,P)$;③ 选择两个哈希函数 $H_1:\{0,1\}^* \to Z_q^*$、$H_2:\{0,1\}^* \times \{0,1\}^* \times G_1 \times G_1 \to Z_q^*$。发布系统参数 $Params = \{G_1, G_2, e, q, P, P_{pub}, g, H_1, H_2\}$,消息空间为 $M = \{0,1\}^*$,主密钥为 s,系统密钥为 $P_{pub} = sP$。

2)用户部分私钥生成算法。KGC 计算 $Q_{ID} = H_1(ID)$,$D_{ID} = \frac{1}{s+Q_{ID}}P$,并将部分私钥 D_{ID} 通过安全信道发送给用户。

3)秘密值生成算法。用户选择一个随机值 $x \in Z_q^*$,产生用户秘密值 x。

4)用户公钥生成算法。用户计算 $PK_{ID} = x(P_{pub} + Q_{ID}P) = x(s+Q_{ID})P$,产生用户的公钥 PK_{ID}。

5)用户私钥生成算法。用户收到部分私钥 D_{ID},通过等式 $e(D_{ID}, P_{pub} + Q_{ID}P) = g$,验证 D_{ID} 的真实性,因为只有 KGC 知道系统主密钥 s。然后,生成用户的私钥对 (x, D_{ID})。

6)签名算法。算法输入 $Params$、用户身份 ID、私钥对 (x, D_{ID}) 和消息 m,执行下列步骤:① 选择一个随机值 $r \in Z_q^*$,计算 $R = g^r$,$h = H_2(m \| ID \| PK_{ID} \| R)$;② 计算 $V = \frac{r+h}{x}D_{ID} = \frac{r+h}{x}\frac{1}{s+Q_{ID}}P$。用户对消息 m 的签名为 $\sigma = (R,V)$。

7)验证算法。给定签名 $\sigma = (R,V)$、用户身份 ID、消息 m 和用户公钥 PK_{ID},执行下列步骤:① 计算 $Q_{ID} = H_1(ID)$,$h = H_2(m \| ID \| PK_{ID} \| R)$;② 验证 $e(V, PK_{ID})g^{-h} = R$ 是否成立,成立输出"真"并接收,否则终止。

4 本文方案的安全性及效率分析

4.1 正确性

方案的正确性可以通过以下等式验证:

$$e(V,PK_{ID})g^{-h} = e\left(\frac{r+h}{x}D_{ID}, PK_{ID}\right)g^{-h} =$$

$$e\left(\frac{r+h}{x}\frac{1}{s+Q_{ID}}P, x(P_{pub}+Q_{ID}P)\right)g^{-h} =$$

$$e\left(\frac{r+h}{x}\frac{1}{s+Q_{ID}}P, x(s+Q_{ID})P\right)g^{-h} =$$

$$e((r+h)P,P) = g^{r+h}g^{-h} = g^r = R$$

4.2 安全性证明与分析

定理　在随机预言机模型下,若无证书签名方案对 $A_Ⅰ$ 和 $A_Ⅱ$ 是存在性不可伪造的,则方案是安全的。

引理 1　若 q-SDHP 假设成立,则在随机预言机模型下,本文方案针对Ⅰ类攻击者 $A_Ⅰ$ 是存在性不可伪造的。

证明　假设有Ⅰ类攻击者 $A_Ⅰ$ 能够以一定得优势攻破本

文方案,则我们构建一个算法 B 利用 A_{I} 解决 q-SDH 问题。令 B 是 q-SDH 问题挑战者,A_{I} 是 Ⅰ 类攻击者,H_1 和 H_2 是随机预言机。B 的目标是对于身份 ID^* 和消息 M^*,能够生成有效签名解决 q-SDH 问题。

假设在群 G_1 上,给定 $q+1$ 元组 $(P,aP,a^2P,\cdots,a^qP)$ 作为 q-SDH 问题的输入,B 的目标可是以找到一个对 $\left(c,\frac{1}{a+c}P\right)$,其中 $a,c,q\in Z_q^*$,$P\in G_1$。

首先,选择生成元 $P'\in G_1$,利用以下过程计算对 $\left(y_i,\frac{1}{a+y_i}P'\right)$,其中 $y_1,y_2\cdots,y_{q-1}\in Z_q^*$,$P'\in G_1$[13]。

