

基于 SM9 算法的部分盲签名方案

吕尧¹, 侯金鹏², 聂冲², 苏锐², 王彬³, 蒋鸿玲³

(1. 中国电子信息产业发展研究院, 北京 100048;

2. 南京理工大学计算机科学与工程学院, 江苏 南京 210094;

3. 北京信息科技大学信息管理学院, 北京 100192)

摘要: 普通的数字签名在有效保护用户隐私方面存在诸多不足, 如对签名的抵赖和跟踪时有发生。针对上述问题, 提出一种基于 SM9 算法的部分盲签名方案, 部分是指签名消息包含用户的消息和其他有关信息, 能够有效抵抗签名抵赖和跟踪, 同时引入可信第三方来防止恶意用户对信息的篡改。通过实验结果和理论分析, 证明了所提算法的安全性和高效性。

关键词: SM9 算法; 盲签名; 部分盲签名; 数字签名

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021037

Partial blind signature scheme based on SM9 algorithm

LYU Yao¹, HOU Jinpeng², NIE Chong², SU Mang², WANG Bin³, JIANG Hongling³

1. China Center for Information Industry Development, Beijing 100048, China

2. School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China

3. School of Information Management, Beijing Information Science & Technology University, Beijing 100192, China

Abstract: Ordinary digital signatures have many deficiencies in effectively protecting users' privacy, and signature repudiation and tracking occur from time to time. In order to solve the above problems, a partial blind signature scheme based on the SM9 algorithm was proposed. Partially means that the signature message contains the user's message and other related information, so it can effectively resist signature repudiation and tracking, and introduce a trusted third party to prevent malicious users from tampering with information. Through experimental results and theoretical analysis, the security and efficiency of the proposed algorithm are proved.

Keywords: SM9 algorithm, blind signature, partial blind signature, digital signature

1 引言

在信息化时代, 消息得以快速传播, 特别是

随着 5G 时代的到来, 物联网应用的发展越来越迅速。这便利了人们的生活, 但也带来了许多潜在的安全威胁: 数据在开放的网络环境下传输,

收稿日期: 2020-09-29; 修回日期: 2020-12-31

通信作者: 苏锐, sumang@njut.edu.cn

基金项目: 国家自然科学基金 (61702266)

Foundation Item: The National Natural Science Foundation of China (61702266)

论文引用格式: 吕尧, 侯金鹏, 聂冲, 等. 基于 SM9 算法的部分盲签名方案[J]. 网络与信息安全学报, 2021, 7(4): 147-153.
LYU Y, HOU J P, NIE C, et al. Partial blind signature algorithm based on SM9[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 147-153.

难免会遭到不法分子的恶意攻击,使隐私数据非法泄露或被篡改。物联网、5G 通信应用快速发展的同时,用户隐私数据被攻击、截获甚至破解的安全风险逐渐增加。这些安全风险不仅可能造成个人或企业的经济损失,甚至可能威胁到国家的安全。SM9 算法和部分盲签名在此背景下显示出极大的发展潜力。

Koblitz^[1]、Miller^[2]分别于 1984 年、1986 年提出了基于椭圆曲线的公钥密码算法,在安全性相同的条件下,可以使用比其他公钥密码算法更短的密钥。1984 年,Shamir^[3]提出标识密码(IBE)的概念,简化了密钥管理环节。2000 年,Sakai^[4]提出基于椭圆曲线和双线性对的密码系统。2001 年,Boneh 和 Franklin^[5]提出使用 Weil 对构造标识公钥加密算法。2016 年,国家密码管理局发布了 SM9 密码算法标准^[6]。SM9 算法简化了密钥管理环节,可以大大减少申请和验证过程,特别适合海量用户的安全交互通信。

Chum^[7]于 1983 年首次提出盲签名概念,通过对签名消息的盲化来达到隐私保护的效果。盲签名比普通的数字签名更能保护用户的隐私。但签名消息对签名者的完全匿名性也带来了安全隐患,签名会被非法分子滥用。为了使签名者在不知道所签消息的同时能在必要时对该签名可控,Brands^[8]提出一种受限盲签名方案,但该方案在验证时需要与消息提供者交互。为了克服该问题,1996 年,Abe 等^[9]提出一个部分盲签名的简单模型,部分盲签名通过在签名中嵌入用户与签名者协商的公共信息,避免了完全匿名留下的安全隐患。但部分盲签名的方案易存在公共信息被替代的漏洞^[10]。如 2013 年,汤志鹏等^[11]发现余丹等^[12]的方案存在公共信息可以被非法篡改的漏洞;何俊杰等^[13]分析了文献[11]的方案,也存在恶意用户可以非法篡改公共信息的缺陷;杨俊芳^[14]分析文献^[13]方案发现,同样存在公共信息被篡改的可能。

