·安全技术· 文章编号：1000-3428(2019)12-0114-05 文献标志码：A 中图分类号：TP309

一种可证安全的短盲签名方案

左黎明[a,b]，夏萍萍[a,b]，陈祚松[a,b]

（华东交通大学 a. 理学院；b. 系统工程与密码学研究所，南昌 330013）

摘 要： 无线网络环境下电子现金、电子投票和电子票据保护等应用场景存在传输带宽受限、超低功耗设备计算性能弱以及传输能力差等问题。为此，通过简化盲化过程和签名过程，提出一种高效的短盲签名方案，并在计算性 Diffie-Hellman 困难问题假设和随机预言机模型下证明其安全性。分析结果表明，与典型同类方案相比，该方案计算量较小，签名较短，适用于计算能力和传输能力均受限的应用场合。

关键词： 数字签名；盲签名；双线性对；短签名；计算性 Diffie-Hellman 问题

开放科学(资源服务)标志码(OSID)：

中文引用格式： 左黎明，夏萍萍，陈祚松. 一种可证安全的短盲签名方案[J]. 计算机工程，2019，45(12)：114-118.

英文引用格式： ZUO Liming，XIA Pingping，CHEN Zuosong. A provably secure short blind signature scheme[J]. Computer Engineering，2019，45(12)：114-118.

A Provably Secure Short Blind Signature Scheme

ZUO Liming[a,b]，XIA Pingping[a,b]，CHEN Zuosong[a,b]

（a. School of Science；b. Research Institute of System Engineering and Cryptography，East China Jiaotong University，Nanchang 330013，China）

【Abstract】 In the wireless network environment，applications of blind signature such as digital cash，digital voting and digital invoice protection are challenged by limited transmission bandwidth，weak transmission capabilities and poor computing performance of ultra-low-power devices. To address the problem，an efficient short blind signature scheme is proposed. The scheme simplifies the blinding procedure and signing process，and its security is proven under the Computational Diffie-Hellman(CDH) assumption and the random oracle model. Analysis results show that compared with other similar typical schemes，the proposed scheme reduces the amount of computations and the length of signature，making it applicable to scenarios with limited computational capabilities and transmission capabilities.

【Key words】 digital signature；blind signature；bilinear pairings；short signature；Computational Diffie-Hellman(CDH) problem

DOI： 10.19678/j.issn.1000-3428.0053144

0 概述

1983 年，CHAUM D 用盲签名方案来构建电子现金系统[1]，在这种机制中，签名者并不知道他所签发文件的具体内容，也无法将签名过程和最终的签名相对应。盲签名作为一种特殊的数字签名，其因具有盲性的特点，可保障签署信息的匿名性，被广泛应用于电子现金、电子投票、电子票据保护等方面[2-3]。随着微电子技术和无线网络的发展，上述应用场景中会配置许多超低功耗的微型无线设备，由于此类设备普遍存在计算能力弱、传输能力受限和传输不稳定等缺点，因此适合使用短签名方案。自从短签名方案[4]被提出以来，目前多数相关研究与分析[5-7]都是围绕文献[4]基础方案展开，或根据具体应用场景在其基础上构造特定方案[8-9]。此外，文献[10]提出一种可恢复消息的盲签名方案，其中原消息无需随签名发送，可有效缩短签名长度。

相对于普通盲签名方案，短盲签名的构造比较困难，难点在于为保证签名的长度较短不能增加额外的辅助验证信息。本文针对使用低功耗无线设备进行数据签名和交互传输的移动环境，通过简化盲化和签名过程，提出一种可证安全的短盲签名方案。

1 基础知识

定义 1 双线性对

在双线性映射中，令 k 为一个安全参数，q 为一

基金项目： 国家自然科学基金(11761033)；江西省教育厅科技项目(GJJ161417，GJJ170386)。

作者简介： 左黎明(1981—)，男，副教授、硕士，主研方向为信息安全、非线性系统；夏萍萍、陈祚松，硕士研究生。

收稿日期： 2018-11-14 **修回日期：** 2018-12-20 **E-mail：** limingzuo@126.com

个 k bit 素数,G_1是由 P 生成的阶为素数 q 的循环加法群,$Q \in G_1$,G_2是有相同阶 q 的循环乘法群,则双线性映射 $e:G_1 \times G_1 \rightarrow G_2$ 满足以下性质:

1)双线性性:对于任意 $a,b \in \mathbb{Z}_q^*$,有 $e(aP,bQ) = e(P,Q)^{ab}$。

2)非退化性:$e(P,Q) \neq 1$。

3)易计算性:存在有效算法计算 $e(P,Q)$。

定义 2　计算性 Diffie-Hellman(Computational Diffie-Hellman,CDH)问题

已知 G_1 为由 g 生成的 q 阶循环加法群,未知随机数 $a,b \in \mathbb{Z}_q^*$,给定 $ag \in G_1$ 和 $bg \in G_1$,求解 abg 是困难的。

定义 3　安全模型

如果不存在概率多项式时间算法(敌手 A)以一个不可忽略的优势在图 1 所示的游戏中获胜,则称盲签名在适应性选择消息和身份攻击下是存在性不可伪造的。

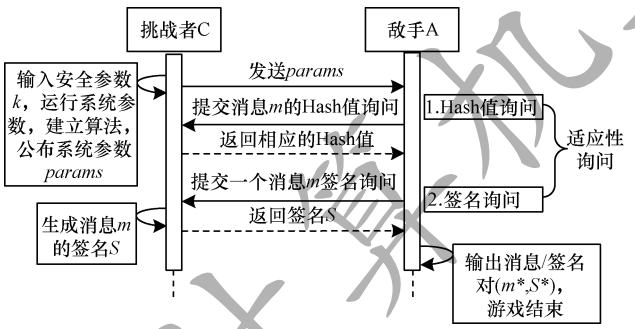

图 1　安全游戏

2　短盲签名方案的构造

本文提出的短盲签名方案具体描述如下:

1)系统参数建立。给定安全参数 k,选择 2 个阶都为素数的群 G_1 和 G_2(其中 G_1 的生成元为 g)、双线性映射 $e:G_1 \times G_1 \rightarrow G_2$,以及安全的抗碰撞哈希函数 $H:\{0,1\}^* \rightarrow G_1$,公布系统参数$\{k,G_1,G_2,g,H\}$。

2)用户私钥生成。系统密钥管理中心为每个用户秘密选择随机数 $x \in \mathbb{Z}_q^*$ 作为私钥,计算 $y = xg$ 作为公钥,将 x 通过安全渠道发送给用户,公开用户公钥 y。以下假设签名者为 A,用户身份为 ID_A,密钥对为(x_A,y_A),签名消息持有者为 B。A 给由 B 提供的消息 m 进行签名。

3)消息盲化。B 计算 $h = H(ID_A,y_A,m)$,随机选择 2 个秘密值 $u,v \in \mathbb{Z}_q^*$,计算 $V = vg$,$\lambda = uh + V$,将 λ 发送给 A。

4)签名。A 计算 $S_1 = x_A\lambda$,将 S_1 发送给 B。

5)脱盲。B 计算 $S_2 = S_1 - vy_A$,$S = u^{-1}S_2$,则 S 为最终 A 对消息 m 的签名。

6)验证。任何第三方对消息签名对(m,S),计算 $h = H(ID_A,y_A,m)$,验证等式 $e(S,g) = e(h,y_A)$,等式成立则接受签名,否则拒绝签名。正确性验证过程如下:

$$\begin{aligned} e(S,g) &= e(u^{-1}S_2,g) = e(u^{-1}(S_1 - vy_A),g) = \\ &e(u^{-1}(x_A\lambda - vy_A),g) = \\ &e(u^{-1}(x_A(uh+V) - vy_A),g) = \\ &e(u^{-1}(x_A(uh+V) - vx_A)g,g) = \\ &e(u^{-1}(x_Auh),g) = e(x_Ah,g) = e(h,x_Ag) = e(h,y_A) \end{aligned}$$

