一种高效的无证书内容可提取签名算法

刘庆华 宋余庆 刘 毅
(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 针对内容可提取数字签名效率低的问题,提出一种基于无证书公钥密码体制的内容可提取签名算法。该算法采用无双线性对的设计思想,用椭圆曲线上的标量乘法运算取代了代价高昂的双线性对运算。同时,该算法在随机预言安全模型下是可证明安全的,能够抵抗适应性选择消息攻击。实验证明,该数字签名算法具有明显的效率优势和更好的实用性。

关键词 双线性对,无证书密码体制,内容可提取签名,离散对数问题,随机语言模型
中图法分类号 TP311 **文献标识码** A

Efficient Content Extraction Signature Scheme without Certification

LIU Qing-hua SONG Yu-qing LIU Yi
(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract For the problem of low efficiency of the existing content extraction signature scheme, based on the certificateless public key cryptography and using the scalar multiplication over elliptic curve group to replace the pairing, this paper proposed an efficient content extraction signature without pairing. The proposed scheme is proved existentially unforgeable under adaptive chosen-message attacks assuming in the random oracle model. Compared with known schemes built from pairings, our schemes are more efficiency and practicality.

Keywords Bilinear pairings, Certificateless public key cryptography, Content extraction signature, Discrete logarithm problem, Random oracle model

1 引言

相对于普通的数字签名而言,内容可提取签名在电子病历、电子商务等方面的应用具有明显的优势。目前,有人提出过一些内容可提取签名方案,如:在传统的基于公钥的密码体制下提出的内容可提取签名方案[1-3],基于身份的密码体制下提出的内容可提取签名方案[4,5]等。

传统的公钥系统中需要用数字证书来保证公钥和用户身份的一致性,这就不可避免地存在证书管理问题。基于身份的密码体制的数字签名方案的公钥是由用户身份决定的,身份的验证不需要证书来保证,所以解决了传统公钥密码体制下的证书管理问题,但是由于在基于身份的公钥密码体制中,用户的私钥由第三方来生成,这样就带来了用户密钥的托管问题,即用户必须完全信任第三方。

无证书公钥密码体制是传统公钥密码体制和基于身份的公钥密码体制的折中,其继承了两者的优点,即不需要证书,也不存在密钥托管问题。在无证书公钥密码体制研究中,绝大多数的数字签名方案都是基于代价很高的双线性对运算的,算法效率很低。为了解决算法的效率问题,目前主要研究方向是在保证算法安全的前提下,采用无双线性对运算的设计方案来设计签名算法,进而提高算法的效率。一种不含双线性对的内容可提取签名方案[6]就是基于无证书的且不需要双线性对运算的签名方案,但是该签名方案采用了大量的指数运算,运行效率仍然较低。

本文在现有的研究基础上,借鉴何[7]的数字签名方案,构造出一种新的基于椭圆曲线的无证书内容可提取签名方案,其安全性基于椭圆曲线上的离散对数问题(elliptic curve discrete logarithm problem, ECDLP)的难解性。由于椭圆曲线上的离散对数运算的高效性,本算法的效率与其他签名方案相比较,得到了明显的提高。

2 相关知识

2.1 椭圆曲线的基本方程

令 E/F_p 表示定义在有限域 F_p 上的椭圆曲线,定义如下:

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

其中 p 为素数。方程判别式为

$$\Delta = 16(4a^3 + 27b^2) \bmod p \neq 0$$

到稿日期:2012-10-27 返修日期:2013-03-23 本文受教育部博士点基金(20113227110010),江苏省普通高校研究生科研创新计划(CXZZ11_0575),校科研项目(1293000483),江苏省博士后科研计划(1202037C),吉林教育厅"十二五"科学技术研究项目(吉教科合字[2013]第448号)资助。

刘庆华(1987—),男,硕士生,主要研究方向为信息安全、嵌入式系统,E-mail:xuelang5321@163.com;宋余庆(1959—),男,教授,博士生导师,主要研究方向为数据库技术、医学图像处理、嵌入式系统;刘 毅(1979—),男,博士生,主要研究方向为嵌入式系统。