现有的基于 SM9 算法的盲签名仅有两个方案:一是张雪峰和彭华提出的一种基于 SM9 算法的盲签名方案研究^[15],二是何德彪等提出的一种基于 SM9 数字签名的盲签名生成方法与系统^[16]。

文献[15]提出的基于 SM9 算法的盲签名方案分为消息盲化、签名生成和签名验证 3 个步骤。通过对消息 M 进行盲化,将盲化后的消息传给签名者进行签名,实现了消息的隐私保护。该方案存在的问题:签名时使用杂凑函数对盲化后的消息 M' 进行单向压缩运算,因此实际得到的是盲化消息 M' 的签名而非待签消息 M 的签名。

文献[16]提出一种基于 SM9 数字签名的盲签名方案,可以在签名者不知道真实消息的情况下生成正确的 SM9 盲签名。签名的过程由签名者和用户共同执行,生成 SM9 盲签名的过程不会向签名者泄露被签名的消息,既能保证签名的正确性,又能保证签名消息的隐私性,是一种实用的盲签名算法。

本文在文献[16]的基础上设计一种基于 SM9 数字签名算法的部分盲签名方案,在签名中植入关于时间的公共信息,在保证用户消息隐私的情况下,使签名具有可控性,同时,算法中的公共信息无法被非法篡改。本文算法可以应用的范围比盲签名更广,如电子现金、电子拍卖、电子投票等领域。

2 基础知识

本节介绍盲签名和部分盲签名的概念,同时介绍一些相关的数学理论。

2.1 盲签名与部分盲签名

盲签名即签名者不知道所签消息的内容,签名后不能对自己的签名抵赖和进行跟踪的一种特殊的数字签名。相比普通的数字签名,盲签名能够更好地保护用户的隐私。基于这一优点,盲签名被广泛应用于电子投票等需要保护自身隐私的场合。

但是,盲签名的完全盲化带来了不可控性,这使它更容易被非法分子滥用。为了解决这个额外风险,产生了部分盲签名。在部分盲签名方案中,签名者在签名时可以加入与用户协商的消息或者自己的信息。消息提供者不能篡改签名者加入的信息,从而阻止签名申请者提供非法信息或篡改信息而滥用签名,这样既有效地保护了用户的隐私又让签名者对所签署的内容部分可控。

2.2 有限域上的椭圆曲线

定义在有限域 F_{p^m} (p 为大素数, $m \geq 1$) 上的椭圆曲线是由点组成的集合,方程如(1)所示。

$$y^2 = x^3 + ax + b, a, b \in F_{p^m}, 4a^3 + 27b^2 \neq 0 \quad (1)$$

椭圆曲线 $E(F_{p^m})$ 定义为

$$E(F_{p^m}) = \{(x, y) | x, y \in F_{p^m}, \text{且满足式(1)}\} \cup \{O\}$$

其中, O 为无穷远点。

设 E 和 E' 是定义在 F_q 上的椭圆曲线, 如果存在一个同构映射 $\psi_d: E'(F_{q^d}) \rightarrow E(F_{q^d})$, 其中 d 是使映射存在的最小整数, 则称 E' 为 E 的 d 次扭曲曲线。

2.3 双线性对

映射 $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ 为双线性对, 如果 e 满足下列性质。

(1) 非退化性: $e(P, Q) \neq 1$ 。

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

(3) 易计算性: 存在有效算法计算 $e(P, Q)$ 。

其中, $\mathbb{G}_1$ 是由 P 生成的阶为 q 的循环加法群, $\mathbb{G}_2$ 是由 Q 生成的阶为 q 的循环加法群, $\mathbb{G}_T$ 是有相同阶 q 的循环乘法群。

