·网络空间安全·　　文章编号：1000-3428(2023)06-0144-10　　文献标志码：A　　中图分类号：TP391

基于SM9的两方协同盲签名方案

陈倩倩[1,2]，秦宝东[1,2]

（1.西安邮电大学 网络空间安全学院，西安 710121；2.无线网络安全技术国家工程实验室，西安 710121）

摘　要：为了解决现有国密SM9盲签名方案中签名私钥易泄露以及签名权力过于集中的问题，提出一种基于国密SM9的两方协同盲签名方案。密钥生成中心将SM9的签名私钥分割成两个部分并分配给两方签名者，同时设计一种两方协同盲签名的协议，在该协议中用户使用特定的盲化因子对待签消息进行盲化，由两个签名参与方合作生成合法的SM9盲签名。该协议保证只有拥有签名权限的通信双方才能合作生成有效的SM9盲签名，且在交互签名的过程中不会泄漏完整的SM9签名私钥，在保护待签消息隐私的同时能有效解决现有SM9盲签名中签名私钥的安全性问题，且两方签名协议的设计能满足特定场景下对分散签名权力的需求。理论分析与仿真结果表明，该方案的签名长度接近现有SM9相关签名方案但功能更加完善，在通用安全构架下被证明满足盲签名的基本安全要求，相较原始SM9签名方案，所提方案在增加合理时间消耗的前提下能够有效提高协同特性。

关键词：SM9算法；基于标识的签名；盲签名；密钥分割；两方协同签名

开放科学（资源服务）标志码（OSID）：

中文引用格式：陈倩倩，秦宝东.基于SM9的两方协同盲签名方案[J].计算机工程，2023，49(6)：144-153，161.

英文引用格式：CHEN Q Q，QIN B D. Two-party cooperative blind signature scheme based on SM9[J]. Computer Engineering，2023，49(6)：144-153，161.

Two-Party Cooperative Blind Signature Scheme Based on SM9

CHEN Qianqian[1,2]，QIN Baodong[1,2]

（1.School of Cyberspace Security，Xi'an University of Posts and Telecommunications，Xi'an 710121，China；
2.National Engineering Laboratory for Wireless Security，Xi'an 710121，China）

【Abstract】In the existing SM9 blind signature scheme，the signature private key is leaked easily and the signature power is centralized，which are problematic. Hence，a two-party collaborative blind signature scheme based on SM9 is proposed. The Key Generation Center（KGC）separates the signature private key of SM9 into two and distributes it to two signers. Additionally，it designs a two-party cooperative blind signature protocol，in which the user uses a specific blinding factor to conceal the message to be signed，and the two signature participants cooperate to generate a legal SM9 blind signature. This protocol ensures that only the communication parties with signature authority can cooperate to generate an effective SM9 blind signature and that the complete SM9 signature private key will not be disclosed during an interactive signature. Thus，the security problem of the signature private key in the existing SM9 blind signature is solved effectively while the privacy of the message to be signed is protected. Furthermore，the design of the two-party signature protocol satisfies the requirements for decentralized signature authority in specific scenarios. Theoretical analysis and simulation results show that the signature length of the proposed scheme is similar to that of the existing SM9-related signature scheme but its function is more ideal；additionally，the proposed scheme can satisfy the basic security requirements of blind signatures under the general security framework. Compared with the original SM9 signature scheme，the proposed scheme can effectively improve its cooperative characteristics by increasing the reasonable time consumption.

【Key words】SM9 algorithm；Identity-Based Signature（IBS）；blind signature；key segmentation；two-party cooperative signature

DOI：10. 19678/j. issn. 1000-3428. 0064968

基金项目：国家自然科学基金面上项目（61872292）；青海省基础研究计划项目（2020-ZJ-701）。

作者简介：陈倩倩（1998—），女，硕士研究生，主研方向为数字签名及应用；秦宝东（通信作者），教授、博士。

收稿日期：2022-06-13　　**修回日期：**2022-08-04　　**E-mail：**qinbaodong@xupt.edu.cn

0　概述

进入21世纪以来，智能手机、平板电脑等移动设备的普及率逐年提升，互联网在人类社会中的覆盖面和应用范围日益扩大，逐渐成为人们工作学习生活中不可或缺的部分。近年来，我国互联网行业发展迅速，已经达到人人互联的新阶段，据中国互联网络信息中心（CNNIC）2022年2月25日发布的第49次《中国互联网络发展状况统计报告》显示，截止2021年12月，我国网民规模达10.32亿，互联网普及率为73%，其中，网民使用手机上网的比例为99.7%[1]。

