高效的基于证书短签名方案①

吴晨煌 [1], 郭瑞景 [1], 陈智雄 [1,2]

[1](莆田学院 数学与应用数学系, 莆田 351100)
[2](福建师范大学 网络安全与密码技术重点实验室, 福州 350007)

摘 要: 针对高效的基于证书数字签名的构造问题, 基于 CDH 困难性假设, 构造了一个基于证书的短签名方案, 并在随机预言机模型下证明了其安全性. 通过与已有可证明安全的基于证书签名方案进行比较, 所构造的签名方案在效率上和长度上都是最优的.

关键词: 基于证书; 短签名; 无证书; 基于身份; 可证明安全; 密码学

Efficient Short Certificate-Based Signature Scheme

WU Chen-Huang[1], GUO Rui-Jing[1], CHEN Zhi-Xiong[1,2]

[1](Department of Mathematics, Putian University, Putian 351100, China)
[2](Key Lab of Network Security and Cryptology, Fujian NormalUniversity, Fuzhou 350007, China)

Abstract: Aiming at the construction problems of the efficient certificate-based signature scheme, based on the computational Diffie-Hellman assumption, an efficient short Certificate-Base signature scheme is proposed with provable security under the random oracle model. Moreover, compared with the available provable security certificate-based signature schemes, this scheme is optimal about the efficiency and the length of signature.

Key words: certificate-based; short signature; certificateless; identity-based; provably secure; cryptography

1 引言

在 2003 年欧洲密码会上, Gentry 首先提出了基于证书公钥密码系统(Certificate-Based Public Key Cryptography, CB-PKC)[1], 它克服了传统基于目录公钥系统(Directory-Based Public Key Cryptography)中的证书管理问题(如 PKI)[2]以及基于身份公钥密码系统(Identity-Based Public Key Cryptography, IB-PKC)中的密钥托管问题[3]. 此外, CB-PKC 还克服了无证书公钥密码系统(Certificateless Public Key Cryptography, CL-PKC)[4]中存在的信任级别不能达到最高级 3 级, 而只能达到 2 级[5]和存在拒绝解密(Denial of Decryption, DoD)攻击[6]等缺点. 而 CB-PKC 中对可信机构的信任级别达到最高的 3 级, 完全达到 PKI 的水平. 因此, 基于证书公钥密码系统(Certificate-Based Public KeyCryptography, CB-PKC)被认为是目前最好的公钥密码系统, 成为当前的研究热点之一.

目前, 国内外关于基于证书的签名方案还不是很多, 特别是国内发表的研究成果还很少. 2004 年, Kang 等[7]首先给出了基于证书数字签名的定义, 同时构造了两个基于证书签名方案, 其中一个利用多重签名(Multisignature)的思想来产生签名密钥, 另一个则利用聚合签名(Aggregate Signature)的思想产生签名密钥. Li 等[8]指出文献[7]中的利用多重签名思想构造的基于证书签名方案能够受到替换公钥攻击, 同时给出了一个改进方案, 但是效率偏低, 我们发现对该签名方案稍作修改, 则可减少一个对运算, 从而进一步提高效率. 2008 年, Liu 等[9]提出两个基于证书签名方案, 其中一个不使用双线性对, 另一个则是在标准模型下证明其安全性. 但是, Zhang 等[10]指出 Liu 等提出的无双线性对的签名方案是不安全的, 并对其进行了改进. 2009 年, Wu 等[11]给出一个由无证书签名(Certificateless Signatures, CLS)构造基于证书签名的一般性方法. 2011

① 基金项目:国家自然科学基金(61170246);福建省高校服务海西建设重点项目(2008HX03);福建省教育厅项目(JA12291,JB12179)
收稿时间:2012-07-25;收到修改稿时间:2012-08-24

年,王雯娟等人[12]基于 Schnorr 签名思想构造了一个新的基于证书签名方案, 签名效率相对较高, 但是签名长度较长. Li 等[13]构造了一个高效的基于证书短签名方案, 虽然签名长度只有一个群元素长度, 但是效率偏低. Liu 等[14]给出了一个效率相对较高的基于证书短签名方案, 遗憾的是, 文献[15]指出该签名方案能够收到替换公钥攻击. 最近, 李志敏等人也给出了一个高效的基于证书数字签名设计方案[16], 但是遗憾的是, 作者犯了一个概念性错误, 文中群被定义为加法群, 作者在签名算法中把群视作加法群, 然而在对应的验证算法中却把群又视作了乘法群, 这显然是不对的. 关于线性对的运算可参见文献[17]. 综上所述, 在现有的基于证书签名方案中普遍存在效率偏低且签名长度偏长等问题.

