一种改进的高效无证书短签名方案

左黎明[1,2] 陈祚松[1,2] 夏萍萍[1,2] 汤鹏志[1] 康文洋[1,2]
(华东交通大学理学院 南昌 330013)[1] (华东交通大学系统工程与密码学研究所 南昌 330013)[2]

摘 要 无证书密码体制解决了PKI(Public Key Infrastructure)证书密码体制中证书的存储和管理问题,同时有效地解决了基于身份的密码系统中的密钥托管问题,一直是密码学研究中的一个热点。鉴于传统的无证书数字签名方案容易遭受公钥替换攻击的问题,对传统的无证书数字签名的定义进行了改进,并在此基础上提出了一种基于新定义的无证书短签名方案。在Inv-CDH(Inverse Computational Diffie-Hellman)困难问题假设和随机预言机模型下证明了方案的安全性,随后对方案进行了实现。最后对所提方案与几种经典方案进行了效率分析和实验比较,结果表明所提方案的计算量小,效率较高,适用于计算能力和传输能力较弱的应用场景。

关键词 无证书密码体制,短签名,随机预言机模型
中图法分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.04.027

Improved Efficient Certificateless Short Signature Scheme

ZUO Li-ming[1,2] CHEN Zuo-song[1,2] XIA Ping-ping[1,2] TANG Peng-zhi[1] KANG Wen-yang[1,2]
(School of Science, East China Jiaotong University, Nanchang 330013, China)[1]
(SEC Institute, East China Jiaotong University, Nanchang 330013, China)[2]

Abstract Certificateless public key cryptography has always been a hot topic in cryptography research, which solves not only the problem of storing and managing certificates in the PKI (public key infrastructure) certificate cryptosystem but also the key escrow problem in the identity-based cryptography system. Aiming at the problem that the traditional certificateless digital signature scheme is susceptiable to the public key substitute attacks, the definition of traditional certificateless digital signature was improved, and a short signature scheme based on the new definition was proposed. It was proved that the scheme is secure under the difficult problem of Inv-CDH (inverse computational Diffie-Hellman) and random oracle model, and the scheme was implemented. Finally, efficiency analysis and experiment comparison with several classic schemes were carried out. The result shows that the scheme has low computational complexity and high efficiency, and is suitable for application scenarios with weak computing capability and transmitting capability.

Keywords Certificateless PKC, Short signature, Random oracle model

1 引言

在基于证书的传统公钥密码系统中,用户的证书发放和管理都是通过权威的证书中心(Certificate Authority,CA)实现的,但在这一传统的实现中大量的时间耗费在了用户公钥证书的传输和验证上。对此,Shamir[1]于1984年提出了基于身份的密码体制(Identity-Based Cryptography,IBC),IBC简化了CA公钥证书管理,所有的用户私钥都是通过一个可信的私钥生成器(Private Key Generator,PKG)生成的。这引出了一个密钥托管问题,即一旦PKG出现安全性问题,就可能导致整个基于身份的密码系统瘫痪。2003年,Al-Riyami等[2]提出了无证书密码体制(Certificateless PKC,CLPKC),该体制很好地解决了基于身份的密码体制中的密码托管问题。因此,无证书密码体制一经提出便成为了研究热点[3-7]。但是在CLPKC中,用户的公钥因为并没有直接验证,所以容易遭受不诚实用户发起的公钥替换攻击[8-10];另一方面,KGC(Key Generation Centre)知道系统主密钥,所以能够计算所有用户的部分私钥,这使得系统容易遭受恶意但被动的KGC攻击[11-13]。恶意用户在获得合法用户的部分私钥后,可以选择一个秘密值并按正常签名过程生成最终私钥、公钥和签名,并宣称自己就是合法用户,而其他人是无法区分的(即使KGC也只能分辨部分私钥是否正确),这正是传统无证书数字签名方案的缺陷所在。为避免公钥替换攻击,本文对传统的无证书数字签名的定义进行了改进,并在此基础上提出了一种基于新的无证书数字签名定义的短签名方案,进而在Inv-CDH困难问题假设和随机预言机模型下证明了该方案的安全性。