2.2 椭圆曲线上点的加法

设 $P,Q\in E/F_p$，l 是过 P,Q 两点的直线(如果 $P=Q$，则取 l 为过 P 点的切线)，则由于椭圆曲线是一条 3 次曲线，因此 l 必和 E/F_p 相交于第三点 R。令 l' 为过 R 和无穷远点的直线(即过 R 且与 x 轴垂直的直线)，则 l' 与 E/F_p 的第三个交点即为 P 与 Q 的和，记为 $P+Q$。

2.3 性质

对所有的 $P,Q\in E/F_p$，

(1)O 是加法的单位元，有 $O=-O$，其中 O 表示无穷远点。

(2)对椭圆曲线上任意一点 P，有 $P+O=O+P$。

(3)如果 $P=(x_1,y_1)$，那么就有 $-P=(x_1,-y_1-ax-b)$。

(4)如果 $Q=-P$，那么 $P+Q=O$。

(5)如果 $P\neq Q,Q\neq O,Q\neq -P,Q\neq P$，设 R 是过点 P 和 Q 的直线与 E/F_p 的交点，那么 $Q+P=-R$。

(6)Q 的倍数定义如下，在点 Q 做 E/F_p 的切线并找出另一点 S，定义 $Q+Q=2Q=-S$，结合(5)，类似地可以定义 $3Q=Q+Q+Q,\cdots,nQ=Q+Q+\cdots+Q$。

定理 1 设 E/F_p 是一条定义在有限域 F_p 上的椭圆曲线，L 是 K 的扩域，则 E/F_p 的全体有理点 $E(L)$ 在弦切律下构成一个交换群，其中单位元为无穷远点。

椭圆曲线的离散对数问题(elliptic curve discrete logarithm problem，ECDLP)：已知椭圆曲线 E 和点 G，随机选择一个整数 k，容易计算 $Q=k\times G$，但是给定 Q 和 G 计算 k 就非常困难。

3 基于椭圆曲线的无证书内容可提取数字签名(CLCES)

3.1 定义

无证书内容可提取数字签名由系统参数建立、部分密钥生成、设置秘密值、设置私钥、设置公钥、签名生成、签名抽取、签名验证 7 个算法组成。其中系统参数建立和部分密钥生成两个算法由 KGC(key generator centre)执行，而其他算法由签名或验证用户执行。算法描述如下：

系统参数建立：输入安全参数 k，输出系统的主密钥 msk 和系统公开参数 $params$。其中 msk 由 KGC 秘密保存，$params$ 向系统用户公开。

设置秘密值：输入系统参数 $params$ 和用户 A 的 ID_A，输出用户 A 的秘密值 x_A。

部分密钥生成：输入一个用户 A 的身份 ID_A、系统公共参数 $params$ 和系统主密钥 msk，输出用户 A 的部分私钥 D_A。

设置私钥：输入系统参数 $params$、用户 A 的 ID_A、秘密值 x_A 和部分私钥 D_A，输出用户的私钥 SK_A。

设置公钥：输入系统参数 $params$、用户 A 的 ID_A、秘密值 x_A 和部分私钥 D_A，输出用户的公钥 PK_A。

签名生成：输入系统参数 $params$、用户 A 的身份 ID_A、公钥 SK_A、公钥 PK_A、明文 M 和 $CEAS$，输出一个可抽取的全局签名 σ_{full}。

签名抽取：输入文档 M、全局签名 σ_{full}、抽取子集 $ext(i)$ 和公钥 PK_A，输出子文档 M' 的签名 σ_{ext}。

签名验证：输入子文档 M'、抽取的签名 σ_{ext} 和公钥 PK_A，输出验证结果。

3.2 实现过程

假设用户 A 的身份为 ID_A。

(1)系统参数建立(Setup)：输入安全参数 k，输出系统主密钥和系统参数 $params$。具体步骤如下：

(a)KGC 选择 k 位的素数 p，得到 $\{F_p,E/F_p,G,P\}$；

(b)KGC 选择 $x\in Z_n^*$ 作为系统主密钥 msk，即系统主密钥 $msk=x$，然后计算系统主公钥 $P_{pub}=xP$；

(c)KGC 选择哈希函数 $H_1:\{0,1\}^*\rightarrow Z_n^*$，$H_2:\{0,1\}^*\rightarrow\{0,1\}^k$，$H_3:\{0,1\}^*\rightarrow\{0,1\}^k$ 和 $H_4:\{0,1\}^*\rightarrow Z_n^*$；