短签名方案由于其签名长度短的优势, 特别适用于通信带宽受限的场合, 在现实的网络传输中将占有更大的优势, 因此受到了众多学者们的关注. 本文在基于证书公钥系统中设计了一个高效的基于证书短签名方案.

2 预备知识

下面是本文将要用到一些相关的重要概念及符号说明.

(1) 符号说明

Z_n 表示模 n 的整数集合, Z_q^* 表示模 q 的整数乘法群($Z_q^* = Z_q \setminus \{0\}$), $x \in_R S$ 表示均匀随机地在集合 S 中选取元素 x, $\|$ 表示字符串的连接符, $\{0,1\}^*$ 表示任意长的二进制串组成的集合, 1_{G_2} 表示群 G_2 中的单位元, $|G|$ 表示群 G 的阶.

(2) 双线性对

假设 G_1 是 q 阶加法循环群, 其生成元是 P, 而 G_2 是一个 q 阶乘法循环群, 其中 q 为素数. 映射 $e: G_1 \times G_1 \to G_2$ 称为双线性对, 如果它满足下面几个性质:

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

2) 非退化性: 存在 $P \in G_1, Q \in G_1$ 使得

$$e(P,Q) \neq 1_{G_2};$$

3) 实效性: 对所有的 $S \in G_1, T \in G_1$, 存在计算 $e(S,T)$ 的有效算法.

(3) 几个困难性假设

群 G_1 上定义以下几个密码学中的困难性假设:

1) 离散对数问题(DLP): 对任意的 $Q \in G_1$, 求满足 $Q = nP$ 的 $n \in Z_q^*$.

离散对数问题困难性假设是指对于任意多项式时间算法 $\Re$ 能够成功解决 DLP 的概率是可忽略的.

2) 计算 Diffie-Hellman 问题(CDHP): 对任意的 $P, aP, bP \in G_1$, 其中 $a,b \in Z_q^*$, 计算 abP.

计算 Diffie-Hellman 问题困难性假设是指对于任意多项式时间算法 $\Re$ 能够成功解决 CDHP 的概率是可忽略的.

3 高效的基于证书短签名方案及安全性证明

3.1 签名方案

一个基于证书签名方案有三个参与者, 分别是: 证书生成中心(CGC, Certificate Generate Center), 签名者, 验证者. 签名方案由下面 5 个算法组成:

•$Setup$: CGC 设立系统参数:

1.选取加法群 G_1 和乘法群 G_2, 满足 $|G_1| = |G_2| = q$, P 是群 G_1 的生成元, q 为素数;

2.选取双线性对 $e: G_1 \times G_1 \to G_2$;

3.选取三个安全的 Hash 函数 $H: \{0,1\}^* \to G_1$, $H_1: \{0,1\}^* \to Z_q^*$, $H_2: \{0,1\}^* \to Z_q^*$;

4.选取系统主私钥 $s \in_R Z_q^*$, 计算系统公钥

$$P_{pub} = sP \in G_1.$$

此时, 系统的公开参数为:

$$\{G_1, G_2, P, P_{pub}, e, q, H, H_1, H_2\}.$$

•$UserKey-Gen$: 用户 ID_A 选取 $x_A \in_R Z_q^*$, 计算公钥 $PK_A = x_A P_{pub}$, 并把 PK_A 及相关身份信息发送给证书生成中心 CGC. PK_A 作为用户的公钥, x_A 作为用户私钥的一部分.

•$Certificate-Gen$: CGC 收到用户的公钥及身份等信息, 验证信息之后为用户生成公钥证书 $Cert_A = sQ_A = sH(ID_A \| PK_A)$. 并把 $Cert_A$ 通过安全信道发送给用户 ID_A. 则用户的私钥 $SK_A = (x_A, Cert_A)$, 其中 x_A 是用户自己选的秘密值, $Cert_A$ 是公钥证书.

•$Sign$: 用户 ID_A 要对消息 m 生成签名, 计算 $U = (h_1 - x_A h_2) Cert_A$, 其中 $h_1 = H_1(m \| ID_A \| PK_A)$, $h_2 = H_2(m \| ID_A \| PK_A)$, 则对应于消息 m 的签名为 $\sigma = (m, U)$.