双线性映射 e 可通过有限域上的超奇异椭圆曲线上的 Weil 对或 Tate 对来构造^[17-21]。

3 本文方案

本文提出的基于 SM9 数字签名算法的部分盲签名方案, 在保证消息盲化的同时可以确定最后生成的签名是对于消息 M 的部分盲签名。对于其他学者提出的部分盲签名方案中出现的公共信息被篡改漏洞, 本文设计的部分盲签名方案通过引入可信任第三方对公共信息是否被篡改进行验证, 能在一定程度上防止公共信息被篡改。

3.1 系统参数组

SM9 算法的主要参数及参数说明如表 1 所示。

3.2 主密钥对与用户私钥的产生

由密钥生成中心 KGC 产生主密钥对 (s, P_{pub}) 及用户的签名私钥 dsa , 具体步骤与 SM9 算法主密钥对和用户私钥的产生一致。

3.3 部分盲签名生成算法

(1) 签名准备

签名前, 向可信任第三方申请一个关于签名有效期的公共信息 $(\text{timeh}, \text{endt})$, 详细描述如下。

表 1 系统参数
Table 1 System parameter

参数	参数说明
cid	曲线识别符
F_q	包含 q 个元素的有限域
a, b	椭圆曲线方程参数
β	扭曲曲线参数
N	椭圆曲线的素因子
cf	椭圆曲线阶相对于 N 的余因子
k	曲线 $E(F_q)$ 相对于 N 的嵌入次数
d_1, d_2	k 的两个因子
G_1	$E(F_q^{d_1})$ 的 N 阶循环子群, 是加法循环群
G_2	$E(F_q^{d_2})$ 的 N 阶循环子群, 是加法循环群
G_T	N 阶乘法循环群, 是双线性对 e 的值域
P_1	G_1 的生成元
P_2	G_2 的生成元
eid	双线性对 e 的识别符
Ψ	G_2 到 G_1 的同态映射

签名开始前向可信第三方发出申请, 第三方收到申请后:

a. 获取当前时间戳, 并将其与预先设置有效期相加获得有效期时间戳 endt ;

b. 产生随机数 $p \in [1, N-1]$, p 由第三方秘密保存;

c. 计算有效时间戳的认证整数 $\text{timeh} = H_2(\text{endt} \parallel p, N)$;

d. 将 endt 与 timeh 的数据类型转换为字节串, 签名中的公共消息为 $(\text{timeh}, \text{endt})$ 。

(2) 公共参数计算

签名者 Signer 在群 G_T 上计算 $g = e(P_1, P_{\text{pub}})$; 产生随机数 $r \in [1, N-1]$, 在群 G_T 上计算 $w = g^r$, 并将 w 发送给 User。

(3) 盲化

a. 收到 w 后, 产生随机数 $\alpha, \beta \in [1, N-1]$, 在群 G_T 上计算 $w_2 = w^\alpha g^\beta$, 转换 w_2 的数据类型为比特串。

b. 计算 $h = H_2(M \parallel w_2, N)$, h 数据类型为整数。

c. 计算 $h' = \alpha^{-1}(h \cdot \text{timeh} - \beta + \text{endt}) \bmod N$, 并将整数 h' 发送给签名者 Signer。

(4) 签名

签名者 Signer 收到 h' 后, 在群 G_1 上计算 $S_1 = [r - h']\text{dsa}$, 并将 S_1 发送给 User。

(5) 解盲

用户 User 收到 S_1 后计算 G_1 中的元素 $S = [\alpha]S_1$, 消息 M 的部分盲签名为 $(h, S, \text{timeh}, \text{endt})$ 。

3.4 部分盲签名验证算法

部分盲签名的验证算法根据被验证对象的不同分为两部分: 一是时间戳的验证, 包括第三方对公共信息是否被篡改的验证和验证方对签名是否在有效期内的验证; 二是部分盲签名正确性的验证。

(1) 时间戳的验证

a. 验证者收到部分盲签名后, 向可信第三方发送公共信息 $(\text{timeh}, \text{endt})$ 。可信第三方收到公共信息后, 根据秘密保存的 p 计算 $\text{timeh}' = H_2(\text{endt} \parallel p, N)$, 判断 timeh 与 timeh' 是否相等, 将判断结果告知验证者。

b. 验证者从第三方获得公共信息是否被篡改的结果, 如果被告知公共信息被篡改, 则签名验证不通过, 否则进行部分盲签名的正确性验证。若签名验证正确, 进行签名有效期验证: 验证者获取当前时间戳, 与 endt 进行时间戳大小比较, 若当前时间戳大于 endt , 则验证不通过, 否则验证通过。