目前，互联网设备主要以笔记本电脑、台式机以及移动设备为代表，且90%以上的网络接入是通过移动智能终端完成的。在这种情景下，用户的隐私数据信息被不法分子截获以从事非法交易的风险大幅增加，而这些安全风险事关社会稳定乃至国家安全。秉承着信息安全风险自主可控以及核心技术自主创新的理念，国家密码管理局组织密码学专家对标识密码算法进行了深入研究，于2007年12月正式完成了属于国家标识密码算法的设计工作，紧接着在2008年确定该密码算法型号为SM9，2016年SM9算法被国家密码管理局正式认定为密码行业标准算法[2]。与公钥证书密码算法相比，SM9算法省去了复杂的密钥管理环节，简化了设备之间的申请和验证流程。2022年，秦宝东等[3]提出一种基于仲裁的SM9标识加密算法，其能够解决现有SM9算法的密钥更新和撤销问题。同年，张博鑫等[4]提出一种高效可撤销的SM9数字签名算法，该算法适用于大量移动设备用户之间交互通信的场景。

进入信息化时代，人们对隐私保护的意识提高，这对数字签名技术提出了更高的要求，也促使各种带有特殊性质的数字签名应运而生，其中，盲签名正是为了在电子支付、电子投票系统中防止签名被追踪到而被提出。1983年，CHAUM[5]首先提出盲签名的概念，盲签名是指由用户把待签名的消息进行盲化处理后发送给签名方进行签名的一个过程，通过对消息进行处理，使得签名方无法得知所签消息的具体内容，从而达到对用户信息进行隐私保护的目的。用户在数字签名过程中保护自身信息不被泄露的需求可以通过盲签名这种特殊性质的签名来满足。

自从盲签名技术被提出以来，国内外学者对其展开了深入研究，针对近年来常见的密码算法，有学者提出了各种不同密码体制下且适用于不同场景的盲签名方案。张学军[6]在基于身份的密码体制下提出改进的代理盲签名方案。曹素珍等[7]提出一种新的基于身份的部分盲签名方案。王方鑫[8]提出一种基于RSA的盲签名算法。顾兆军等[9]提出一种基于身份的ElGmal盲签名方案。张雪锋等[10]提出一种基于SM9算法的盲签名方案。王倩[11]设计基于编码的盲签名在电子投票系统中的应用方案。何德彪等[12]提出一种SM9数字签名的盲签名生成方法。吕尧等[13]在张雪锋等[10]所提方案的基础上提出一种基于SM9算法的部分盲签名方案。陈丽燕[14]提出Hash-RSA盲签名的数字货币方案。姜昊堃等[15]提出一种改进的具有前向安全性的无证书代理盲签名方案。唐卫中等[16]提出基于SM2的无证书盲签名方案。关于盲签名的研究方案众多，但是目前少有基于国家标识密码算法SM9的盲签名研究方案。

2021年11月11日，党的十九届六中全会圆满闭幕。为了响应党的“发展数字经济”的号召，我国科研工作者积极开展了关于数字货币的一系列研究。比特币作为数字货币的代表，以区块链技术为核心架构，匿名性是其一个重要特点[17]。区块链系统通过嵌入椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA）来实现，用公钥产生地址，而ECDSA中的公私钥对与现实生活中用户的身份无关。因此，在数字货币的研究中，有必要嵌入基于身份的数字签名，用户隐私可以使用盲签名技术来进行安全保护。我国推出的SM9系列算法从2020年11月开始被陆续纳入ISO/IEC国际标准，得到了国际社会的认可[18]。基于SM9的盲签名可以视为数字货币系统中基于身份的数字签名候选方案，然而，尽管SM9算法避免了证书管理的环节，但是始终存在密钥托管的问题，如密钥丢失、单点攻击、签名私钥拥有者不可信等问题。若要实现相对安全的SM9盲签名方案，必须考虑如何保证用户的私钥安全以及在某些场景中签名权力集中在一方所导致的权力滥用问题。在通常情况下，进行私钥分割是一种密钥保护手段。2017年，何德彪等[19]提出一种两方分布式SM9数字签名生成方法，其本质是运用私钥分割的方法。2020年，MU等[20]将SM9数字签名与Paillier加密相结合，提出一种安全两方SM9协同签名方案。