随机选择 $y_1,y_2\cdots,y_{q-1}\in Z_q^*$,有展开式 $f(x)=\prod_{i=1}^{q-1}(x+y_i)$,若 $c_0,c_1\cdots,c_{q-1}\in Z_q^*$,则有 $f(x)=\sum_{i=0}^{q-1}c_ix^i$。设 $P'=\sum_{i=0}^{q-1}c_i(a^iP)=f(a)P$,系统公钥 $P_{\mathrm{pub}}'=\sum_{i=1}^{q}c_{i-1}(a^iP)=aP'$,$a$ 是主密钥。B 展开 $f_i(x)=\frac{f(x)}{(x+y_i)}=\sum_{i=0}^{q-2}c_ix^i(1\leqslant i\leqslant q-1)$,有 $\sum_{i=0}^{q-2}c_i(a^iP)=f_i(a)P=\frac{f(a)}{a+y_i}P=\frac{1}{a+y_i}P'$,可以计算出对 $\left(y_i,\frac{1}{a+y_i}P'\right)$。

B 设 $g'=e(P',P')$,$P_{\mathrm{pub}}'=aP'$,a 为系统主密钥,对 B 保密。系统参数 $Params=\{G_1,G_2,e,q,P,P_{\mathrm{pub}},g,H_1,H_2\}$,$q_H$ 为 H_1 询问的最大次数。

H_1 询问:B 保持一个列表 $L_1=\{ID_i,Q_i\}$,初始为空,设 ID_i 是 A_{I} 对 H_1 的第 i 次询问。若 ID_i 在 L_1 列表中,返回对应 Q_i 值。否则,执行下列步骤:如果 $ID_i=ID^*$,B 选择 $Q^*\in Z_q^*$,且 $Q^*\notin\{Q_1,Q_2,\cdots,Q_{qh}\}$,将 Q^* 返回,并将 (ID_i,Q^*) 添加到表 L_1 中;否则,从 $\{Q_1,Q_2,\cdots,Q_{qH}\}$ 中选择一个值,返回给 A_{I} 并将 (ID_i,Q_i) 添加到表 L_1 中。

H_2 询问:B 保持一个列表 $L_2=\{m,ID,PK_{ID},R,h\}$,初始为空。A_{I} 提出对 (m,ID_i,PK_i,R_i) 的询问,若列表 L_2 中存在询问项,B 将 h 值返回给 A_{I};否则,B 随机选取 $h\in Z_q^*$,令 $h=H_2(m\|ID_i\|PK_i\|R_i)$,$B$ 将 h 返回给 A_{I},并将 (m,ID_i,PK_i,R_i,h) 添加到表 L_2。

部分密钥询问:A_{I} 提出对 ID_i 的询问,B 保持一个列表 $E=\{ID_i,Q_i,D_i\}$,初始为空。对于给定的 ID_i,B 从列表 L_1 获得元组 (ID_i,Q_i),若 $ID_i=ID^*$,B 终止并返回“失败”。否则,计算 $D_i=\frac{1}{a+Q_i}P'$,返回 D_i 给 A_{I},并将 (ID_i,Q_i,D_i) 添加到表 E。

公钥询问:B 保持一个列表 $L=\{ID_i,x_i,PK_i,t\}$,初始为空。当 A_I 询问 ID_i 的公钥时,B 检查 L 表中是否包含询问内容,若包含,返回 PK_i 给 A_{I}。否则,执行下列过程:如果 $ID_i=ID^*$,B 查表 L_1 获得元组 (ID^*,Q^*),并随机选择 $x^*\in Z_q^*$,计算 $PK^*=x^*(P_{\mathrm{pub}}'+Q^*P')$,返回 PK^* 给 A_{I} 并将 $(ID^*,x^*,PK^*,1)$ 添加到 L 表中;否则,B 查表 L_1 获得元组 (ID_i,Q_i),并随机选择 $x_i\in Z_q^*$,计算 $PK_i=x_i(P_{\mathrm{pub}}'+Q_iP')$,返回 PK_i 给 A_{I} 并将 $(ID_i,x_i,PK_i,1)$ 添加到 L 表中。

私钥询问:当 A_{I} 询问 ID_i 时,若 $ID_i=ID^*$,B 终止并返回“失败”。否则,若表 L 存在 (ID_i,x_i,PK_i,t) 项、表 E 存在 (ID_i,Q_i,D_i) 项,B 将 (x_i,D_i) 返回给 A_{I};若不存在,B 对 ID_i 进行部分密钥询问和公钥询问获得 (x_i,D_i),并将 (x_i,D_i) 返回给 A_I。