2. 盲签名正确性的验证

为了检验收到的消息 M 的正确性与完整性, 需要验证部分盲签名 $(h, S, \text{timeh}, \text{endt})$ 的正确性, 作为验证者的用户应实现以下运算步骤:

a. 转换 h 的数据类型为整数, 检验 h 是否在 $[1, N-1]$ 内, 若不在规定范围内, 则验证不通过;

b. 转换 S 的数据类型为椭圆曲线上的点, 检验 S 是否为群 G_1 中元素, 若不是, 则验证不通过;

c. 在群 G_T 上计算 $g = e(P_1, P_{\text{pub}})$;

d. 转换 timeh 与 endt 的数据类型为整数, 在群 G_T 上计算 $t = g^{h \cdot \text{timeh} + \text{endt}}$;

e. 计算 $h_1 = H_1(\text{ID}_A \parallel \text{hid}, N)$;

f. 在群 G_2 上计算 $P = [h_1]P_2 + P_{\text{pub}}$;

g. 在群 G_T 上计算 $u = e(S, P)$;

h. 在群 G_T 上计算 $w' = ut$, 转换 w' 的数据类型为比特串;

i. 计算 $h_2 = H_2(M' \parallel w', N)$, 判断整数 h_2 与 h 是否相等, 若相等, 则验证正确, 进行签名有效期验证; 否则不通过。

3.5 方案的正确性证明

本文提出的基于 SM9 算法的部分盲签方案是可验证正确的。证明如下。

盲签名过程中

$$w_2 = w^\alpha w^\beta = g^{\alpha r + \beta} = e(P_1, P_{\text{pub}})^{\alpha r + \beta} = e(P_1, P_2)^{s(\alpha r + \beta)}$$

验证过程中, 若数字签名 (h, S) 与用户标识 ID_A 均正确, 则

$$\begin{aligned} w' &= u \cdot t = e(S, P) \cdot g^{h \cdot \text{timeh} + \text{endt}} = \\ &= e([\alpha]S_1, [h_1]P_2 + P_{\text{pub}}) \cdot (P_1, P_{\text{pub}})^{h \cdot \text{timeh} + \text{endt}} = \\ &= e([\alpha][r - h']\text{dsa}, [h_1]P_2 + [s]P_2) \cdot e(P_1, P_2)^{S(h \cdot \text{timeh} + \text{endt})} = \\ &= e([\alpha][r - \alpha^{-1}(h \cdot \text{timeh} - \beta + \text{endt})]\text{dsa}, [h_1 + s]P_2) \cdot \\ &= e(P_1, P_2)^{s(h \cdot \text{timeh} + \text{endt})} \end{aligned}$$

$$\text{因为 } \text{dsa} = [t_2]P = \left[\frac{s}{H_1(\text{ID}_A \parallel \text{hid}, N) + s} \right] P_1 = \left[\frac{s}{h_1 + s} \right] P_1$$

$$\begin{aligned} w' &= e([\alpha][r - \alpha^{-1}(h \cdot \text{timeh} - \beta + \text{endt})] \cdot \\ &\quad \left[\frac{s}{h_1 + s} \right] P_1, [h_1 + s]P_2) e(P_1, P_2)^{s(h \cdot \text{timeh} + \text{endt})} = \\ &= e(P_1, P_2)^{\alpha \cdot \left[r - \frac{h \cdot \text{timeh} - \beta + \text{endt}}{\alpha} \right] \left[\frac{s}{h_1 + s} \right] (h_1 + s)} \cdot \\ &= e(P_1, P_2)^{s(h \cdot \text{timeh} + \text{endt})} = e(P_1, P_2)^{s(\alpha r + \beta)} \end{aligned}$$

所以 $w' = w_2$, 若收到的消息 M 未被篡改, 则 $h_2 = h$, 验证通过。

4 实验分析

本节从安全性、正确性和效率 3 方面分析所提部分盲签名算法。

4.1 安全性分析

部分盲签名算法的安全性包括不可伪造性和盲性, 不可伪造性是指签名结果不能被任意攻击

方伪造,盲性是指签名的消息不被除消息拥有者外的任何人知道。本节分别给出二者的定义和证明。

定义 1 不可伪造性。假设任意消息 M 的部分盲签名结果为 $\text{Pbs}(h, S, \text{timeh}, \text{endt})$ 。攻击方 $\mathcal{A}$ 可以在多项式时间内伪造关于消息 M 的部分盲签名结果 $\text{Pbs}'(h', S', \text{timeh}', \text{endt}')$ 。若 Pbs 与 Pbs' 相同的概率 $\Pr(\text{Pbs}=\text{Pbs}')$ 是一个可忽略量,则可认为部分盲签名方案所设计的算法具有不可伪造性。