3　安全性证明

3.1　盲性证明

定理 1　本文方案满足盲性[1]。

证明　对于任意给定的有效签名(m,S)和签名阶段中产生的中间值(λ,V,h,S_1,S_2),总存在唯一的一对盲化因子 $u,v \in \mathbb{Z}_q^*$。

给定签名(m,S)和中间值(λ,V,h,S_1,S_2),u、v 满足:

$$\lambda = uh + V \tag{1}$$

$$S = u^{-1}S_2, S_2 = S_1 - vy_A, S_1 = x_A\lambda \tag{2}$$

$$V = vg \tag{3}$$

由式(3)可知 $v = \log_g V \in \mathbb{Z}_q^*$ 是唯一存在的,再由式(1)可知 $u = \log_h(\lambda - V) \in \mathbb{Z}_q^*$ 也是唯一存在的。

以下证明 u、v 满足式(2)中所有等式。由双线性对的不可退化性可知 $S_2 = S_1 - vy_A \Leftrightarrow e(S_2,y_A) = e(S_1 - vy_A,y_A)$,因此,只需证明 u、v 满足等式 $e(S_2,y_A) = e(S_1 - vy_A,y_A)$。

因为(m,S)是有效签名,所以有:

$$e(S,g) = e(h,y_A) = e(u^{-1}S_2,g) \tag{4}$$

$$e(x_A\mu h,g) = e(S_2,g) \tag{5}$$

$$\begin{aligned} e(S_1 - vy_A,y_A) &= e(x_A\lambda - vx_Ag,y_A) = \\ &e(x_A(\mu h + vg) - vx_Ag,y_A) = \\ &e(x_Auh,y_A) = e(S_2,y_A) \end{aligned} \tag{6}$$

通过攻击者 Alice 和用户 Bob 间的挑战游戏证明消息的不可区分性。游戏过程如下:

S0:运行系统参数建立和密钥生成算法,发送相应参数给攻击者 Alice 和用户 Bob,Alice 掌握签名私钥。

S1:Alice 随机选择等长的消息 m_0 和 m_1 发给 Bob。

S2:Bob 随机选择一个比特值 $c \in \{0,1\}$,运行盲化算法生成盲化消息 $h_c = H(ID_A,y_A,m_c)$ 和 $h_{1-c} = H(ID_A,y_A,m_{1-c})$,随机选择 2 组秘密值 $u_c,v_c \in \mathbb{Z}_q^*$ 和 $u_{1-c},v_{1-c} \in \mathbb{Z}_q^*$,计算 $V_c = v_cg$,$\lambda_c = u_ch_c + V_c$,$V_{1-c} = v_{1-c}g$,$\lambda_{1-c} = u_{1-c}h_{1-c} + V_{1-c}$,将 λ_c 和 λ_{1-c}按照随机顺序先后发送给 Alice 请求签名。

S3:Alice 分别计算 $S_{1,c} = x_A\lambda_c$ 和 $S_{1,1-c} = x_A\lambda_{1-c}$,将 $S_{1,c}$和 $S_{1,1-c}$先后发送给 Bob。

S4:Bob 利用(u_c,v_c)、(u_{1-c},v_{1-c})和脱盲算法

得到 2 组最终的消息签名对(m_c,S_c)和(m_{1-c},S_{1-c}),并先后发送给 Alice。

S5:Alice 输出一个对比特值 c 的猜测值 $c'\in\{0,1\}$。

下面分析 Alice 正确猜对 c 的概率。因为盲化因子(u_c,v_c)、(u_{1-c},v_{1-c})是在$\mathbb{Z}_q^*$上均匀随机选取的,选取的过程完全独立于 m_c 和 m_{1-c},而盲化过程是可逆线性仿射变换且每次盲化因子是独立随机选取的,所以盲化因子(u_c,v_c)、(u_{1-c},v_{1-c})完全独立于最终消息签名对(m_c,S_c)、(m_{1-c},S_{1-c})。从 Alice 的视角观察,其分布也是相同的,并且完全独立于 c。由于 c 是随机均匀选取的,(m_c,S_c)和(m_{1-c},S_{1-c})对于 c 在计算上具有不可区分性,因此 Alice 正确猜对 c 的概率是 1/2,即攻击者 Alice 无法以不可忽略的优势猜对 c。