公钥替换询问:当 A_{I} 询问 (ID_i,PK_i') 时,若 L 中存在 (ID_i,x_i,PK_i,t) 项,B 将 PK_i 改为 PK_i',$t=0$,并将 (ID_i,x_i,PK_i',t) 添加到 L 表中。否则,B 作公钥询问获得 (ID_i,x_i,PK_i,t),然后设置 $PK_i=PK_i'$,假设 B 能够获得替换公钥 PK_i' 对应的秘密值 x_i',添加 (ID_i,x_i',PK_i',t) 到表 L。

签名询问:若 A_{I} 作 (m,ID_i,PK_i,R_i) 签名询问,B 查表 L_1 和 L,获得 (ID_i,Q_i) 和 (ID_i,x_i,PK_i,t),若 $ID_i=ID^*$,B 终止并返回“失败”。否则,执行下列过程:若 $t=1$,B 随机选取 $r_i\in Z_q^*$,计算 $R_i=g^{r_i}$,然后查表 L_2 得到 h_i,计算 $V_i=\frac{r_i+h_i}{x_i}D_i=\frac{r_i+h_i}{x_i}\frac{1}{a+Q_i}P'$,则签名为 $\sigma=(R_i,V_i)$,B 返回 σ 给 A_{I}。若 $t=0$,B 从 A_{I} 获得 x_i' 值。选取 $r_i\in Z_q^*$,计算 $R_i=g^{r_i}$,计算 $V_i=\frac{r_i+h_i}{x_i'}D_i=\frac{r_i+h_i}{x_i'}\frac{1}{a+Q_i}P'$,则签名为 $\sigma=(R_i,V_i)$,B 返回 σ 给 A_{I}。

最后使用分叉技术[14]:假设 ID^* 是 A_{I} 攻击目标的身份,ID 的公钥是 PK_{ID*},则 A_{I} 对消息 m 的伪造签名为 $\sigma=(R,V)$。通过重放技术,A_I 可以获得另一个有效签名 $\sigma'=(R,V')$,且有 $h\neq h'$。σ 和 σ' 满足下列等式:

$$e(V,PK_{ID*})g'^{-h}=e(V',PK_{ID*})g'^{-h'}\Leftrightarrow$$
$$e(V,PK_{ID*})e(V',PK_{ID*})^{-1}=g'^{(h-h')}\Leftrightarrow$$
$$e(V-V',PK_{ID*})=g'^{(h-h')}\Leftrightarrow$$
$$e(V-V',x^*(P_{\mathrm{pub}'}+Q^*P'))=e((h-h')P',P')\Leftrightarrow$$
$$e((V-V')x^*(a+Q^*),P')=e((h-h')P',P')$$

这样,B 能够成功计算 $(V-V')x^*(a+Q^*)=(h-h')P'$,有 $\frac{1}{a+Q^*}P'=(V-V')x^*(h-h')^{-1}$ 成立。对于 $Q^*\notin\{Q_1,Q_2,\cdots,Q_{qh}\}$,输出一个对 $\left(Q^*,\frac{1}{a+Q^*}P'\right)$。

这样,如果 A_{I} 能够攻破本文方案,B 利用 A_{I} 就可以得到 q-SDH 困难问题的一个解,出现矛盾。

引理2 若 Inv-CDHP 假设成立,则在随机预言机模型下,本文方案针对 Ⅱ 类攻击者 $A_{\mathrm{Ⅱ}}$ 是存在性不可伪造的。

证明 假设有 Ⅱ 类攻击者 $A_{\mathrm{Ⅱ}}$ 能够以一定得优势攻破本文方案,则我们构建一个算法 B 利用 $A_{\mathrm{Ⅱ}}$ 解决 Inv-CDH 问题。令 B 是 Inv-CDH 问题挑战者,有 $A_{\mathrm{Ⅱ}}$ 是 Ⅱ 类攻击者,H_1 和 H_2 是随机预言机。B 的目标是对于身份 ID^* 和消息 M^*,能够生成有效的签名解决 Inv-CDH 问题。