收稿日期:2018-03-21 返修日期:2018-05-25 本文受国家自然科学基金资助项目(11361024),江西省自然科学基金项目(20171BAB201009),江西省教育厅科技项目(GJJ161417,GJJ170386),江西省研究生创新专项资金项目(YC2017-S257)资助。
左黎明(1981-),男,硕士,副教授,CCF会员,主要研究方向为信息安全、非线性系统,E-mail:limingzuo@126.com(通信作者);**陈祚松**(1993-),男,硕士生,主要研究方向为信息安全;**夏萍萍**(1995-),女,硕士生,主要研究方向为信息安全;**汤鹏志**(1961-),男,硕士,教授,主要研究方向为信息安全;**康文洋**(1993-),男,硕士生,主要研究方向为信息安全。

2　预备知识

2.1　安全性假设

定义 1(Inv-CDH 问题)　给定 $b\in Z_q^*$ 和 P，$aP\in G_1$，其中 G_1 是循环加法群，$a\in Z_q^*$ 是未知的随机数，计算出 $\frac{1}{a+b}P\in G_1$ 是困难的。

定义 2(双线性映射)　假设 G_1 是由 P 生成的阶为 q 的循环加法群，其中 P 为 G_1 的生成元，q 为安全的大素数，G_T 为循环乘法群，则称映射 $e:G_1\times G_1\to G_T$ 是满足以下 3 条性质的双线性映射。

(1)双线性性：对于 $\forall a,b\in Z_q^*$，$\forall P,Q\in G_1$，有 $e(aP,bQ)=e(P,Q)^{ab}$；

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

(3)可计算性：$\forall P,Q\in G_1$，存在有效算法计算 $e(P,Q)$。

2.2　改进后的无证书数字签名的定义

原有的无证书数字签名[2]定义中，用户的部分私钥是 KGC 在系统参数建立完后，根据系统公开参数、系统主密钥和用户身份 ID 输出的。这一过程虽然是根据用户身份 ID 及其他参数生成的用户部分私钥，但并不能使用户的公钥得到直接的验证，当存在不诚实的用户或者恶意的 KGC 泄露了用户部分私钥时，签名方案容易遭受公钥替换攻击。

改进后的无证书数字签名方案由以下 7 个算法构成。

(1)系统参数建立：KGC 选择安全参数 k，然后计算相应的系统公开参数 $params$ 和系统主密钥 s_{kgc}。

(2)秘密值建立：用户在 KGC 公开的系统公共参数 $params$ 的空间内选择秘密值 x_{ID}，并根据秘密值 x_{ID} 计算用户的部分公钥 y_{ID}，然后将用户部分公钥 y_{ID} 发送给 KGC。

(3)部分私钥建立：KGC 根据系统公开参数 $params$、系统主密钥 s_{kgc}、用户身份 ID 和用户部分公钥 y_{ID}，计算出用户的部分私钥 d_{ID}，然后通过安全信道将其发给相应的用户。

(4)私钥建立：用户根据系统公开参数 $params$、用户的部分私钥 d_{ID} 和秘密值建立时选择的秘密值 x_{ID}，计算用户私钥 sk_{ID}。

(5)公钥建立：用户根据系统公开参数 $params$、选择的秘密值 x_{ID} 和部分公钥 y_{ID}，计算用户的公钥 pk_{ID}。

(6)签名：签名者根据系统公开参数 $params$、待签名信息 m、用户(签名人)身份 ID、用户公钥 pk_{ID} 和私钥 sk_{ID}，计算签名 S。

(7)验证：签名验证者根据系统公开参数 $params$、签名人的身份 ID、公钥 pk_{ID}、消息 m 和签名 S 验证签名。返回“1”，说明验证通过；返回“0”，说明验证失败。

与 Al-Riyami 和 Paterson 提出的无证书数字签名[2]的定义相比，改进后的无证书签名方案具有以下特点。

(1)秘密值建立算法是在部分私钥建立算法之前执行的。

(2)在秘密值建立时选择了秘密值 x_{ID} 的同时还计算了用户的部分公钥 y_{ID}。

(3)部分私钥建立是 KGC 根据系统公开参数 $params$、用户的身份 ID 和用户部分公钥 y_{ID} 输出的用户部分私钥 d_{ID}，间接地将用户部分私钥与用户选择的秘密值进行了绑定。