本文在何德彪等[19]研究工作的基础上，提出一种应用SM9算法分割签名密钥并分配给两方签名者进行盲签名的方案，将分割后的部分私钥分别交由参与盲签名的两方通讯设备保存，签名双方持有各自的部分私钥，运用本文所提SM9协同盲签名协议进行交互合作，从而生成合法盲签名。

1　预备知识

1.1　双线性对

双线性对定义在一组椭圆曲线群上，其作为密码学算法的构造工具被应用于众多加密、签名等技术中。假设λ是一个安全参数，N是一个与λ相关的大素数。双线性对中循环群G_1、G_2及G_T的阶都为素数N，其中，G_1和G_2两个群是加法群，G_T是一个乘法群。假设群元素Q_1是群G_1的生成元，群元素Q_2是

群G_2的生成元，如果存在一个从群G_2到G_1的同态映射φ使得$\varphi(Q_2)=Q_1$，在这3个群上存在映射关系$G_1\times G_2\to G_T$并且满足下列3个条件，则称映射e：$G_1\times G_2\to G_T$是一个双线性对映射[21]：

1）双线性性。对于任意元素$P\in G_1$、$Q\in G_2$且$a,b\in\mathbb{Z}_N$，存在$e(aP,bQ)=e(P,Q)^{ab}$。

2）非退化性。$e(Q_1,Q_2)\neq 1$。

3）易计算性。对于任意$P\in G_1$、$Q\in G_2$，都存在一个可行的算法能快速计算出$e(P,Q)$。

1.2 困难问题假设

本文所提协同盲签名方案的安全性基于定义1所示的困难问题假设，其中，在双线性群G_1和G_2上，P是G_1的生成元，Q是G_2的生成元。

定义1（q-强Diffie-Hellman问题（q-Strong Diffie-Hellman，q-SDH））[22] 给定$q+1$个元素$P,sP,s^2P,\cdots,s^qP$，不存在一个概率多项式算法能以不可忽略的概率计算出$\left(c,\frac{1}{c+s}P\right)$，其中，$s,c\in\mathbb{Z}_N^*$。

1.3 SM9数字签名算法

SM9数字签名算法是国家密码管理局发布的SM9算法系列下基于标识的签名（Identity-Based Signature，IBS）[23]算法。与传统公钥签名算法不同，IBS中由基于用户的身份标识信息生成签名私钥以及相关的系统参数，因此，在SM9数字签名算法中，B方通过密钥生成中心（Key Generation Center，KGC）派发的签名私钥对消息进行签名，若A方想验证B方的签名，A可以通过获取B方的身份信息得到公钥来进行签名验证，从而提高安全性和效率。SM9数字签名算法方案描述具体如下：

1）系统主密钥生成。

KGC随机产生数字$ks\in[1,N-1]$作为系统的主私钥，为了计算主公钥并计算群G_2中的元素$P_{\text{pub}}=[ks]P_2$，则系统主密钥对为(ks,P_{pub})，KGC秘密保存主私钥ks，公开主公钥P_{pub}。

2）用户签名密钥生成。

KGC选择并公开用一个字节表示的私钥生成函数识别符hid，用户B的标识为ID_B，为产生用户B的私钥，KGC首先计算$t_1=H_1(\text{ID}_\text{B}\|\text{hid},N)+ks$：若$t_1=0$，则需重新计算产生主私钥，公开主公钥，并更新已有用户的私钥；否则，计算$t_2=ks\cdot t_1^{-1}\ (\text{mod}\ N)$，然后计算签名私钥$d_\text{B}=[t_2]P_1$。