B 执行 Setup 算法,选择 $s\in Z_q^*$ 为系统主密钥,生成元为 $P\in G_1$。设 $g=e(P,P)$,$P_{\mathrm{pub}}'=sP$,$X=xP$,系统参数为 $Params=(G_1,G_2,e,g,P,P_{\mathrm{pub}},H_1,H_2)$,然后执行下列询问。

H_1 询问与 H_2 询问同引理1中的询问。

私钥询问:B 保持一个列表 $E_1=\{ID_i,x_i,D_i\}$,初始为空。对于给定的 ID_i,若 $ID_i=ID^*$,B 终止并返回“失败”。否则,若 L_1 和 L 中存在 ID_i 项,计算 $D_i=\frac{1}{s+Q_i}P$,返回 (x_i,D_i) 给 $A_{\mathrm{Ⅱ}}$,并将 (ID_i,x_i,D_i) 添加到表 E_1;若不存在对应项,B 对 ID_i 进行 H_1 询问和公钥询问,然后计算 $D_i=\frac{1}{s+Q_i}P$,返回 (x_i,D_i) 给 $A_{\mathrm{Ⅱ}}$,并将 (ID_i,x_i,D_i) 添加到表 E_1。

公钥询问:B 保持一个列表 $L=\{ID_i,Q_i,PK_i,x_i\}$,初始为

空。当 A_{II} 询问 ID_i 的公钥时,B 检查 L 表中是否包含询问内容,若包含,返回 PK_i 给 A_{II}。否则,执行下列过程:如果 $ID_i = ID^*$,B 查表 L_1 获得(ID^*, Q^*),计算 $PK^* = sX + Q^*X$,返回 PK^* 给 A_{II} 并将$(ID^*, Q^*, PK^*, \perp)$ 添加到 L 表中;否则,B 查表 L_1 获得 (ID_i, Q_i),并随机选择 $x_i \in Z_q^*$,计算 $PK_i = x_i(P_{\text{pub}} + Q_iP)$,返回 PK_i 给 A_{II} 并将(ID_i, Q_i, PK_i, x_i) 添加到 L 表中。

签名询问:A_{II} 作签名询问时,若 $ID_i = ID^*$,B 终止并返回“失败”。否则,B 查表 L、E_1 和 L_2,然后随机选取 $r_i \in Z_q^*$,计算 $V_i = \frac{r_i + h_i}{x_i}D_i = \frac{r_i + h_i}{x_i}\frac{1}{s + Q_i}P$,$R_i = e(V_i, PK_i)g^{-hi}$,则签名为 $\sigma = (R_i, V_i)$,B 返回 σ 给 A_{II}。

最后使用分叉技术:假设 ID^* 是 A_{II} 攻击目标的身份,ID 的公钥是 PK_{ID*},A_{II} 对消息 m 的伪造签名为 $\sigma = (R, V)$。通过重放技术,A_{II} 可以获得另一个有效签名 $\sigma' = (R, V')$,且有 $h \neq h'$。σ 和 σ' 满足下列等式:

$$e(V, PK_{ID*})g^{-h} = e(V', PK_{ID*})g^{-h'} \Leftrightarrow$$
$$e(V, PK_{ID*})e(V', PK_{ID*})^{-1} = g^{h-h'} \Leftrightarrow$$
$$e(V - V', PK_{ID*}) = g^{h-h'} \Leftrightarrow$$
$$e(V - V', PK_{ID*}) = e((h - h')P, P)$$

又 $PK^* = sX + Q^*X$,$X = xP$。这样,有$(V - V')(s + Q^*)x = (h - h')P$ 成立,B 能够成功计算 $\frac{1}{x}P = (V - V')(s + Q^*)(h - h')^{-1}$。$B$ 利用 A_{II} 可以得到 Inv-CDH 困难问题的一个解,出现矛盾。

由引理 1 和引理 2,定理 1 得证。

本文方案的安全性主要体现在两个方面:1)使用“绑定”技术将用户公钥“绑定”到 H_2 哈希函数中,降低了公钥替换攻击的可能;2)方案依赖于 q 强 Diffie-Hellman 困难问题(q-SDHP) 和逆计算 Diffie-Hellman 困难问题(Inv-CDHP),并在随机预言机模型下,证明了方案能够抵抗适应性选择消息攻击下的存在性伪造。因此,方案具有安全性保障。