(d)KGC 保存主密钥 msk，将系统公共参数 $params=\{F_p,E/F_p,G,P,P_{pub},H_1,H_2,H_3,H_4\}$ 公开。

(2)设置秘密值(Set-Secret-Value)：任意用户 A 随机选择 $x_A\in Z_n^*$ 作为其秘密值，计算 $P_A=x_A\cdot P$，然后将 P_A 传送给 KGC 用于部分私钥生成。

(3)部分密钥生成(Partial-Private-Key-Extract)：输入系统主密钥、用户传送过来的 P_A 和系统参数，输出用户 A 的部分私钥 D_A。具体步骤如下：

(a)KGC 计算 $h_A=H_1(ID_A,R_A,P_A)$，其中，$R_A=r_A\cdot P$，随机选择 $r_A\in Z_n^*$；

(b)KGC 计算 $s_A=r_A+h_Ax \bmod n$，然后将 $\{s_A,R_A\}$ 通过秘密渠道发送给用户 A。

(4)设置私钥(Set-Private-Key)：用户 A 将自己的秘密值 x_A 和 KGC 传送过来的 s_A 合并在一起作为用户的私钥 SK_A，即用户私钥 $SK_A=(x_A,s_A)$。

(5)设置公钥(Set-Public-Key)：用户 A 将 P_A 和 KGC 传送过来的 R_A 合并在一起作为用户的公钥 PK_A，即用户公钥 $PK_A=(P_A,R_A)$。

(6)签名生成(Sign)：设需要加密的明文为 $M=m_1,m_2,\cdots,m_n$，其中 $i\in(1,2,\cdots,n)$，代表子消息段在 M 中的编号。M' 表示提取后的消息，$i\in ext(i)$ 表示 M' 中所包含的 M 中子消息段编号的集合，$CEAS$ 是内容提取访问控制结构。签名者完成如下操作：

(a)对每个子消息 m_i，计算 $H_2(m_i,CEAS)$，并将 M 中子消息的顺序从左向右级联，然后计算级联后的值，即：$M'=H_3(\sum_{i=1}^{n}H_2(m_i,CEAS))$，其中 $\sum_{i=1}^{n}H_2(m_i,CEAS)$ 表示级联运算。

(b)随机选择 $l\in Z_n^*$，计算 $R=lP$。

(c)计算 $h=H_4(M',R,PK)$。

(d)判断 $\gcd(l+h,n)=1$ 是否成立，若不成立则返回(b)，否则继续。

(e)计算 $s=(l+h)^{-1}(x_A+s_A) \bmod n$。

(f)输出整体签名 $\sigma_{full}=(CEAS,R,s)$。

(7)签名抽取(Sign-Extract)：提取者收到签名者对 M 的整体签名 σ_{full} 后，按照签名生成算法中的操作(a)计算出总散列表值 M'，同时计算 $h_A=H_1(ID_A,R_A,P_A)$，$h=H_4(M',R,PK)$，验证 $s(R+hP)=P_A+R_A+h_AP_{pub}$，若不成立，则停止，否则执行如下步骤：

(a)根据 CEAS 构造 $ext(i)$。

(b)用 $M'=m'_1,m'_2,\cdots,m'_n$ 替代 $M=m_1,m_2,\cdots,m_n$，具体方法是：若 $i\in ext(i)$，则 $m'_i=m_i$，表示该子消息段是被提取的；否则，$m'_i=H_2(m_i,CEAS)$，表示该子消息没有被提取。

(c)输出提取之后的子消息 M' 的签名 $\sigma_{ext}=(M',CEAS,$

$ext(i)$,R,s)。

(8)签名验证(Verify):

验证者收到M'的内容提取签名σ_{ext}后,做如下验证操作:

(a)判断$ext(i)\in CEAS$是否成立,若成立,则继续,否则,终止算法。

(b)根据$ext(i)$和M'恢复总的散列值M'',具体方法是:首先判断$i\in ext(i)$是否成立,若成立,则用$H_2(m_i,CEAS)$恢复m'_i的值;否则,保持原值不变。然后按消息M'中的顺序从左向右级联,依照签名生成算法的操作(a)计算出级联后的散列值M''。

(c)计算$h_A=H_1(ID_A,R_A,P_A)$和$h=H_4(M',R,PK)$,验证等式$s(R+hP)=P_A+R_A+h_AP_{pub}$是否成立,若成立则签名通过,否则,签名无效。

4 算法分析

数字签名效果主要通过签名的正确性、安全性、签名效率等指标进行评价。

4.1 签名的正确性

本文主要从以下两个方面说明算法的正确性。

(1)确保签名算法中的M'值与验证算法中所恢复的M''值的一致性。

内容提取算法中对各个子消息的替换算法方法是:

$$m_i'=\begin{cases}m_i, & i\in ext(i)\\ H_2(m_i,CEAS), & i\notin ext(i)\end{cases}\tag{1}$$

验证算法中的恢复方法是:

$$m_i=\begin{cases}H_2(m_i,CEAS), & i\notin ext(i)\\ m_i', & i\in ext(i)\end{cases}\tag{2}$$

由式(1)和式(2)可知验证时各子消息段的值为$H_2(m_i,CEAS)$,与签名算法中保持一致。

(2)确保验证算法中等式的正确性

因为公钥$P_{pub}=x\cdot P$,且$s_A=r_A+h_Ax \bmod n$,所以有$s_A\cdot P=R_A+h_A\cdot P_{pub}$。因为$s=(l+h)^{-1}(x_{ID}+s_{ID}) \bmod n$,所以有等式左边$=s\cdot(R+hP)=(h+l)^{-1}\cdot(x_A+s_A)\cdot(l\cdot P+h\cdot P)=(h+l)^{-1}(x_A+s_A)(l+h)\cdot P=(x_A+s_A)P=x_AP+s_AP=P_A+s_A\cdot P=P_A+R_A+h_A\cdot P_{pub}=$右边。因此等式$s(R+hP)=P_A+R_A+h_AP_{pub}$是正确的。

算法的可终止性是显然的。通过上述分析可知,本方案是正确的。

4.2 签名的安全证明

本论文在文献[8]中的随机预言机安全模型下是可证明安全的,能够抵抗适应性选择消息攻击。以下给出在随机预言机安全模型下本方案的安全性证明。

由于在第一类攻击下的证明与第二类攻击下的证明过程类似,鉴于篇幅限制,本论文只给出在第一类攻击下的完整证明。

证明:如果存在攻击者A_1,以第一类攻击方式攻破上述算法。以A_1的能力构造一个算法F来解决ECDLP问题的一个实例,即给定(P,Q),求解$x\in Z_n^*$,使得$Q=x\cdot P$。以下演示算法F是如何利用A_1来求解x,进而解决EDCLP难题的。

在证明中,F扮演挑战者的角色,我们假设A_1在请求以ID为身份的用户的公钥PK_{ID}对消息M的签名时,必须先进行相应的数字摘要计算。

系统初始化:F首先运行系统建立系统参数$params=\{F_p,E/F_p,G,P,P_{pub}=Q,H_1,H_2,H_3,H_4\}$,然后$F$将$params$发送给$A_1$。