注: 签名算法中之所以使用两个不同的 Hash 函数

H_1, H_2，因为两个不同的 Hash 函数，可以认为即使两个 Hash 函数的输入相同，但两者输出是不同的，而且输出结果具有一定的随机性.

•*Verify*：验证者要验证签名 $\sigma=(m,U)$ 的有效性，通过验证下面等式是否成立:

$$e(PK_A,Q_A)^{h_2}e(P,U)=e(P_{pub},Q_A)^{h_1}$$

其中 $Q_A=H(ID_A\|PK_A)$，

$$h_1=H_1(m\|ID_A\|PK_A),$$

$$h_2=H_2(m\|ID_A\|PK_A).$$

3.2 签名方案的安全性分析

定理 1. 本文的基于证书签名方案是正确的.

证明: $e(PK_A,Q_A)^{h_2}e(P,U)$

$$=e(x_Ah_2P_{pub},Q_A)e(P,(h_1-x_Ah_2)Cert_A)$$

$$=e(P_{pub},x_Ah_2Q_A)e(P_{pub},h_1Q_A-x_Ah_2Q_A)$$

$$=e(P_{pub},h_1Q_A)$$

$$=e(P_{pub},Q_A)^{h_1}$$

定理 2. 在随机预言机模型下，本文的签名方案能够抵抗型攻击，否则 CDH 问题可解.

证明: 假设 I 型攻击者为 A_I，任意给定的一个 CDH 问题实例: (P,aP,bP). 下面我们证明: 若 A_I 能够成功伪造签名，那么存在算法 $\Im$ 能够利用 A_I 的能力求出这个 CDH 问题实例的解: abP. 首先，$\Im$ 置 $P_{pub}=aP$，然后 Hash 函数 H_1,H_2 将充当预言机的角色并且这些预言机都是由 $\Im$ 来模拟的. $\Im$ 通过维护以下一些列表: $H-list$，H_1-list，H_2-list，$PK-list$，$Cert-list$ 来回答 A_I 的询问. 这些列表的元素形式分别是: (ID_i,PK_i,v_i)，(m_i,ID_i,PK_i,h_{1i})，(m_i,ID_i,PK_i,h_{2i})，(ID_i,PK_i,x_i)，$(ID_i,PK_i,Cert_i)$. 接下来，$\Im$ 回答 A_I 的询问的方法如下(其中 • 表示通配符，⊥ 表示该值为空):

(1) 公钥询问: 假设 A_I 向 $\Im$ 询问用户 ID_i 的公钥，则 $\Im$ 选择 $x_i\in_R Z_q^*$ 使得 $(\bullet,\bullet,x_i)$ 不在 $PK-list$ 中出现过，则把 (ID_i,x_iP,x_i) 保存到 $PK-list$ 中，同时把 x_iP 返回给 A_I.

(2) 替换公钥询问: 假设 A_I 欲替换用户 ID_j 的公钥为 PK_j，则 $\Im$ 把 (ID_j,PK_j,x_j) 保存到 $PK-list$ 中.

(3) Hash 函数 H 询问: 假设 A_I 向 $\Im$ 询问 (ID_i,PK_i) 对应的 Hash 值(不妨设在询问时 A_I 时，已对 ID_i 询问过公钥，或者对其公钥替换过，否则，$\Im$ 可自己询问一次. 下面的 H_1,H_2 询问类似.)，则 $\Im$ 选择 $v_i\in_R Z_q^*$ 使得 $(\bullet,\bullet,v_i)$ 不在 H_1-list 中出现过，则把 (ID_i,PK_i,v_i) 保存到 $H-list$ 中，同时把 v_iP 返回给 A_I. 特别地，若 A_I 向 $\Im$ 询问的目标用户 (ID^*,PK^*) 对应的 Hash 值，则 $\Im$ 把 (ID^*,PK^*,bP) 保存到 $H-list$，同时把 bP 返回给 A_I.

(4) Hash 函数 H_1 询问: 假设 A_I 向 $\Im$ 询问 (m_i,ID_i,PK_i) 对应的 Hash 值，则 $\Im$ 选择 $h_{1i}\in_R Z_q^*$ 使得 $(\bullet,\bullet,\bullet,h_{1i})$ 不在 H_1-list 中出现过，则把 (m_i,ID_i,PK_i,h_{1i}) 保存到 H_1-list 中，同时把 h_{1i} 返回给 A_I.