(4)公钥建立是用户根据系统公开参数 $params$、用户的秘密值 x_{ID} 和用户部分公钥 y_{ID} 输出用户公钥 pk_{ID}。

根据以上 4 点可知，通过提前运行秘密值建立了算法并生成了用户的部分公钥，然后将用户的部分公钥作为 KGC 生成用户的部分私钥的参数。这个过程使得 KGC 生成的用户部分私钥与用户选择的秘密值存在了间接关联，当存在不诚实的用户或恶意的 KGC 泄露了用户的部分私钥而导致遭受公钥替换攻击时，可以根据这个关联关系对公钥进行验证，从而判定用户公钥的真假。因此，改进的无证书数字签名的定义可以避免签名方案遭受公钥替换攻击。

2.3　无证书数字签名的安全模型

传统的无证书密码系统中有两种类型的敌手[14]：一种是不诚实的用户，即在不知道系统主密钥及用户部分私钥的情况下进行用户公钥替换攻击；另一种是恶意但被动的 KGC，即在不能替换用户公钥但知道系统主密钥和用户部分私钥的情况下进行恶意攻击。在改进的无证书数字签名方案的定义中，关于第一类攻击者和第二类攻击者的敌手能力和模型以及证明思路已经有诸多论述，详见文献[15]。本文讨论一种新的敌手模型。

定义 3(第三类攻击者)　攻击者无法替换用户的部分公钥，不知道系统主密钥，但可以知道用户的部分私钥。

定义 4(安全模型)　若不存在一个敌手 A 可以在概率多项式时间内以一个不可忽略的优势在游戏中获胜(其中敌手的优势指其获胜的概率)，则证明一个无证书数字签名可以抵抗适应性选择消息和身份的存在性伪造攻击。游戏交互过程如图 1 所示，询问过程可以适应性多项式有界次。

当满足以下条件时，A 赢得了这场游戏。

(1)ID^* 从未进行过秘密值建立询问。

(2)元组(m^*,S^*,ID^*,PK_{ID^*})并不是从签名预言机中得到的。

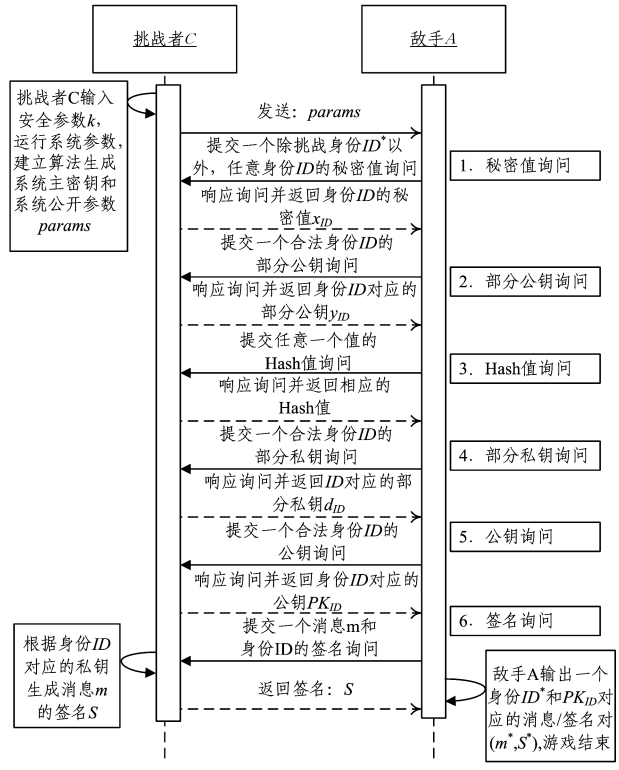

图 1　签名伪造游戏的过程图

Fig. 1　Process chart of signature forgery game

3 签名方案的构造

(1)系统参数建立:给定安全参数 k,KGC 选择一个安全的双线性映射 $e:G_1\times G_1\rightarrow G_T$,其中群 G_1 为素数 q 阶加法群,生成元为 g,G_T 为素数 q 阶乘法群。KGC 挑选安全 Hash 函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$,$H_2:\{0,1\}^*\times G_1\rightarrow Z_q^*$。KGC 随机选择 $x_{kgc}\in Z_q^*$ 作为系统主私钥,计算 $y_{kgc}=x_{kgc}g\in G_1$,并将其作为系统主公钥。KGC 公布系统参数$\{k,G_1,G_T,e,g,y_{kgc},H_1,H_2\}$,并保存系统私钥 x_{kgc}。