用户公钥设为Q_B，可由系统内任一用户生成$Q_\text{B}=\left[H_1(\text{ID}_\text{B}\|\text{hid},N)\right]P_2+P_{\text{pub}}$。

3）SM9数字签名生成算法。

假设待用户B签名的明文消息为比特串M，用户B需执行以下步骤来获取明文消息M的数字签名(h,S)：

（1）计算群G_T中的元素$g=e(P_1,P_{\text{pub}})$。

（2）产生随机数$r\in[1,N-1]$。

（3）计算群G_T中的元素$w=g^r$，将w的数据类型转换为比特串。

（4）计算整数$h=H_2(M\|w,N)$。

（5）计算整数$L=(r-h)\bmod N$，若$L=0$，则返回第（2）步。

（6）计算群G_1中的元素$S=[L]d_\text{B}$。

（7）将h和S的数据类型转换为字节串，消息M的签名为(h,S)。

4）SM9数字签名验证算法。

验证用户A，即为检验收到的消息M'及其数字签名(h',S')是否合法，执行以下步骤：

（1）首先将h'转换为整数的数据类型，然后检验$h'\in[1,N-1]$是否满足，若不满足条件，则验证不通过。

（2）将S'转变为椭圆曲线上的点的类型，检验是否满足要求，若不满足，则验证不通过。

（3）计算群G_T中的双线性对元素$g=e(P_1,P_{\text{pub}})$。

（4）计算群G_T中的元素$t=g^{h'}$。

（5）计算整数$h_1=H_1(\text{ID}_\text{B}\|\text{hid},N)$。

（6）计算群G_2中的元素$P=[h_1]P_2+P_{\text{pub}}$。

（7）计算群G_T中的元素$u=e(S',P)$。

（8）计算群G_T中的元素$w'=u\cdot t$，将w'的数据类型转换为比特串。

（9）计算整数$h_2=H_2(M'\|w',N)$，检验$h_2=h'$等式是否成立：如果成立，则检验通过；否则，不是合法的签名。

1.4 盲签名技术

盲签名是一种签名消息对签名者不可见的具有特殊性质的数字签名，即签名者在无法看到消息原始内容的条件下进行数字签名[24]，其基本原理可以形象化表示为：对文件签名时可以通过在信封里加上复写纸，使签名者在信封外的签名能透过复写纸签署到文件上。

盲签名的签名方无法获得待签消息的具体内容，这就使得盲签名具有一般数字签名不具备的两个特性：

1）盲性。除了待签名消息的拥有者知道消息的具体内容以外，其余任何人都不可见。

2）不可追踪性。因为签名者不知道消息的具体内容，即使签名消息被公布，签名者也无法得到签名与此前签署过消息的对应信息。

盲签名的签名步骤描述如下：

1）用户对原始消息进行运算得到盲化后的信息，将该盲化后的信息发送给签名者。

2）签名者在收到盲化消息后，使用KGC分配的签名私钥对盲化后的信息进行签名得到盲签名。

3）签名者将盲签名发送给用户，用户对盲签名

进行去盲运算从而得到正常的签名。

由于盲签名由签名者发送给用户进行去盲操作，此时的签名已经和普通的数字签名无异，因此盲签名的验证步骤与普通数字签名一致。盲签名流程如图1所示。

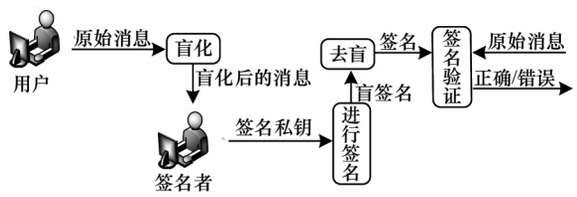

图1　盲签名流程

Fig.1　Blind signature procedure

2　两方协同盲签名方案

2.1　方案定义

一个两方协同盲签名方案由以下4个多项式时间算法描述：

1）系统建立Setup(λ)。以系统安全参数λ为输入，系统建立算法输出系统主公钥mpk和主私钥msk，该算法由密钥生成中心（KGC）运行。

2）密钥生成Setup(msk, ID)。定义用户的身份ID为用户的签名密钥，密钥生成中心生成通信双方A和B签名所需的密钥，令$\mathrm{ID_A}$表示第一通信方，$\mathrm{ID_B}$表示第二通信方，该算法由密钥生成中心运行。