综上所述,盲化因子 u、v 在签名过程中是随机选取的,由于求解 u、v 都面临椭圆曲线上离散对数问题,因此本文签名方案满足盲性。

3.2 随机预言机模型下的安全性证明

定理 2 本文方案在随机预言机模型和 CDH 困难问题假设下,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 假定存在一个适应性选择消息和身份的攻击算法 $\Re$,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_H、t_H 分别为询问 H 预言机的次数和一次询问所需时间,q_s、t_s 分别为签名询问的次数和一次询问所需时间,则存在概率多项式时间算法 C,在时间 $t'<t+(q_st_s+2q_Ht_H)$内以不可忽略的优势$\varepsilon'\geqslant\left(\varepsilon-\frac{1}{2^k}\right)\left(1-\frac{1}{q_H}\right)^{q_s}\frac{1}{q_H}$解决 CDH 问题。

证明 假定给 C 一个 CDH 困难问题的实例为:给定 $ag\in G_1$ 和 $bg\in G_1$,要输出 CDH 问题的一个解 abg。

C 的目标是通过调用算法 $\Re$ 来解决上述困难问题实例,游戏中假定 $\Re$ 不会对预言机发起 2 次相同的询问。

设定挑战身份 ID 的公钥为 $y=ag$,挑战消息为 m^*,C 在系统初始化后公布系统参数$\{k,G_1,G_2,g,H\}$,将系统参数和 y 发送给 $\Re$。

1)H 询问:C 维护一个由数组(m_i,d_i,h_i)组成的列表,当 $\Re$ 向 C 提交(ID,y,m)的 H 询问时,查询列表 L,如果 L 中存在记录(m,d,h),则返回相应的 h 给 $\Re$,否则:

(1)如果 $m\neq m^*$,则随机选择一个 $d\in\mathbb{Z}_q^*$,计算 $h=dg$,C 在将其作为 $H(ID,y,m)$的值返回给 $\Re$ 的同时,将(m,d,h)保存到列表 L 中。

(2)如果 $m=m^*$,则 C 将 bg 作为 $H(ID,y,m)$的值返回给 $\Re$ 的同时,将$(m,\perp,bg)$保存到列表 L 中,其中“$\perp$”表示空。

2)签名询问:当 $\Re$ 向 C 提交一个关于 m 的签名询问时:

(1)当 $m=m^*$时,C 返回“$\perp$”,记此事件为 E_1。

(2)当 $m\neq m^*$ 时,C 从 L 中恢复数组列表(m,d,h),随机选择 $u,v\in\mathbb{Z}_q^*$,计算 $V=vg,\lambda=uh+V,S_1=udy+vy,S_2=S_1-vy,S=u^{-1}S_2$ 返回给 $\Re$,容易验证 C 返回的签名满足验证等式 $e(S,g)=e(h,y)$。

经过适应性询问后,$\Re$ 终止询问,输出一个消息 $\bar{m}$ 且满足最终验证等式的消息/签名对$(\bar{m},S^*)$。如果 $\bar{m}\neq m^*$,则伪造失败,记此事件为 E_2;否则,$m=m^*$,C 从列表 L 中恢复数组$(m^*,\perp,bg)$,因为签名验证等式 $e(S^*,g)=e(h^*,y)$成立,所以等式 $e(S^*,g)=e(bg,ag)=e(abg,g)$成立。

由此,C 成功地计算出 $S^*=abg$,并输出 S^*作为 CDH 问题的一个实例的解答。以下分析 C 成功解决困难问题的时间和优势:

1)对于 H 的询问的答案是均匀且独立分布在 $\mathbb{Z}_q^*$ 内的,并且答案是有效的。

2)只有当事件 E_1、E_2 不发生时,最终的伪造签名才是有效的。

3)如果事件 E_1、E_2 都不发生,则 C 能解决 CDH 问题的一个实例。在签名询问阶段,若 $m=m^*$,即 E_1 事件发生,因为 H 询问共有 q_H 次,所以问到目标挑战消息 m^* 的概率为 $\Pr(E_1)=\frac{1}{q_H}$,共进行 q_s 次独立的签名询问,而由于每次询问是相互独立不相关的,因此 E_1 事件不发生的概率为 $\Pr(\neg E_1)=\left(1-\frac{1}{q_H}\right)^{q_s}$;在签名伪造阶段,只有当伪造的消息是挑战消息 m^* 的签名时才能解决困难问题的实例,即 E_2事件不发生,因此,E_2 事件不发生的概率为 $\Pr(\neg E_2)=\frac{1}{q_H}$。综上可得事件 E_1、E_2 都不发生的概率为:$\Pr(\neg E_1\wedge\neg E_2)=\left(1-\frac{1}{q_H}\right)^{q_s}\cdot\frac{1}{q_H}$。

当 $\Re$ 没有询问 H 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$\frac{1}{2^k}$(其中 k 为安全参数),因此,C 在该游戏中的一个优势下界为 $\varepsilon'\geqslant(\varepsilon-\frac{1}{2^k})\left(1-\frac{1}{q_H}\right)^{q_s}\frac{1}{q_H}$,运行时间的一个上界为 $t'<t+(q_st_s+2q_Ht_H)$。因此,攻击者在概率多项式时间 t'内以一个不可忽略的概率 ε'成功解决了一个 CDH 问题实例,这与 CDH 问题的难解性矛盾。

因此,由引理 1 即证定理 2,即本文方案在随机预言机模型和 CDH 困难问题假设下,在适应性选择消息攻击下是存在性不可伪造的。

4　效率分析与代码实现

4.1　效率分析

将本文方案与相关典型的签名方案进行效率对比[11],如表 1 所示,其中,M 表示 G_1 中的标量乘,P 表示双线性对运算,E 表示 G_2 中的幂乘运算,I 表示 $\mathbb{Z}_q^*$ 中的求逆运算,H 表示散列运算。

表 1　方案效率比较

方案	签名	验证	签名长度/bit
文献[4]方案	1M	1P + 1M	160
文献[10]方案	3M + 1H + 1P + 1I	1P + 1E	320
文献[12]方案	1P + 6M	2P + 1E	320
文献[13]方案	1M + 1E	3P + 1E + 2H + 1I	320
文献[14]方案	3P + 4E + 4M	2P + 1E	320
文献[15]方案	1P + 1M + 4I	1P + 1I + 1E	160
本文方案	1M	1H + 2P	160

由表 1 可以看出:在签名和验证签名的总效率方面,本文方案与 BLS 短签名方案[4]基本相同,与其他方案相比效率较高;在签名长度方面,选择阶为 160 bit 的椭圆曲线上的群和双线性对映射[16],本文方案的签名长度为 160 bit,与 BLS 短签名方案[4]基本相同,与文献[4,15]方案的签名长度相同,而与文献[10,12-14]签名方案相比长度较短。

4.2　关键代码实现

本文以斯坦福大学研究人员开发的一个开源 C 语言库(Pairing-based Cryptography library,PBC)为基础,在操作系统为 64 位 Windows 7,CPU 为 Intel i7-7700 3.6 GHz,主板为华硕 H270,内存为金士顿 DDR4 2 400 MHz 的实验基准测试环境中实现本文方案。