(5) Hash 函数 H_2 询问: 假设 A_I 向 $\Im$ 询问 (m_i,ID_i,PK_i) 对应的 Hash 值，则 $\Im$ 选择 $h_{2i}\in_R Z_q^*$ 使得 $(\bullet,\bullet,\bullet,h_{2i})$ 不在 H_2-list 中出现过，则把 (m_i,ID_i,PK_i,h_{2i}) 保存到 H_2-list 中，同时把 h_{2i} 返回给 A_I.

(6) 证书询问: 假设 A_I 向 $\Im$ 询问 (ID_i,PK_i) 对应的证书 $Cert_i$ 的值(不妨设在询问时，A_I 已对 ID_i 进行过 H 询问，否则，$\Im$ 可自己先询问一次.) 此时，$\Im$ 在 $H-list$ 找到记录 (ID_i,PK_i,v_i)，则把 v_iP_{pub} 返回给 A_I. 同时把 (ID_i,PK_i,v_iP_{pub}) 记录到 $Cert-list$ 中.

(7) 签名询问: 假设 A_I 向 $\Im$ 询问身份 ID_i 的对应于消息 m_i 的签名，则 $\Im$ 利用 ID_i 查询 $H-list$，H_1-list，H_2-list，$PK-list$ 和 $Cert-list$，若没有记录则自己询问一次. 接着产生模拟签名为 $U_i=v_ih_{1i}aP-v_ih_{2i}PK_i$，显然 U_i 能通过验证式.

在上述这些询问之后，假设攻击者 A_I 对于目标用户 ID^* 最终成功伪造了一个有效签名 (m^*,U^*)，而且 A_I 没有向 $\Im$ 询问过 ID^* 的对应于消息 m^* 的签名以及 ID^* 对应公钥的证书. 则 (m^*,U^*) 满足:

$$e(PK^*,Q^*)^{h_2^*}e(P,U^*)=e(P_{pub},Q^*)^{h_1^*}$$

从上式 $\Im$ 可计算得到 CDH 问题 (P,aP,bP) 的解 abP，具体如下:

注意到 $e(PK^*,Q^*)^{h_2^*}e(P,U^*)=e(P_{pub},Q^*)^{h_1^*}$

即: $e(P,h_2^*x^*bP)e(P,U^*)=e(P,h_1^*abP)$，

$$e(P,h_2^*x^*bP+U^*)=e(P,h_1^*abP),$$

也就是: $h_2^*x^*bP+U^*=h_1^*abP$，

则 $abP=h_1^{*-1}(h_2^*x^*bP+U^*)$.

定理 3. 在随机预言机模型下，本文的签名方案能够抵抗 II 型攻击，否则 CDH 问题可解.

证明: 证明思路与定理 2 的类似. 假设 II 型攻击者 A_{II} 及任意给定的一个 CDH 问题实例: (P,aP,bP). 若 A_{II} 能够成功伪造签名，那么存在算法 $\Im$ 能够利用 A_{II} 的能力求出这个 CDH 问题实例的解: abP. 首先，$\Im$ 置 $P_{pub}=sP$，并把 s 告诉 A_{II}. 在询问过程中置目标用户 ID^* 的公钥为 $PK^*=aP$，$H(ID^*,PK^*)=bP$. 然后 Hash 函数 H_1,H_2 将充当预言机的角色并且这些预言机

都是由 $\Im$ 来模拟的. 在进行若干询问之后, 假设攻击者 A_{II} 对于目标用户 ID^* 最终成功伪造了一个有效签名 (m^*,U^*), 而且 A_{II} 没有向 $\Im$ 询问过 ID^* 的对应于消息 m^* 的签名. 则 (m^*,U^*) 满足:

$$e(PK^*,Q^*)^{h_2^*}e(P,U^*)=e(P_{pub},Q^*)^{h_1^*},$$

从上式 $\Im$ 可计算得到 CDH 问题 (P,aP,bP) 的解 abP. 具体如下:

注意到 $e(aP,bP)^{h_2^*}e(P,U^*)=e(sP,bP)^{h_1^*}$,

即: $e(P,h_2^*abP)e(P,U^*)=e(P,h_1^*sbP)$,

$e(P,h_2^*abP+U^*)=e(P,h_1^*sbP)$,

则 $abP=(h_2^*)^{-1}(h_1^*sbP-U^*)$.

定理 4. 本文的签名方案在适应性选择消息、适应性选择身份以及替换公钥攻击下是不可伪造.