3）协同盲签名。假设比特串m为待签名的消息，如果要得到待签消息m的数字签名(h,S)，则由消息拥有者对消息m进行盲化。通信双方A和B基于分配的签名密钥进行交互合作生成完整盲签名，再交由消息拥有者进行解盲。

4）签名验证Verify(mpk, ID, M,δ)。第三方验证是否生成合法的盲签名。

SM9两方协同盲签名方案的模型结构如图2所示。

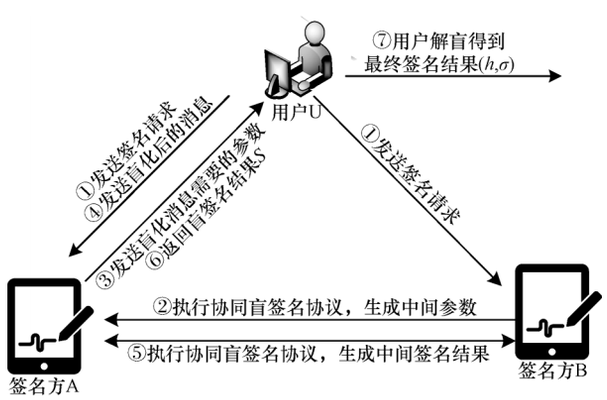

图2　两方协同盲签名系统模型结构

Fig.2　Two-party cooperative blind signature system model structure

2.2　方案构造

两方协同盲签名方案描述如下：

1）生成系统参数。

给定安全参数λ，KGC选取N阶循环群G_1、G_2及其生成元P_1、P_2，存在映射关系$P_1=\varphi(P_2)$，以及双线性对e的值域为N阶的乘法循环群G_T，其中$N>2^{\lambda}$，构成双线性群$B=(G_1,G_2,G_T,e,N)$。随机选取$ks\in[1,N-1]$作为主私钥，计算$P_{\mathrm{pub}}=[ks]P_2$，并选择密码杂凑函数$H_1:\{0,1\}^*\to\mathbb{Z}_N^*$、$H_2:\{0,1\}^*\times G_T\times N\to\mathbb{Z}_N^*$。计算群$G_T$中的元素$g=e(P_1,P_{\mathrm{pub}})$，然后选取用一个字节表示的签名私钥生成函数识别符hid，设系统主公钥为$\mathrm{mpk}=(B,g,P_1,P_2,P_{\mathrm{pub}},H_1,H_2,\mathrm{hid})$。

2）签名密钥生成。

给定用户标识$\mathrm{ID}\in\{0,1\}^*$，按如下步骤生成签名通信方A和B的签名密钥：

（1）KGC首先计算$t_1=H_1(\mathrm{ID}\|\mathrm{hid},N)+ks$，若$t_1=0$，则需重新计算系统主公钥并公开；否则，计算$t_2=ks\cdot t_1^{-1}\pmod N$，其中，$t_1^{-1}$表示$t_1$模$N$的逆元。

（2）KGC随机选取$c_1\in[1,N-1]$，并计算$c_2=c_1^{-1}\cdot t_2\pmod N$。

（3）KGC计算通信方A所掌握的部分签名密钥$D_{\mathrm{ID_A}}=c_1$，计算$Q_0=[c_2]\cdot P_1$，通信方B所掌握的另一部分密钥$D_{\mathrm{ID_B}}=Q_0$。

（4）分别将$D_{\mathrm{ID_A}}$和$D_{\mathrm{ID_B}}$存储到设备A和B中。

3）协同盲签名算法。

给定待签明文数据$M\in\{0,1\}^*$，为了得到消息M的数字签名(h,σ)，消息拥有者U盲化消息M和签名方A、签名方B进行协同盲签名，步骤如下：

（1）首先由签名方B随机选取$k_1,k_2\in[1,N-1]$，计算$w_1=g^{k_1}$，$w_2=g^{k_2}$，将w_1和w_2发送给签名方A。

（2）签名方A随机选取$k_3,k_4\in[1,N-1]$，接收到签名方B发送的w_1和w_2后，计算$w=w_1^{c_1^{-1}k_3}\cdot w_2\cdot g^{k_4}$，然后签名方A将$w$发送给消息拥有者。