询问:A_1允许以多项式时间随时访问下列询问。这些询问由F模拟。

(1)创建用户询问:当A_1对ID_i进行创建用户询问时,F选择一个随机数$t\in\{1,2,\cdots,q_c\}$。当$i\neq t$时,F随机选择a,b,$c\in Z_n^*$,计算$R_i=a\cdot P_{pub}+b\cdot P$,$P_i=c\cdot P$,$s_i=b$,$x_i=c$,$h_i=H_1(ID_i,R_i,P_i)\leftarrow-a \bmod n$,然后返回$(ID_i,R_i,P_i,s_i,x_i,h_i)$,并添加$(ID_i,R_i,P_i,h_i)$到列表$L_{H_1}$中。注意此处$(R_i,s_i,h_i)$这3个量要满足等式$s_i\cdot P=R_i+h_i\cdot P_{pub}$。当$i=t$时,$F$随机选择$a$,$b$,$c\in Z_n^*$,计算$R_i=a\cdot P_{pub}+b\cdot P$,$P_i=c\cdot P$,$s_i=x_i=\perp$,$h_i=H_1(ID_i,R_i,P_i)\leftarrow-a \bmod n$,注意:此处由于不知道私钥,公钥也是随机选择的,因此会引起h_i的不一致。最后,将$(ID_i,R_i,P_i,s_i,x_i,h_i)$添加到$C\text{-}List$,将$(ID_i,R_i,P_i,h_i)$添加到$L_{H_1}$中。其中$C\text{-}List$和$L_{H_1}$初始化的值为空。然后将$(ID_i,R_i,P_i,h_i)$返回给攻击者$A_1$。

(2)部分私钥提取询问:如果ID_i没有被创建,则输出$\perp$。如果ID_i已经存在,且$i\neq t$,F返回部分私钥s_i;否则,F返回失败并终止模拟。

(3)公钥替换询问:A_1可以将用户i的公钥PK_i替换成自己选择的PK_i'。如果ID_i已经被创建,F将ID_i的原始公钥PK_i替换成PK_i';否则输出$\perp$;注意,替换公钥时不需要与新公钥相应的秘密值,同时替换后并不存入$C\text{-}List$中,而是存到表L_R中。

(4)秘密值提取询问:A_1进行秘密值提取算法询问时,输入ID_i,如果ID_i没有创建,则F输出$\perp$。如果已经创建且$i\neq t$,则F发送$x_i=c$给A_1;若$i=t$,则F返回失败并终止模拟。

(5)摘要计算请求询问:A_1对$w_i=(M'',R,PK_i)$进行摘要计算请求时,如果ID_i不存在被创建,则F输出$\perp$。否则,对于第i次H_4询问,如果$ID_i\neq ID_t$,F首先浏览$C\text{-}List$。若$(ID_i,R_i,P_i,s_i,x_i,h_i)$在$C\text{-}List$中,算法$F$随机选择$h\in Z_n^*$并令$h=H_4(M',R,PK_i)$。若$(ID_i,R_i,P_i,s_i,x_i,h_i)$不在$C\text{-}List$中,意味着用户的公钥已经被替换,则算法$F$会随机生成$a$,$b$,$c\in Z_n^*$,并且令$s=a$,$R=a^{-1}h_iP_{pub}$,$h=H_4(M'',R,PK_i)\leftarrow a^{-1}(r_i+x_i)$。如果$ID_i=ID_t$,$F$随机选择$\zeta\in\{0,1\}$,并设$\Pr[\zeta=1]=\xi$则$\Pr[\zeta=0]=1-\xi$。若$\zeta=1$,算法$F$随机选择$h\in Z_n^*$,并令$h=H_4(M',R,PK_i)$。若$\zeta=0$,$F$随机选择$a$,$b$,$c\in Z_n^*$,并且令$h=H_4(M',R,PK_i)\leftarrow a^{-1}(r_i+x_i)$。最后,$F$将$h$返回给$A_1$,并将$(ID_i,M',R_i,PK_i,h)$添加到$H_4\text{-}List$中(初始化时为空)。

(6)签名提取询问:当A_1对$(M',ID_i,H_4(w_i))$进行签名提取时,如果被询问的ID_i没有被创建,则F输出$\perp$。如果ID_i已经存在,则根据之前的假设,A_1已经进行过了H_4询问。如果$ID_i\neq ID_t$,且$(ID_i,R_i,P_i,s_i,x_i,h_i)$在$C\text{-}List$中,则$F$用相应的私钥对其进行签名。

若$(ID_i,R_i,P_i,s_i,x_i,h_i)$不在$C\text{-}List$中,说明原始的公钥已经被替换。则令$s=a$,$R=a^{-1}h_iP_{pub}$,输出$(R,s)$作为签名返回。如果$ID_i=ID_t$,若$\zeta=1$,$F$返回失败并结束模拟。否则,若$\zeta=0$,令$s=a$,$R=a^{-1}h_iP_{pub}$,然后将$(R,s)$作为签名返