证明 由 3.5 节正确性证明可以看出,盲签名结果若可以被伪造,则需要 Pbs 和 Pbs' 中对应参数全部相等。其中, endt 是可信第三方设置的固定值,攻击方 $\mathcal{A}$ 可以通过多次查询获取,但是只要保证 4 个参数至少有一个不可伪造,那么整个部分盲签名就是不可伪造的。下面逐个证明 timeh , h , S 这 3 个参数的不可伪造性。

timeh 的不可伪造性: 假设当前时间戳为 time 。 timeh 是由可信第三方使用单向哈希函数生成的,哈希函数的输入是一个随机数 $p \in [1, N-1]$ 与 $\text{time}+\text{endt}$ 的位连接。这保证了即使攻击方 $\mathcal{A}$ 与被攻击方同时生成签名,也可以获得不同的公共消息。只要 N 足够大, p 就不可能在多项式时间内被推测出来,由此, $\Pr(\text{timeh}=\text{timeh}')$ 是一个可忽略量。

h 的不可伪造性: 因为 $h = H_2(M \parallel w^\alpha g^\beta, N)$, 其中随机数 $\alpha, \beta \in [1, N-1]$, 所以 h 的不可伪造性依赖于 α, β , 与上一个证明类似,只要 N 足够大, $\Pr(h=h')$ 就是一个可忽略量。

S 的不可伪造性: $S = [\alpha][r - (\alpha^{-1}(h \cdot \text{timeh} - \beta + \text{endt}) \bmod N)]\text{dsa}$, 由此可以看出, S 的不可伪造性依赖于 timeh 和 h 的不可伪造性, 这二者的不可伪造性已经在上面证毕, 因此 S 具有不可伪造性。

定义 2 盲性。对于任意消息 M , 攻击方 $\mathcal{A}$ 可以在多项式时间内根据签名结果推测消息为 M' , 若 M 与 M' 相同的概率 $\Pr(M=M')$ 是一个可忽略量,则可认为部分盲签名方案具有盲性。

证明 给予攻击方 $\mathcal{A}$ 最强的攻击能力,即 $\mathcal{A}$ 可以冒充可信第三方和签名方。因此, $\mathcal{A}$ 可以获得 time 、 endt 和 h' 。其中 $h' = \alpha^{-1}(h \cdot \text{timeh} - \beta + \text{endt}) \bmod N$, $h = H_2(M \parallel w_2, N)$ 。

$\mathcal{A}$ 首先需要推测出随机数 $\alpha, \beta \in [1, N-1]$,

然后通过碰撞攻击等方法攻破单向哈希函数 $H_2(M \parallel w_2, N)$, 才能获得 M 。当 N 足够大时, $\mathcal{A}$ 推测出 α 和 β 的概率是可以忽略的,更进一步,即使推测出 α 和 β , 只要使用安全性高的单向哈希函数, $\mathcal{A}$ 也无法获取真实消息 M 。因此部分盲签名方案具有盲性。

4.2 正确性测试

本文实现的算法中 SM9 的参数使用《GMT 0044-2016 SM9 标识密码算法》。

本节测试算法的主密钥对和用户私钥的生成功能、签名验签功能,其中盲签名的验证测试分为正确性测试和时间戳验证测试。以下测试是在程序中定义了一个宏 `#define SELF_CHECK 1` 的情况下进行的,即在本次测试中除结束时间戳,其他随机数均采用预设的值。

主私钥为文献[10]中数字签名算法示例所规定的值,为 0130e7 8459d785 45cb54c5 87e02cf4 80ce0b66 340f319f 348a1d5b 1f2dc5f4。