（3）消息拥有者user为了盲化消息，随机选取两个盲化因子$\alpha,\beta\in[1,N-1]$，计算$w'=w^{\alpha}\cdot g^{\beta}$，$h=H_2(M\|w',N)$，$h'=\alpha^{-1}(h-\beta)\bmod N$，消息拥有者将$h'$发送给签名方A。

（4）签名方A收到h'后计算$h''=(k_4-h')\bmod N$，将h''发送给签名方B。

（5）签名方B计算$Q_1=[k_1]\cdot Q_0$，收到h''后计算$Q_2=[h''+k_2]\cdot Q_0$，将Q_1和Q_2发送给签名方A。

（6）签名方A收到Q_1和Q_2后计算签名$S=[k_3]\cdot Q_1+[c_1]\cdot Q_2$，将盲签名$S$发送给消息拥有者user。

（7）消息拥有者user收到盲签名S后进行解盲，$\sigma=[\alpha]S$，输出消息M和最后的签名$\delta=(h,\sigma)$。

4)签名验证算法。

验证者对收到的消息M'和签名$\delta'=(h,\sigma)$进行验证,执行以下步骤:

(1)检验$h\in[1,N-1]$、$\sigma\in G_1$是否成立。

(2)计算整数$h_1=H_1(\mathrm{ID}\|\mathrm{hid},N)$。

(3)计算$P=[h_1]P_2+P_{\mathrm{pub}}$。

(4)计算$u=e(\sigma,P),t=g^h$。

(5)计算$w''=u\cdot t$。

(6)计算$h_2=H_2(M'\|w'',N)$。

(7)若$h_2=h$,则签名验证通过。

2.3 正确性分析

本文基于SM9协同盲签名方案的正确性验证过程如下:

在消息拥有者user、签名方A和签名方B的协同盲签名过程中:

$$w'=w^{\alpha}\cdot g^{\beta}=\left(w_1^{c_1^{-1}k_3}\cdot w_2\cdot g^{k_4}\right)^{\alpha}\cdot g^{\beta}=$$
$$\left(g^{c_1^{-1}k_1k_3}\cdot g^{k_2}\cdot g^{k_4}\right)^{\alpha}\cdot g^{\beta}=g^{\alpha\left(c_1^{-1}k_1k_3+k_2+k_4\right)+\beta}$$

在签名验证过程中,若解盲后的协同盲签名(h,σ)和用户标识ID均正确,则有:

$$w''=u\cdot t=e(\sigma,P)\cdot g^h=$$
$$e\left([\alpha]\cdot S,[h_1]P_2+P_{\mathrm{pub}}\right)\cdot e\left(P_1,P_{\mathrm{pub}}\right)^h=\left([\alpha]\cdot\left([k_3]\cdot Q_1+[c_1]\cdot Q_2\right),[h_1+ks]\cdot P_2\right)\cdot e\left(P_1,P_2\right)^{ks\cdot h}=$$
$$e\left([\alpha]\left([k_3]\cdot[k_1]\cdot[c_2]\cdot P_1+[c_1]\cdot[h''+k_2]\cdot[c_2]\cdot P_1\right),[h_1+ks]\cdot P_2\right)\cdot e\left(P_1,P_2\right)^{ks\cdot h}=$$
$$e\left([\alpha]\cdot\left([k_3\cdot k_1\cdot c_1^{-1}\cdot ks\cdot t_1^{-1}]\cdot P_1+[c_1]\cdot\left[k_4-\alpha^{-1}\cdot(h-\beta)+k_2\right]\cdot[c_1^{-1}\cdot ks\cdot t_1^{-1}]\cdot P_1\right),[h_1+ks]\cdot P_2\right)\cdot$$
$$e\left(P_1,P_2\right)^{ks\cdot h}=e\left([\alpha]\left(k_3\cdot k_1\cdot c_1^{-1}\cdot ks\cdot(h_1+ks)^{-1}+\left[k_4-\alpha^{-1}\cdot(h-\beta)+k_2\right]\cdot[c_1]\cdot\left[c_1^{-1}\cdot ks\cdot(h_1+ks)^{-1}\right]\right)P_1,\right.$$
$$\left.[h_1+ks]\cdot P_2\right)\cdot e\left(P_1,P_2\right)^{ks\cdot h}$$