回。

伪造：A_1 停止询问，并输出一个有效的签名 $S=\{R, s^{(1)}\}$，如果 $ID_i \neq ID^*$，则算法 F 失败并终止。否则，伪造成功，A_1 在游戏中获胜。然后，F 充分利用无证书签名的一般化 Forking 引理[9]，如果我们使用不同的 H_2，将上述模拟过程重放两次，得到另外两个有效的签名，分别是 $\{R, s^{(2)}\}$，$\{R, s^{(3)}\}$。然后我们有 $s^{(k)} \cdot (R+h^{(k)}P)=(P_i+R_i+h_iP_{pub})$，$k=1,2,3$。因为 $R=lP$，$P_i=r_iP$，$P_{pub}=xP$，所以有 $s^{(k)} \cdot (l+h^{(k)})=x_i+r_i+h_ix$，$k=1,2,3$。

在这些等式中，只有 l, r_i, x 是未知数，F 可以从上面 3 个线性无关的等式解出这 3 个未知数，输出 x，进而解决离散对数问题。

获胜的概率分析：事实上，若 F 成功，必须满足以下条件：

T_1：F 在模拟中没有终止。

T_2：(R,s) 是对 (ID^*, PK_{ID}^*, m^*) 的有效签名伪造。

T_3：q_s 并且 $\zeta=1$。

F 获胜的概率 $Adv_F^{ECDLP}=\Pr[T_1 \wedge T_2 \wedge T_3]=\Pr[T_1] \cdot \Pr[T_2 \mid T_1] \cdot \Pr[T_3 \mid T_1 \wedge T_2]$。如果事件 T_1 发生，则有：

F 在模拟过程中，进行部分私钥提取询问而没有失败的概率为 $(1-(1/q_c))^{q_{PKEx}}$，其中 q_{PKEx} 表示对部分私钥的询问次数。

F 在模拟过程中，进行秘密值提取而没有失败的概率为 $(1-(1/q_c))^{q_{VEx}}$，其中 q_{VEx} 表示对秘密值的询问次数。

F 在模拟过程中，进行签名询问而没有失败的概率为 $(1-(1/q_c)\xi) \geqslant (1-\xi)^{q_s}$，其中 q_s 表示对签名的询问次数。

所以，$\Pr[T_1] \geqslant (1-(1/q_c))^{q_{PKEx}+q_{VEx}}(1-\xi)^{q_s}$。另外，在 T_1 发生的前提下，我们将 T_2 发生的概率设为 ε，即 $\Pr[T_2 \mid T_1]=\varepsilon$，在 T_1 和 T_2 发生的前提下，T_3 发生的概率为 $\Pr[T_3 \mid T_1 \wedge \wedge T_2]=\xi/q_c$，所以有 $Adv_F^{ECDLP} \geqslant (1-(1/q_c))^{q_{PKEx}+q_{VEx}}(1-\xi)^{q_s} \cdot (\xi/q_c) \cdot \varepsilon$。因为 $(1-\xi)^{q_s}\xi$ 在 $\xi=1/(q_s+1)$ 取最大值，因此 $Adv_F^{ECDLP} \geqslant (1-(1/q_c))^{q_{PKEx}+q_{VEx}}(1-1/(q_s+1))^{q_s}(1/q_c(q_s+1))\varepsilon$。显然，由于 $(1-(1/q_c))^{q_{PKEx}+q_{VEx}}(1-1/(q_s+1))^{q_s}(1/q_c(q_s+1))$ 为常数，因此如果 ε 不可忽略，则 Adv_F^{ECDLP} 也不可忽略。与假设矛盾。证毕。

5 效率分析

本方案与文献[4-6]方案的效率分析中，由于算法的运行时间主要由幂模运算、标量乘法运算、双线性对运算和哈希函数决定，因此我们采用了与文献[7]相同的方法来计算运行效率，即先根据 Miracl 库[10]计算出幂模运算、标量乘法运算、双线性对运算和哈希函数的运行时间，然后根据不同方案中用到的不同运算的个数来计算各个方案的运行时间。