4.3　效率分析

在一般的无证书签名方案中,pair 对计算很消耗时间。本文方案将 $g = e(P, P)$ 作为预运算并随系统参数发布,因此签名生成过程不需要 pair 对计算,签名验证过程仅需要一个 pair 对计算。同时,本文方案使用传统密码学哈希函数代替一般无证书方案中的 Map-To-Point 哈希函数,提高了方案的效率。在表 1 中,列出了本文方案与其他方案所需的运算量。其中 p 表示对运算,e 表示指数运算,s 表示乘运算。分析表 1 数据可知,本文方案的效率是比较高的。

表 1　运算量对比

方案	签名	验证	Map-To-Point 哈希函数
文献[2]	1p + 3s	4p + 1e	使用
文献[3]	2p + 3s	5p + 1e	使用
文献[6]	3s	4p	使用
文献[13]	2e + 1s	1p + 1e + 1s	不使用
文献[15]	1e + 1s	3p + 1e + 1s	不使用
本文方案	1e + 1s	1p + 1e + 1s	不使用

5　结语

本文提出了一个基于双线性对的无证书签名方案,方案签名过程只需要一个指数运算而不需要对运算,验证过程只需要一个对运算和一个指数运算,具有比较高的效率。在随机预言机模型下证明了方案能够抵抗适应性选择消息攻击下的存在性伪造。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology, LNCS 196. Berlin: Springer-Verlag, 1985: 47 - 53.

[2] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// Cryptology-Asiacrypt 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 452 - 473.

[3] HUANG XIN-YI, SUSILO W, MU YI, *et al*. On the security of certificateless signature schemes from Asiacrypt 2003 [C]// Cryptology and Network Security: CANS 2005, LNCS 3810. Berlin: Springer-Verlag, 2005: 13 - 25.

[4] YUM D H, LEE P J. Generic construction of certificateless signature [C]// Australasian Conference on Information Security and Privacy: ACISP 2004, LNCS 3108. Berlin: Springer-Verlag, 2004: 200 - 211.

[5] HU B C, WONG D S, ZHANG ZHEN-FENG, *et al*. Key replacement attack against a generic construction of certificateless signature [C]// Australasian Conference on Information Security And Privacy: ACISP2006, LNCS 4058. Berlin: Springer-Verlag, 2006: 235 - 246.

[6] ZHANG ZHEN-FENG, WONG D S, XU JING, *et al*. Certificateless public-key signature: Security model and efficient construction [C]// Fourth International Conference on Applied Cryptography and Network Security: ACNS 2006, LNCS 3989. Berlin: Springer-Verlag, 2006: 293 - 308.

[7] GORANTLA M C, SAXENA A. An efficient certificateless signature scheme [C]// Proceedings of Computational Intelligence and Security: CIS 2005, LNAI 3802. Berlin: Springer-Verlag, 2005: 110 - 116.

[8] YAP W-S, HENG S-H, GOI B-M. An efficient certificateless signature scheme [C]// Emerging Directions in Embedded and Ubiquitous Computing: EUC 2006, LNCS 4097. Berlin: Springer-Verlag, 2006: 322 - 331.

[9] GOYA G H. Proposta de esquemas de criptografia e de assinatura sob modelo de criptografia de cha publica sem certificado [EB/OL]. [2008 - 09 - 22]. http://www.ime.usp.br/~dhgoya/dis_denise.pdf.

[10] CAO XUE-FEI, PATERSON K G, KOU WEI-DONG. An attack on a certificateless signature scheme: Cryptology ePrint Archive, Report 2006/367 [R/OL]. (2006 - 10 - 25) [2008 - 09 - 12]. http://eprint.iacr.org/2006/367.

[11] PARK J H. An attack on the certificateless signature scheme from EUC workshops2006: Cryptology ePrint Archive, Report 2006/442 [R/OL]. (2006 - 11 - 24) [2008 - 09 - 12]. http://eprint.iacr.org/2006/442.

[12] RAFAEL C, RICARDO D. Two notes on the security of certificateless signatures [C]// Provable Security 2007, LNCS 4784. Berlin: Springer-Verlag, 2007: 85 - 102.

[13] ZHANG L, ZHANG F T, ZHANG F G. New efficient certificateless signature scheme [C]//Emerging Directions in Embedded and Ubiquitous Computing: EUC 2007, LNCS 4809. Berlin: Springer-Verlag, 2007: 692 - 703.

[15] 明洋,王育民. 有效的无证书签名方案[J]. 电子科技大学学报, 2008, 37(2): 175 - 177.

[14] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361 - 396.