整理上式得到:

$$w''=e\left([\alpha]\left(k_3\cdot k_1\cdot c_1^{-1}+k_4-\alpha^{-1}(h-\beta)+k_2\right)\cdot\left[ks\cdot(h_1+ks)^{-1}\right]\cdot P_1,[h_1+ks]\cdot P_2\right)\cdot e\left(P_1,P_2\right)^{ks\cdot h}=$$
$$e\left([\alpha]\left(k_3\cdot k_1\cdot c_1^{-1}+k_4-\alpha^{-1}(h-\beta)+k_2\right)\cdot[ks]\cdot P_1,P_2\right)^{(h_1+ks)^{-1}\cdot[h_1+ks]}\cdot e\left(P_1,P_2\right)^{ks\cdot h}=$$
$$e\left([\alpha]\left(k_3\cdot k_1\cdot c_1^{-1}+k_4-\alpha^{-1}(h-\beta)+k_2\right)\cdot[ks]\cdot P_1,P_2\right)\cdot e\left(P_1,P_2\right)^{ks\cdot h}=$$
$$e\left(P_1,P_2\right)^{\left(\alpha\left(k_3\cdot k_1\cdot c_1^{-1}+k_4+k_2\right)-h+\beta\right)\cdot ks+h\cdot ks}=e\left(P_1,P_2\right)^{\left(\alpha\left(k_3\cdot k_1\cdot c_1^{-1}+k_4+k_2\right)-h+\beta+h\right)\cdot ks}=$$
$$e\left(P_1,ks\cdot P_2\right)^{\alpha\left(k_3\cdot k_1\cdot c_1^{-1}+k_4+k_2\right)+\beta}=g^{\alpha\left(k_3\cdot k_1\cdot c_1^{-1}+k_4+k_2\right)+\beta}$$

$w''=w'$,即等价于验证了$h_2=h$的正确性,因此,签名验证通过,本文方案能够满足正确性要求。

3 安全性分析

3.1 安全型模型定义

与普通的盲签名方案类似,本文协同盲签名方案也应该满足不可伪造性和盲性。两方协同盲签名方案需要由消息拥有者和两方签名者合作生成合法盲签名,在此假设参与协同盲签名的三方都是诚实且好奇的。下面给出协同盲签名方案的不可伪造性和盲性的形式化定义。

定义2(不可伪造性) 给定一个协同盲签名方案$\Gamma=(\Gamma_{\mathrm{U}},\Gamma_{\mathrm{A}},\Gamma_{\mathrm{B}})$,三元素分别表示消息拥有者U、签名方A和签名方B在协同盲签名方案中按照各自步骤执行方案的过程。定义一个概率多项式时间内的攻击算法$\Re$,并可能存在至多能腐化一位诚实且好奇的参与者$\mathrm{I}\in\{\mathrm{A},\mathrm{B}\}$。通过攻击者$\Re$与挑战者$\Im$的如下攻击游戏,定义协同盲签名方案的不可伪造性攻击实验$\mathrm{Exp}_{\Re,\Gamma}^{\mathrm{EU\text{-}CMA}}(\lambda)$[25]:

1)初始化阶段。给定系统参数λ,挑战者运行系统参数生成算法Setup(λ)生成系统主公钥mpk和主私钥msk。挑战者将系统主公钥发送给攻击者。

2)询问阶段。攻击者可以进行以下询问:

(1)私钥生成询问。攻击者需要多次选择一个身份ID并将其发送给挑战者,挑战者执行协同密钥生成算法$\mathrm{KeyGen}(\mathrm{msk},\mathrm{ID})$,返回第一签名人和第二签名人的部分私钥$D_{\mathrm{ID_A}}$和$D_{\mathrm{ID_B}}$给攻击者。