在计算不同运算的运行时间时，运行环境为：PIV 3-GHZ 处理器、512MB 内存、windows XP 操作系统。

为了达到相同的安全级别，基于双线性对运算采用定义在超奇异椭圆曲线 $E/F_p: y^2=x^3+x$ 上的 Tate 对运算，椭圆曲线的嵌入次数为 2，素数 p 满足 $2^{510}<p<2^{511}$，$p+1=12qr$，其中 $q=2^{159}+2^{17}+1$。基于 ECC 的标量乘法运算时采用素数 $p=2^{160}-2^{31}-1$。令 Par 表示双线性对运算，exp 表示幂模运算，sca 表示基于 ECC 的标量乘法运算，has 表示哈希函数运算，运行时间详见表 1。

表 1

运算	双线性对运算 (Par)	幂模运算 (exp)	标量乘法 (sca)	哈希函数 (has)
运行时间	20.04ms	5.31ms	2.21ms	3.04ms

得到不同运算的运行时间后，再找出文献[4-6]中的方案和本文方案中所用到的不同运算的个数，详见表 2。

表 2

方案	签名及截取算法	验证算法
文献[4]方案	2Par+4has	2Par+2has
文献[5]方案	1Par+1exp+2sca+3has	1Par+2sca+2has
文献[6]方案	5exp+4has	3exp+2has
本文方案	4sca+4has	3sca+2has

根据表 1 和表 2 中的数据，计算出不同方案的运行时间，详见表 3。

表 3

方案	签名及截取算法	验证算法
文献[4]方案	52.24ms	46.12ms
文献[5]方案	38.89ms	30.54ms
文献[6]方案	38.71ms	21.99ms
本文方案	21.00ms	12.71ms

由表 3 可以看出，与文献[4-6]相比，本方案在效率方面具有明显优势。

结束语 无证书内容可提取签名方法不仅具有内容可提取签名的优点，还解决了公钥体制下的证书管理问题，从整体上提高了效率。性能分析表明，本文提出的方案与现有的可截取签名方案相比，在计算效率方面具有较大的优势。本方法在电子病历和电子商务上具有较高的实用性和广泛的应用前景。

参 考 文 献

[1] Steinfeld R, Bull L. Content Extraction Signatures [C]// Proc. of the 4th International Conference on Information Security and Cryptology. Berlin, Germany: Springer-Verlag, 2001: 285-304

[2] Bull L, Stanski P, Mcg S D. Content Extraction Signatures Using XML Digital Signatures and Custom Transforms On-demand [C]// Proc. of the 12th International World Wide Web Conference. New York, USA: ACM Press, 2003: 170-177

[3] 梁成全，宋余庆，耿飙，等. 基于 ECC 的病历文档内容抽取签名方案的研究[J]. 计算机应用研究，2010，27(7)：2650-2653

[4] 蓝才会，王彩芬. 基于身份的可截取签名方案[J]. 计算机应用，2007，27(10)：2456-2458

[5] Ye Shu-ying, Ou Fu-na, Zhang Hai-ling. An ID-Based Content Extraction Signatures Without Trusted Party. Industrial Electronics and Applications(ICIEA)[C]// 2010 the 5th IEEE Conference on Digital Object Identifier. 2010: 1801-1804

[6] 曹素珍，王彩芬，陈小云，等. 一种不含双线性对的可截取签名方案[J]. 计算机工程，2012，38(3)：110-112

[7] He D B, Chen J H, Zhang R. Efficient and provably-secure certificateless signature scheme without bilinear pairings[R]. Report 2010/632. Cryptology ePrint Archive, 2010

[8] Al-Riyami S, Paterson K. Certificateless public key cryptography [C]// LNCS 2894: Proceedings of Asiacrypt'03. Berlin: Springer-Verlag, 2003: 452-473

[9] David P, Jacque S. Security Arguments for Digital Signatures and Blind Signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396

[10] Miracl. Multiprecision integer and rational arithmetic C/C++ library[OL]. http://indigo.ie/mscott/