本文方案首先对消息进行哈希处理,再随机选择 2 个秘密值 $u,v \in \mathbb{Z}_q^*$,计算 $V = vg$ 和 $\lambda = uh + V$,以此进行盲化处理。盲化处理的部分代码如下:

```
//盲化处理
sign_start = clock();
element_t h,u,v,V,r,uh;
charm[50] = "SignMessagexpp20180218163438";
element_init_G1(h,pairing);
strcat(m,IDUi);
element_from_hash(h,m,strlen(m));
element_init_Zr(u,pairing);
element_init_Zr(v,pairing);
element_init_G1(V,pairing);
element_init_G1(r,pairing);
element_init_G1(uh,pairing);
printf("签名消息:\n% s\n\n",m);
element_random(u);//选择随机数 u
element_random(v);//选择随机数 v
element_mul(U,u,g);//计算 U = u * g;
element_mul(uh,u,h);//计算 uh = u * h;
element_add(r,uh,V);//计算 r = u * h + V;
```

对盲化后的消息进行签名,生成消息 m 的签名 S 的代码。图 2 为对消息“SignMessagexpp20180218163438”签名后的结果。

```
签名消息:
SignMessagexpp20180218163438

签名结果:
[220677019935783425559733035370935053824631525963547738538
3674184814016363871441801946198696143525524145020339575856
1227972518700417233549436300996319539631905252854691485560
7154321598937864574599866051107599460186298760117800054268
4203546642493280980450373724866388758543083647418869995796
4403975591561801, 625223053036416397567454216787935319419734
574549994767709692518685038063415781075311166979221235859289
2469357122925457618718802452530604526502664274457265089239
3648125038747222803574696971229997166906013764955113336615
9354475851564508596744236103325179631828859030112688094574
3916611473173254507679030992509]
```

图 2　对消息进行盲签名后的结果

对盲化后的签名进行脱盲处理,具体代码如下所示,其中 S 为消息 m 的签名。

```
//脱盲处理
element_init_G1(S2,pairing);
element_init_G1(temp,pairing);
element_mul(temp1,v,yA);//temp1 = v^yA
element_sub(S2,S1,temp1);//计算 S2 = S1 - v * yA;
element_init_Zr(w,pairing);
element_init_Zr(inv_u,pairing);
element_invert(inv_u,u);//求 u 的逆
//输出最终签名 S
element_init_G1(S,pairing);
element_mul(S,inv_u,S2);//计算 S = U^ - 1 * S2;
sign_end = clock();//结束计时
element_printf("S = % B\n",S);
```

第三方验证消息签名对(m,S)的代码如下所示,验证结果如图 3 所示。

```
//验证签名
element_t left,right;
verify_start = clock();
element_init_GT(left,pairing);//等式左边
element_init_GT(right,pairing);//等式右边
element_pairing(left,S,g);
element_pairing(right,h,yA);
verify_end = clock();//运行耗时
double verifyTime = difftime(verify_end,verify_start);
element_printf("e(S,g) = \n% B\n",left);
element_printf("e(h,yA) = \n% B\n\n",right);
//左右比较
```

```
    if (! element_cmp(left,right))
    printf("验证成功! \n\n\n");//左右相同
    printf("待签名消息 m:% s \n",m);
    printf("消息长度:% d \n",strlen(m));
    printf("签名生成耗时:% f ms\n",signTime);
```

```
e(S,g)=
582403611770656699842619673393418089185723611479913416624564
138383693606593721630146729228191827259746871094576377112569
259137126384438321017286092568196441849885572296071834618094
e(h,yA)=
582403611770656699842619673393418089185723611479913416624564
138383693606593721630146729228191827259746871094576377112569
259137126384438321017286092568196441849885572296071834618094

验证成功!
```

图 3 验证签名后的结果

5 结束语

本文提出一种短盲签名方案,并在随机预言机模型和 CDH 问题假设下,证明该方案在适应性选择消息上是存在性不可伪造的。与典型盲签名方案相比,本文方案签名长度短,签名和盲化过程计算简单,适合在带宽受限且使用超低功耗设备的环境下进行数据签名、验证以及交互传输。下一步将在文献[17-18]研究基础上,把短签名方案应用于基于便携式设备的电子票据安全交互协议中,实现对电子票据的匿名保护。

参考文献

[1] CHAUM D. Blind signatures for untraceable payments[C]// Proceedings of Cryptology' 83. Berlin, Germany: Springer, 1983:199-203.