输入主公钥与用户私钥,测试消息 M 为 Chinese IBS standard。测试结果如图 1 所示。

图 1 盲签名结果
Figure 1 Blind signature result

对算法验证环节中的各种异常情况进行测试的结果如表 2 所示,可以看出,本文的算法可以将恶意篡改错误信息的敌手与正常用户区分出来。

4.3 效率测试

在 Intel(R) Core(TM) i5-10210U CPU @ 1.60 GHz

表 2 正确性测试
Table 2 Correcteness test

验证内容	操作类型	预计结果	实际结果
对 h 的验证	篡改后的 h 不在 $[1, N-1]$ 范围内	验证失败	与预计结果一致
	篡改后的 h 在 $[1, N-1]$ 范围内, 但并非真正的签名值		
对 S 的验证	篡改后的 S 不是 G_1 的元素	验证失败	与预计结果一致
	篡改后的 S 是 G_1 的元素, 但与真正的签名值不符		
对数据 M 的验证	修改 M , 将 Chinese IBS Standard 改为 Chinese IBS		
对签名者用户标识 ID 验证	修改用户 ID		

2.11 GHz 的处理器上运行本文算法(下文简称 PBS)和参考文献[12]算法, 测试结果如表 3 所示。

表 3 效率测试
Table 3 Efficiency test

消息	算法	签名时间/ms	验证时间/ms
Heputsomem orecoalsonth efiresotha	PBS	61	807
	文献[12]	59	742
Tthereshould beacheerfulbl azewhen	PBS	62	824
	文献[12]	56	792
Ecameintotea sheputitoverh islegsa	PBS	61	789
	文献[12]	58	630
Ndtuckeditro undhisfeetclo sedthem	PBS	64	719
	文献[12]	55	585

从表 3 可以看出, 本文算法在不计算与可信第三方通信时间的情况下, 与文献[12]算法在运行时间上处于相同数量级。

5 结束语

本文提出了一种基于 SM9 数字签名算法的部分盲签名方案。在保证用户消息隐私的情况下, 必要时可以通过公共信息追踪用户身份, 与何德彪等提出的盲签名方案^[12]相比, 避免了完全盲性。本文主要论述了方案中的盲签名生成与验证算法以及相关密钥生成算法, 并从盲签名、时间戳两个方面进行了正确性验证和分析, 通过编程测试验证了该方案的主密钥对、用户私钥、部分盲签名生成算法以及验签算法。本文方案可以为电子现金、电子投

票、电子拍卖等系统中的盲签名^[22-23]额外提供时效性与可控性, 是一个很有应用前景的方案。

参考文献:

[1] KOBLITZ N I. Introduction to elliptic curves and modular forms[M]. Springer Science & Business Media, 2012.

[2] MILLER V S. Use of elliptic curves in cryptography[C]// Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 198: 417-426.

[3] SHAMIR A. Identity-based cryptography and signature schemes[C]// Proceedings of CRYPTO'84. 1984.

[4] SAKAI R. Cryptosystems based on pairing[C]//SCIS2000. 2000.

[5] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Annual International Cryptology Conference. 2001: 213-229.

[6] 袁峰, 程朝辉. SM9 标识密码算法综述[J]. 信息安全研究, 2016, 2(11): 1008-1027.

YUAN F, CHENG C H. A survey of SM9 identity cryptography algorithms[J]. Research on Information Security, 2016, 2(11): 1008-1027.

[7] CHAUM D. Blind signatures for untraceable payments[J]. Advances in Cryptology, 1983: 199-203.

[8] BRANDS S. Restrictive binding of secret-key certificates[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 1995: 231-247.

[9] ABE M, FUJISAKI E. How to date blind signatures[C]//International Conference on the Theory and Application of Cryptology and Information Security. 1996:244-251.

[10] GMT 0044-2016 SM9 标识密码算法: 第 5 部分 参数定义[R]. GMT 0044-2016 SM9 identity cipher algorithm: part 5 Parameter Definitions[R].

[11] 汤志鹏, 李晓雄, 左黎明, 等. 高效安全无证书部分盲签名[J]. 计算机工程与设计, 2013, 34(02): 339-446.

TANG Z P, LI X X, ZUO L M, et al. Efficient, secure, certificateless partial blind signature[J]. Computer Engineering and Design, 2013, 34(02): 339-446.

[12] 余丹, 杨晓元, 黄大威. 新的无证书部分盲签名方案[J]. 计算机应用研究, 2010, 27(11): 4319-4321.