(2)秘密值建立:用户 A 选择一个随机数 $x_A\in Z_q^*$,并计算部分公钥 $y_A=x_Ag$,然后将用户身份 ID_A 和 y_A 发送给 KGC。

(3)部分私钥提取:KGC 计算 $K_A=H_1(ID_A,y_A)$,$d_A=\frac{K_A}{x_{kgc}+K_A}g$,然后通过安全信道将 d_A 发送给用户 A。

(4)私钥建立:用户将(x_A,d_A)作为私钥。

(5)公钥建立:用户计算 $T=y_{kgc}+K_Ag$,$Y=x_AT$,然后将(y_A,Y)作为用户公钥对外公开。

(6)签名:对给定消息 $m\in(0,1)^*$ 进行如下签名。

1)计算 $h=H_2(m,ID_A,Y)$;

2)计算 $S=\frac{1}{x_A+h}d_A$,则 S 为用户对消息 m 的签名。

(7)签名验证:对给定消息/签名对(m,S)进行如下验证。

1)计算 $K_A=H_1(ID_A,y_A)$,$h=H_2(m,ID_A,Y)$;

2)验证等式 $e(S,K_A^{-1}(Y+hT))=e(g,g)$。

验证方案正确性的过程如下:

$$\begin{aligned}&e(S,K_A^{-1}(Y+hT))\\&=e(S,\frac{(x_A+h)T}{K_A})\\&=e(S,\frac{(x_A+h)(y_{kgc}+K_Ag)}{K_A})\\&=e(\frac{K_A}{(x_A+h)(x_{kgc}+K_A)}g,\frac{(x_A+h)(x_{kgc}+K_A)}{K_A}g)\\&=e(g,g)\end{aligned}$$

4 安全性证明

定理 1 针对第三类攻击者,在随机预言机模型以及 Inv-CDH 困难问题假设下,本文方案可以抵抗适应性选择消息攻击下的存在性伪造攻击。

引理 1 假定敌手 A 经过有限次询问后在多项式时间 t 内以不可忽略的优势 ε 攻破了本文方案。记 q_X 和 t_X 分别为秘密值询问次数和一次询问所需的时间;记 q_Y 和 t_Y 分别为部分公钥询问次数和一次询问所需的时间;记 q_{H_i} 和 t_{H_i} 分别为敌手 A 询问 $H_i(i=1,2)$预言机的次数和一次询问所需的时间;记 q_E 和 t_E 分别为部分私钥解析询问次数和一次询问所需的时间;记 q_{pk} 和 t_{pk} 分别为公钥询问的次数和一次询问所需的时间;记 q_S 和 t_S 分别为签名询问的次数和一次询问所需的时间。因此,存在挑战者 C 在时间 $t'<t+(q_Xt_X+q_Yt_Y+q_Et_E+q_St_S+q_{pk}t_{pk}+2q_{H_1}t_{H_1}+2q_{H_2}t_{H_2})$ 内以 $\varepsilon'\geqslant(\varepsilon-\frac{1}{2^k})(1-\frac{1}{q_X})(1-\frac{1}{q_S})$的优势解决 Inv-CDH 问题。

证明:假设挑战者 C 挑战的 Inv-CDH 困难问题的实例为:给定 $b\in Z_q^*$ 和 P,$aP\in G_1$,其中 $a\in Z_q^*$ 未知,计算出$\frac{1}{a+b}P$。

设安全参数为 k,C 进行系统初始化,选择随机数 $x_{kgc}\in Z_q^*$ 作为系统主密钥,$y_{kgc}=x_{kgc}g$。C 挑选身份 ID^* 作为挑战身份,发送$\{k,G_1,G_T,e,g,y_{kgc},H_1,H_2\}$给敌手 A。假设 A 不会做相同的询问,且在私钥询问、公钥询问、签名询问和伪造签名之前都已经做过相应的 H_1 和 H_2 预言机询问,所有记录列表初始化为空。