证明: 由定理 2 和定理 3 的证明可知, 只有同时知道公钥所对应的秘密值及其公钥证书的人, 即签名者, 才能生成一个有效的签名, 因此, 本文的签名方案是不可伪造的.

3.3 签名方案的效率分析

下面将本文签名方案与已有 4 个可证明安全的基于证书签名方案进行效率比较.

表 1　5 个可证明安全基于证书签名方案比较

方 案	签名算法	验证算法	签名长度
文[7]	$3M+3H$	$3BP+2SM+3H$	$3\|G_1\|$
文[8]	$1M+2SM+2H$	$4BP+3H$	$2\|G_1\|$
文[12]	$1M+1E+1H$	$3BP+3E+3H$	$\|G_1\|+\|Z_q\|$
文[13]	$1M+1H$	$4BP+1SM+2H$	$\|G_1\|$
本文	$1M+2H$	$3BP+2E+2H$	$\|G_1\|$

上表 1 中, 表示群中的标量乘运算; 表示群中的形如的同时标量乘运算; 表示群中的指数运算; 表示双线性对运算; 表示 Hash 函数运算; 表示群中元素的长度, 表示群中元素的长度. 从耗时角度, 这些运算的耗时次序如下: , 其中双线性对运算是最耗时的, 具体可参见文献[17].

从上表 1 可以看到, 本文签名方案无论是签名的效率还是签名的长度都优于现有的可证明安全的基于证书签名方案. 与文献[13]的方案比较, 虽然本文的方案多了一个 Hash 预算, 但是验证算法效率明显更高, 而且签名通常是一次签名多次验证的. 因此, 本文的方案更具优势.

4 结语

基于证书数字签名是当前的研究热点之一, 本文基于 CDH 问题构造了一个高效的基于证书短签名方案. 但是, 目前具有附加性质的基于证书数字签名方案还不多, 因此研究更多、更高效的具有附加性质的基于证书签名方案是值得继续研究的.

参考文献

1 Gentry C. Certificate-based Encryption and the Certificate Revocation Problem. Cryptology-Eurocrypt 2003. LNCS 2656, Berlin: Springer-Verlag, 2003: 272–293.

2 Gutmann P. PKI: It's not Dead, Just Resting. IEEE Computer, 2002,35(8):41–49.

3 Shamir A. Identity-Based Cryptosystems and Signature Schemes. Crypto 1984. LNCS 196, Berlin: Springer-Verlag, 1984: 47–53.

4 Al-Riyami S, Paterson K. Certificateless Public Key Cryptography. Asiacrypt 2003. LNCS 2894, Berlin: Springer-Verlag, 2003: 452–473.

5 Girault M. Self-certified Public Keys. Eurocrypt 1991. LNCS 547, Berlin: Springer-Verlag, 1991: 490–497.

6 Liu J, Au M, Susilo W. Self-Generated-Certificate Public Key Cryptography and Certificateless Signature/Encryption Scheme in the Standard Model. Proc. of the 2nd ACM Symposium on Information, Computer and Communications Security, 2007: 273–283.

7 Kang B, Park J, Hahn S. A Certificate-Based Signature Scheme. CT-RSA 2004. LNCS 964, Berlin: Springer-Verlag, 2004: 99–111.

8 Li J, Huang X, Mu Y, et al. Certificate-Based Signature: Security Model and Efficient Construction. EuroPKI 2007. LNCS 4582, Berlin: Springer-Verlag, 2007: 110–125.

9 Liu K, Baek J, Susilo W, et al. Certificate-Based Signature Schemes Without Pairings or Random Oracles. 2008, http://eprint.iacr.org/275.

10 Zhang J. On the Security of a Certificate-Based Signature Scheme and its Improvement with Pairings. ISPEC 2009. LNCS 5451, Berlin: Springer-Verlag, 2009: 47–58.

11 Wu W, Mu Y, Susilo W, et al. Certificate-Based signatures revisited. Journal of Universal Computer Science, 2009, 15(8):1659–1684.