[2] SONG Chengyuan, ZHANG Chuanrong, CAO Shuai. Blind signature scheme and its application in electronic voting protocol [J]. Computer Engineering, 2012, 38(6):139-141,144. (in Chinese)
宋程远,张串绒,曹帅. 一种盲签名方案及其在电子投票协议中的应用[J]. 计算机工程,2012,38(6):139-141,144.

[3] KUMAR M, KATTI C P, SAXENA P C. An untraceable identity-based blind signature scheme without pairing for e-cash payment system [C]//Proceedings of International Conference on Ubiquitous Communications and Network Computing. Berlin, Germany: Springer, 2017:67-78.

[4] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2001: 514-532.

[5] WEI Chunyan, CAI Xiaoqiu. Efficient certificateless short signature scheme under standard model [J]. Computer Engineering, 2012, 38(13):119-121. (in Chinese)
魏春艳,蔡晓秋. 标准模型下的高效无证书短签名方案[J]. 计算机工程,2012,38(13):119-121.

[6] BAO Sigang, GU Haihua. Fault attack on BLS short signature[J]. Computer Engineering, 2014, 40(8):112-115. (in Chinese)
包斯刚,顾海华. 针对 BLS 短签名的故障攻击[J]. 计算机工程,2014,40(8):112-115.

[7] TSAI J L. A new efficient certificateless short signature scheme using bilinear pairings [J]. IEEE Systems Journal, 2015, 11(4):2395-2402.

[8] KARATI A, BISWAS G P. Cryptanalysis and improvement of a certificateless short signature scheme using bilinear pairing[C]//Proceedings of International Conference on Advances in Information Communication Technology and Computing. New York, USA: ACM Press, 2016.

[9] LIN Chen, SHEN Zhidong, CHEN Qian, et al. A data integrity verification scheme in mobile cloud computing[J]. Journal of Network and Computer Applications, 2017, 77:146-151.

[10] VERMA G K, SINGH B B. Efficient identity-based blind message recovery signature scheme from pairings[J]. IET Information Security, 2017, 12(2):150-156.

[11] Certicome Corporation. SEC 2: recommended elliptic curve domain parameters [EB/OL]. [2018-10-12]. https://perso.univ-rennes1.fr/sylvain.duquesne/master/standards/sec2_final.pdf.

[12] ZHANG Fangguo, KIM K. ID-based blind signature and ring signature from pairings [C]//Proceedings of International Conference on Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2002:533-547.

[13] ZHANG Lei, ZHANG Futai. Certificateless signature and blind signature [J]. Journal of Electronics (China), 2008, 25(5):629-635.

[14] XU Guosheng, XU Guoai. An ID-based blind signature from bilinear pairing with unlinkability [C]// Proceedings of the 3rd International Conference on Consumer Electronics, Communications and Networks. Washington D. C., USA: IEEE Press, 2013:101-104.

[15] VERMA G K, SINGH B B. Efficient message recovery proxy blind signature scheme from pairings [J]. Transactions on Emerging Telecommunications Technologies, 2017, 28(9).

[16] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [C]//Proceedings of Cryptology' 01. Berlin, Germany: Springer, 2001:213-229.

[17] ZUO Liming, CHEN Zuosong, XIA Pingping, et al. Efficient and provably secure short proxy signature scheme [J]. Journal of Computer Applications, 2018, 38(12):2529-2533. (in Chinese)
左黎明,陈祚松,夏萍萍,等. 一个高效的可证安全短代理签名方案[J]. 计算机应用,2018,38(12):2529-2533.

[18] ZUO Liming, HU Kaiyu, ZHANG Mengli, et al. A short identity-based signature scheme with bilateral security[J]. Netinfo Security, 2018(7):47-54. (in Chinese)
左黎明,胡凯雨,张梦丽,等. 一种具有双向安全性的基于身份的短签名方案[J]. 信息网络安全,2018(7):47-54.

编辑 金胡考