(1)秘密值询问:C 维护一个列表 LX,记录结构为数组(ID_i,x_i,y_i)。当 A 提交一个关于 ID 的秘密值询问时:

1)若 $ID=ID^*$,C 终止模拟,并输出“FALSE”(记该事件为 E_1)。

2)若 $ID\neq ID^*$,查询列表 LX,若 LX 有记录,则返回相应记录中的 x_{ID} 给 A;否则随机选择 $x_{ID}\in Z_q^*$,计算 $y_{ID}=x_{ID}g$,返回 x_{ID} 给 A 并将(ID,x_{ID},y_{ID})添加到列表 LX。

(2)部分公钥询问:当 A 提交一个关于 ID 的部分公钥询问时:

1)若 $ID=ID^*$,C 返回 $y_{ID}=ag$ 给 A,并添加$(ID,\perp,ag)$到列表 LX 中,其中$\perp$表示空。

2)若 $ID\neq ID^*$,C 查询列表 LX,若 LX 有记录,则返回相应记录的 y_{ID}给 A;否则先执行秘密值询问,再返回相应的 y_{ID}给 A。

(3)H_1 预言机询问:C 维护一个列表 LH_1,记录结构为数组(ID_i,y_i,K_i)。当 A 提交一个关于(ID,y)的 H_1 询问时,若(ID,y,K)已经在 LH_1 中,则 C 向 A 返回 K_{ID};否则随机选择一个值 $K_{ID}\in Z_q^*$,将 K_{ID} 返回给 A,并将(ID,y_{ID},K_{ID})记录到列表 LH_1 中。

(4)部分私钥询问:当 A 提交一个关于身份 ID 的部分私钥询问时,C 先执行 H_1 预言机询问获得数组(ID,y_{ID},K_{ID}),计算 $d_{ID}=\frac{K_{ID}}{x_{kgc}+K_{ID}}g$,返回 d_{ID}给 A。

(5)公钥询问:C 维护列表 L_{pk},记录结构为数组(ID_i,y_i,K_i,Y_i)。当 A 提交一个关于身份 ID 的公钥询问时,C 检查列表中是否存在该询问值,若存在,则返回相应的值(y_{ID},Y_{ID})给 A,否则进行如下操作:

1)若 $ID=ID^*$,则 C 在LH_1 中找到数组(ID,y_{ID},K_{ID}),令 $Y_{ID}=x_{kgc}(y_{ID}+K_{ID}y_{ID})$并将其返回给 A,同时将数组$(ID,y_{ID},K_{ID},Y_{ID})$记录到列表 L_{pk};

2)否则,C 首先进行秘密值询问以获得相应的回答(ID,x_{ID},y_{ID}),然后进行 H_1 询问以获取数组(ID,y_{ID},K_{ID}),计算 $Y_{ID}=x_{ID}(y_{kgc}+K_{ID}g)$,将$(y_{ID},Y_{ID})$返回给 A,将 $(ID,y_{ID},K_{ID},Y_{ID})$记录到列表 L_{pk}中。

(6)H_2 预言机询问:C 维护一个列表 LH_2,记录结构为数组(ID_i,m_i,Y_i,h_i),当 A 向 C 提交关于(ID,m_{ID},Y_{ID})的 H_2 询问时,C 检查列表 LH_2 中是否已存在该询问值,若存在则返回相应的 h_{ID}给 A,否则:

1)当 $ID=ID^*$ 时,C 将 b 作为$H_2(ID,m_{ID},Y_{ID})$的值,返回 b 给 A,同时将(ID,m_{ID},Y_{ID},b)添加到列表 LH_2 中;

2)当 $ID\neq ID^*$ 时,C 随机选择 $h_{ID}\in Z_q^*$,将 h_{ID} 作为 H_2

(ID, m_{ID}, Y_{ID})的值，返回 h_{ID} 给 A，同时将$(ID, m_{ID}, Y_{ID}, h_{ID})$添加到列表 LH_2 中。