(下转第 145 页)

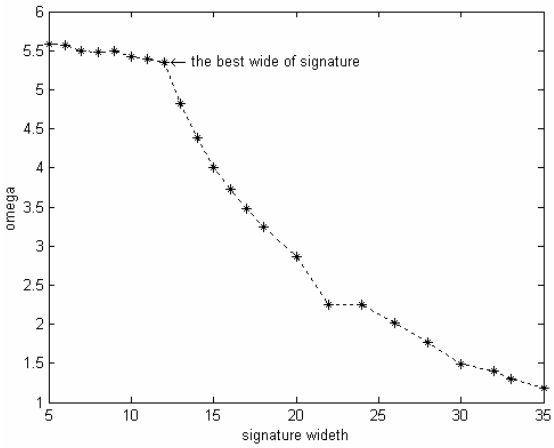

图 3 宽度为 12 的特征提取过程

按照 MS-PADS 提取算法，先选择 30 组多重随机参数作为迭代开始的初始位置，宽度初始设置为 35byte，在 30 组初始选择的随机开始位置中选取匹配分数最高的第 17 组作为最优的迭代结果，再不断减少特征宽度. 从图 3 可以看出，实验提取了 code-red II 中最大部分的序列，提取每个位置出现概率最大值还原为 http/1.0\r\n；当在流中把该部分去掉后继续运行该算法，得到图 4 所示提取过程，其提取的特征部分还原出来为.ida?，流中余下部分的特征提取过程类似.

经过实验评估，采用 MS-PADS 提取出的 PADS 特征码具有高检测精度及适用范围广等特点.

4 结语

目前在多态蠕虫的特征码提取研究中，PADS 在容忍性和检测新攻击方面优势突出. 本文针对单一 PADS 特征表征多态蠕虫特定性不足，探讨了多态蠕虫特征码的自动提取算法，分析了 PADS 特征片段长度判定方法. 该算法能在高噪声情况下产生良好的特征，提取速度快，具有很强的容错能力，可应用于病毒或攻击特征的提取过程，具有广泛应用前景.

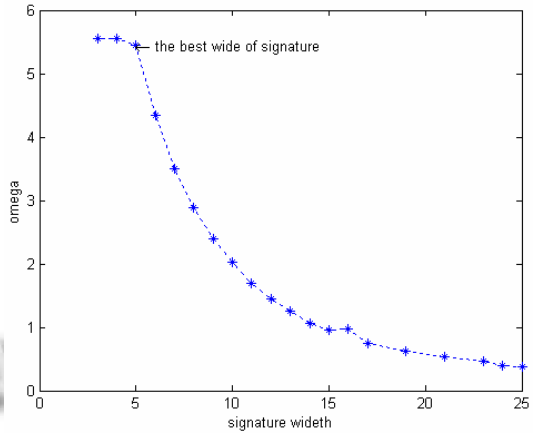

图 4 宽度为 5 的特征提取过程

参考文献

1 盛津芳,谭云桥,王斌.网络攻击中多态变形技术分析及其对抗策略.计算机安全,2007,1:11–13.

2 祝仰金,秦拯.Zero_day 多态蠕虫特征自动提取技术研究.微计算机信息,2011,27(1):198–200.

3 赵旭,何聚厚.Polymorphic 蠕虫特征自动提取算法及检测技术研究.计算机工程与应用,2008,44(36):106–108.

4 Tang Y, Chen SG. An Automated Signature-Based Approach against Polymorphic Internet Worms. IEEE Trans. on Parallel & Distributed Systems, 2007,18(7): 879 –892.

5 Hideo K, Genya K. Gibbs sampling methods for Bayesian quantile regression. Journal of Statistical Computation & Simulation, 2011,81(11):1565–1578.

(上接第 132 页)

12 王雯娟,黄振杰,郝艳华.一个高效的基于证书数字签名方案.计算机工程与应用,2011,47(6):89–92.

13 Li J, Huang X, Zhang Y, et al. An Efficient Short Certificate-Based Signature Scheme. The Journal of Systems and Software, 2012,85:314–322.

14 Liu J, Baek J, Susilo W, et al. Short and Efficient Certificate-Based Signature. Networking 2011 Workshops, LNCS6827, Berlin: Springer-Verlag, 2011: 167–168.

15 Cheng L, Xiao Y, Wang G. Cryptanalysis of a Certificate-Based on Signature Scheme. Procedia Engineering, 2012, 29:2821–2825.

16 李志敏,徐馨,李存华.高效的基于证书数字签名设计方案.计算机应用研究,2012,29(4):1430–1433,1444.

17 Barreto P, Kim H, Lynn B, et al. Efficient Algorithms for Pairing Based Cryptosystems. Crypto 2002. LNCS 2442, Berlin: Springer-Verlag, 2002: 354–368.