- YU D, YANG X Y, HUANG D W. A new certificateless partial blind signature scheme[J]. Computer Application Research, 2010, 27(11): 4319-4321.
- [13] 何俊杰, 张帆, 绍辉. 对一个无证书部分盲签名方案的分析与改进[J]. 信阳师范学院学报: 自然科学版, 2014, 27(2): 170-175.
HE J J, ZHANG F, SHAO H. Analysis and improvement of a certificateless partial blind signature scheme[J]. Journal of Xinyang Normal University: Natural Science Edition, 2014, 27(2): 170-175.
- [14] 杨俊芳. 部分盲签名研究及其应用[D]. 南昌: 华东交通大学, 2016.
YANG J F. Research and Application of partial Blind signature[D]. Nanchang: East China Jiaotong University, 2016.
- [15] 张雪峰, 彭华. 一种基于 SM9 算法的盲签名方案研究[J]. 信息网络安全, 2019, 19(8): 61-67.
ZHANG X F, PENG H. Research on a Blind signature scheme based on SM9 algorithm[J]. Information Network Security, 2019, 19(8): 61-67.
- [16] 何德彪, 张语荻, 张宇波, 等. 一种基于 SM9 数字签名的盲签名生成方法及系统: 中国, CN201810333911.4[P]. 2018-04-13.
HE D B, ZHANG Y D, ZHANG Y B, et al. A blind signature generation method and system based on SM9 digital signature: China, CN201810333911.4[P]. 2018-04-13.
- [17] 苏志图. 双线性对的快速计算研究[D]. 西安: 西安电子科技大学, 2012.
SU Z T. Study on the fast calculation of bilinear pairs[D]. Xi'an: Xi'an University of Electronic Science and Technology, 2012.
- [18] 赵昌安. 双线性对的有效计算[D]. 广州: 中山大学, 2008.
ZHAO C A. Efficient calculation of bilinear pairs[D]. Guangzhou: Sun Yat-sen University, 2008.
- [19] 赵昌安, 张方国. 双线性对有效计算研究进展[J]. 软件学报, 2009, 20(11): 3001-3009.
ZHAO C A, ZHANG F G. Research progress of bilinear pair effective computation[J]. Journal of Software, 2009, 20(11): 3001-3009.
- [20] 李彬, 王新梅. 高效的 R-ate 对的参数构造方法[J]. 通信学报, 2010, 31(1): 118-121.
LI B, WANG X M. An efficient parameter construction method for R-ate pairs [J]. Journal on Communication, 2010, 31(1): 118-121.
- [21] 甘植旺, 廖方圆. 国密 SM9 中 R-ate 双线性对快速计算[J]. 计算机工程, 2019, 45(6): 171-174.
GAN Z W, LIAO F Y. Fast calculation of R-ate bilinear pairs in national secret SM9[J]. Computer Engineering. 2019, 45(6): 171-174.
- [22] 张骁, 周清雷, 李斌. 基于 HRCA 的可重构 SM4 密码算法研究与实现[J]. 网络与信息安全学报, 2020, 6(5): 101-109.
ZHANG X, ZHOU Q L, LI B. Research and implementation of Reconfigurable SM4 cryptographic algorithm based on HRCA[J]. Journal of Network and Information Security, 2020, 6(5): 101-109.
- [23] 吴邱涵, 胡卫. 基于 SM2 算法和区块链的移动端身份认证协议设计[J]. 网络与信息安全学报, 2018, 4(9): 60-65.
WU Q H, HU W. Design of mobile authentication protocol based on SM2 algorithm and block chain[J]. Journal of Network and Information Security, 2018, 4(9): 60-65.

[作者简介]



吕尧 (1984-), 男, 陕西宝鸡人, 中国电子信息产业发展研究院助理研究员, 主要研究方向为信息安全、电子认证、密码、数据安全和个人信息保护。



侯金鹏 (1997-), 男, 黑龙江宝清人, 南京理工大学硕士生, 主要研究方向为密码学、联邦学习隐私保护、安全计算。



聂冲 (1998-), 男, 河南信阳人, 南京理工大学硕士生, 主要研究方向为网络空间安全。



苏铨 (1987-), 女, 内蒙古赤峰人, 南京理工大学副教授, 主要研究方向为云计算安全、访问控制、代理重加密。



王彬 (1998-), 男, 北京人, 主要研究方向为大数据分析、等级测评。



蒋鸿玲 (1986-), 女, 天津人, 博士, 北京信息科技大学讲师, 主要研究方向为网络安全、大数据分析。