(7)签名询问：当 A 提交(ID, m_{ID})的签名询问时，C 进行如下操作：

1)若 $ID=ID^*$，则停止询问，返回“FALSE”，记该事件为 E_2；

2)若 $ID\neq ID^*$，C 从 LX 中获得记录(ID, x_{ID}, y_{ID})，从 L_{pk} 中获得记录$(ID, y_{ID}, K_{ID}, Y_{ID})$，然后从 LH_2 中获得记录$(ID, m_{ID}, Y_{ID}, h_{ID})$，计算 $S_{ID}=\frac{1}{x_{ID}+h_{ID}}d_{ID}=\frac{K_{ID}}{(x_{ID}+h_{ID})(x_{kgc}+K_{ID})}g$，并将其作为 C 对消息 m_{ID} 的签名 S_{ID}。

最后，A 停止询问，并输出一个 ID^* 的有效消息签名对(m_{ID^*}, S_{ID^*})。

1)若 $ID\neq ID^*$，则停止并输出“FALSE”；

2)否则 C 分别调出数组$(ID^*, y^*, K^*, Y_{ID^*})$和$(ID^*, m^*, K^*, Y^*, h^*)$，此时 $h^*=b, y^*=ag$。从而可以根据验证等式 $e(S_{ID^*}, K_{ID^*}^{-1}(Y_{ID^*}+h_{ID^*}T_{ID^*}))=e(g,g)$，即：

$$\begin{aligned}&e(S_{ID^*}, K_{ID^*}^{-1}(Y_{ID^*}+bT_{ID^*}))\\&=e(S_{ID^*}, \frac{(a+b)T_{ID^*}}{K_{ID^*}})\\&=e(S_{ID^*}, \frac{(a+b)(y_{kgc}+K_{ID^*}g)}{K_{ID^*}})\\&=e(S_{ID^*}, \frac{(a+b)(x_{kgc}+K_A)}{K_A}g)\\&=e(g,g)\end{aligned}$$

成功计算 $\frac{1}{a+b}g=\frac{x_{kgc}+K_{ID^*}}{K_{ID^*}}S_{ID^*}$，即将输出 $\frac{(x_{kgc}+K_{ID^*})}{K_{ID^*}}S_{ID^*}$ 作为对困难问题的解答，由此 C 解决了 Inv-CDH 问题。

以下分析 C 要成功解决困难问题的时间和优势：

(1)对于 H_1 和 H_2 的询问的答案是均匀且独立分布在 Z_q^* 内的，并且答案是有效的。

(2)只有当事件 E_1 和 E_2 不发生时，对秘密值询问和签名询问所得到的答案才是有效的。

(3)当事件 E_1 和 E_2 都不发生时，C 才能解决 Inv-CDH 问题的一个实例。因此，可得事件 E_1 和 E_2 都不发生的概率为：$\Pr(\neg E_1\wedge\neg E_2)=(1-\frac{1}{q_X})(1-\frac{1}{q_S})$。当 A 没有询问 H_2 而伪造了一个有效的签名时，这种模拟是存在漏洞的，其发生的概率为 $\frac{1}{2^k}$，因此 C 在该游戏中的优势为 $\varepsilon'\geqslant(\varepsilon-\frac{1}{2^k})(1-\frac{1}{q_X})(1-\frac{1}{q_S})$，运行时间为 $t'<t+(q_Xt_X+q_Yt_Y+q_Et_E+q_St_S+q_{pk}t_{pk}+2q_{H_1}t_{H_1}+2q_{H_2}t_{H_2})$。

5　方案的实现与效率分析

5.1　方案的实现

在 Windows 7 64 位操作系统下，基于微软 Visual Studio 2012 开发平台，用 C 语言实现了本文方案。方案的核心代码如下：

```
pairing_t pairing;//定义双线性对
//初始化双线性对
if (pairing_init_set_buf(pairing,eparam,strlen(eparam)))
printf("pairing init failed");
  //1.系统参数建立阶段
  element_random(xKgc);//随机选择 xKgc
  element_random(g);//选择生成元
  element_mul(yKgc,xKgc,g);//计算 yKgc=xKgc*g;
  //2.秘密值建立阶段
  element_random(xA);//选择随机数 xA
  element_mul(yA,xA,g);//计算 yA=xA*g;
  //3.部分私钥提取阶段
  char IDa[20]="czs_2018";
  element_from_hash(kA,IDa,strlen(IDa));
  element_mul(xKgc_kA,xKgc,kA);// (xKgc+kA);
  //计算(xKgc+kA)^-1
  element_invert(inv_xKgc_kA,xKgc_kA);
  //计算 temp=(xKgc+kA)^-1*kA;
  element_mul(temp,inv_xKgc_kA,kA);
  //计算 dA=(xKgc+kA)^-1*kA*g
  element_mul(dA,temp,g);
  //4.公钥生成阶段
  element_mul(kA_g,kA,g);//kA*g;
  //计算 T=(yKgc+kA*g)=(xKgc+kA)*g
  element_mul(T,xKgc_kA,g);
  element_mul(Y,xA,T);//计算公钥 Y=xA*T;
  //5.签名生成阶段
  char m[100]="Chen Zuosong SEC Institute,East China Jiaotong
              University,Nanchang 2018-1-15";
  element_from_hash(h,m,IDa,Y,strlen(m));
  element_add(xA_h,xA,h);//计算 xA+h
  element_invert(inv_xA_h,xA_h);//计算(xA+h)^-1
  //计算 S=(xA+h)^-1*dA
  element_mul(S,inv_xA_h,dA);
  //6.签名验证阶段
  element_invert(inv_kA,kA);//计算 kA^-1
  //计算 kA^-1*(xA+h)
  element_mul(temp2,inv_kA,xA_h);element_mul(temp3,temp2,
  T);//计算 kA^-1*(Y+h*T)
  //等式左边:e(S,kA^-1*(Y+h*T))
  element_pairing(left,S,temp3);element_pairing(right,g,g);//等
  式右边:e(g,g)
  // 左右比较
  if (!element_cmp(left,right))
  printf("验证成功!");//左右相同
```

5.2　效率分析

5.2.1　性能比较

本文方案与几种具有代表性的无证书签名方案的对比情况如表 1 所列，其中 Sm 表示标量乘运算，Pr 表示双线性对运算，Exp 表示指数运算。从表 1 中可知，本文方案在签名过程中进行了一个标量乘运算，签名验证过程中进行了两个标量乘和一个双线性对运算，相较于其他方案其效率更高。对于签名长度，本文方案通过选择阶长为 160 bits 的群和椭圆曲线上的双线性映射，实现了 160 bits 的签名长度，相较于其他方案其签名长度更短。

表 1 几个无证书签名方案的效率比较

Table 1 Comparison of efficiency of several certificateless signature schemes

方案	签名算法	验证算法	签名长度/bits
文献[2]	3Sm+1Pr	1Exp+4Pr	320
文献[16]	2Sm	2Sm+4Pr	320
文献[17]	2Sm	2Pr+2Sm	320
文献[18]	2Sm	1Sm+3Pr	320
本文方案	1Sm	2Sm+1Pr	160

5.2.2 运行效率分析

本文对几种无证书签名方案进行了实现，并在同一测试环境下多次运行以进行耗时比较，测试结果如表 2 所列。实验基准测试环境为：CPU 为 Intel i5 7500 3.4 GHz，内存为海力士 DDR3 1600 MHz 8 GB，主板为华硕 B85，操作系统为 64 位 Windows 7 操作系统。由表 2 可知，本文方案运行的平均总耗时约为 0.109 s，其中签名生成和签名验证所消耗的平均时间分别为 0.012 s，0.034 s。在方案总耗时方面，本文方案相比文献[2]方案减少了约 46.6%，相比文献[16]方案减少了约 54.2%，相比文献[17]方案减少了约 33.9%，相比文献[18]方案减少了约 42%。从以上运行结果可知，本文短签名方案的实际运行效率是较高的。

表 2 方案运行 100 次的平均耗时比较

Table 2 Average time-consuming comparison of schemes running 100 times

(单位：s)

方案	签名平均耗时	验证平均耗时	方案平均总耗时
文献[2]方案	0.053	0.102	0.204
文献[16]方案	0.027	0.151	0.238
文献[17]方案	0.024	0.061	0.165
文献[18]方案	0.025	0.079	0.187
本文方案	0.012	0.034	0.109

结束语 本文对传统的无证书数字签名的定义进行了改进，并在此基础上提出了一种基于新的无证书数字签名定义的短签名方案。在 Inv-CDH 困难问题假设和随机预言机模型下证明了方案的安全性，并对签名方案进行了实现，同时进行了效率分析，结果表明本文签名方案计算量小、效率较高。进一步的研究是在此基础上构造可证安全的基于云服务[19]的无证书短签名方案。

参 考 文 献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Workshop on the theory and application of cryptographic techniques. Berlin Heidelberg: Springer, 1984: 47-53.

[2] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin Heidelberg: Springer, 2003: 452-473.

[3] DU H, WEN Q. Efficient and provably-secure certificateless short signature scheme from bilinear pairings[J]. Computer Standards & Interfaces, 2009, 31(2): 390-394.

[4] ISLAM S K H, BISWAS G P. Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography[J]. International Journal of Computer Mathematics, 2013, 90(11): 2244-2258.

[5] HORNG S J, TZENG S F, HUANG P H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Information Sciences, 2015, 317(C): 48-66.

[6] DU H Z. A Secure and Efficient Certificateless Signature Scheme in the Standard Model[C]// The International Conference on Computer Science and Technology. Singapore: World Scientific, 2017: 278-286.

[7] KARATI A, ISLAM S H, KARUPPIAH M. Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments[J]. IEEE Transactions on Industrial Informatics, 2018, PP(99): 1-1.

[8] TSAI J L, LO N W, WU T C. Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings[J]. International Journal of Communication Systems, 2014, 27(7): 1083-1090.

[9] LIU E G, WANG X, ZHOU H J, et al. Improved Certificateless Proxy Blind Signature Scheme[J]. Computer Science, 2016, 43(8): 92-94. (in Chinese)
刘二根，王霞，周华静，等. 改进的无证书代理盲签名方案[J]. 计算机科学，2016，43(8)：92-94.

[10] CHANG S, LEE H S, LEE J, et al. Security Analysis of a Certificateless Signature from Lattices[J/OL]. http://www.hidawi.com/journals/scn/2017/3413567/.

[11] GONG P, LI P. Further improvement of a certificateless signature scheme without pairing[J]. International Journal of Communication Systems, 2015, 27(10): 2083-2091.

[12] BHATIA T, VERMA A K. Cryptanalysis and improvement of certificateless proxy signcryption scheme for eprescription system in mobile cloud computing[J]. Annals of Telecommunications, 2017, 72(9-10): 563-576.

[13] LI J, YUAN H, ZHANG Y. Cryptanalysis and Improvement for Certificateless Aggregate Signature[J]. Fundamenta Informaticae, 2018, 157(1-2): 111-123.

[14] HU X M, LIU Y, XU H J, et al. Analysis and Improvement of Two Certificateless Signature Scheme[J]. Journal of Chinese Computer Systems, 2016, 37(10): 2264-2268.

[15] ZHANG L, ZHANG F T. A Method to Constr-uct a Class of Certificateless Signature Schemes [J]. Chinese Journal of Computers, 2009, 32(5): 940-945.

[16] LI X, CHEN K, SUN L. Certificateless signatu-re and proxy signature schemes from bilinear pairin-gs[J]. Lithuanian Mathematical Journal, 2005, 45(1): 76-83.

[17] YAP W S, HENG S H, GOI B M. An efficient certificateless signature scheme[C]// International Conference on Embedded and Ubiquitous Computing. Berlin Heidelberg: Springer, 2006: 322-331.

[18] GORANTLA M C, SAXENA A. An efficient certificateless signature scheme[C]// Computational Intelligence and Security. Berlin Heidelberg: Springer, 2005: 110-116.

[19] ZHANF Y Q, LU W L, TANG C M. Research on An Efficient and Practical Cloud-based Digital Signature Scheme[J]. Netinfo Security, 2016, 2016(7): 1-6.