(2)挑战私钥询问。攻击者需要选择一个挑战身份ID^*并将其发送给挑战者,挑战者执行协同密钥生成算法$\mathrm{KeyGen}(\mathrm{msk},\mathrm{ID}^*)$,得到挑战身份的第一签名人以及第二签名人的部分私钥$D_{\mathrm{ID}_{\mathrm{A}}^*}$和$D_{\mathrm{ID}_{\mathrm{B}}^*}$。

(3)腐化询问。挑战者腐化$\mathrm{I}\in\{\mathrm{A},\mathrm{B}\}$,若$\mathrm{I}=\mathrm{A}$(或$\mathrm{I}=\mathrm{B}$),则挑战者将部分私钥$D_{\mathrm{ID}_{\mathrm{A}}^*}$(或$D_{\mathrm{ID}_{\mathrm{B}}^*}$)返回给攻击者。

(4)盲签名询问。攻击者可以与挑战者交互执行多项式次协同盲签名协议,并获取相应消息的签名结果。

3）伪造阶段。假设攻击者询问挑战身份的签名为m次并输出$m+1$个消息-签名对$(M_1,\delta_1),\cdots,(M_m,\delta_m),(M_{m+1},\delta_{m+1})$。

4）输出阶段。对于任意的$i,j\in\{1,m+1\}$，若$M_i\neq M_j$，$\mathrm{Verify}(\mathrm{mpk},\mathrm{ID}^*,M_i,\delta_i)=1$，则返回1；否则，返回0。

在上述游戏中，若返回1，代表攻击者通过m次协议交互得到m+1个合法签名。因此，攻击者至少成功伪造了一个签名。攻击者在实验$\mathrm{Exp}_{\Re,\Gamma}^{\mathrm{EU\text{-}CMA}}(\lambda)$中成功的概率定义为：

$$\mathrm{Adv}_{\Re,\Gamma}^{\mathrm{EU\text{-}CMA}}(\lambda)=\Pr\left[\mathrm{Exp}_{\Re,\Gamma}^{\mathrm{EU\text{-}CMA}}(\lambda)=1\right]$$

若$\mathrm{Adv}_{\Re,\Gamma}^{\mathrm{EU\text{-}CMA}}(\lambda)$是一个可忽略的概率，则称该方案满足不可伪造性。

定义3（盲性）　给定一个协同盲签名方案$\Gamma=(\Gamma_{\mathrm{U}},\Gamma_{\mathrm{A}},\Gamma_{\mathrm{B}})$，假设$\Re$是任意一个概率多项式时间攻击者，定义盲性实验$\mathrm{Exp}_{\Re,\Gamma}^{\mathrm{Blind}}(\lambda)$如下：

1）初始化阶段。首先，攻击者$\Re$利用协同盲签名方案的系统参数生成算法Setup(λ)生成系统主公钥mpk和主私钥msk；然后，攻击者$\Re$选择一个挑战身份ID^*，并利用密钥生成算法$\mathrm{KeyGen}(\mathrm{msk},\mathrm{ID}^*)$分别生成第一签名人和第二签名人的私钥$D_{\mathrm{ID_A}}$和$D_{\mathrm{ID_B}}$；最后，攻击者将主公钥mpk和挑战身份$\mathrm{ID}^*$发送给挑战者$\Im$。

2）挑战阶段。挑战者$\Im$选择两个消息$M_0,M_1\in\{0,1\}^*$，通过与攻击者$\Re$交互分别获得挑战身份ID^*下的两个签名δ_0和δ_1。挑战者随机选择1 bit的$b\in\{0,1\}$，并将(M_0,M_1,δ_b)发送给攻击者$\Re$。

3）猜测阶段。攻击者$\Re$输出1 bit的$b'\in\{0,1\}$，作为对b的猜测结果。

4）输出阶段。若$b=b'$，则返回1；否则，返回0。

攻击者在实验$\mathrm{Exp}_{\Re,\Gamma}^{\mathrm{Blind}}(\lambda)$中成功的优势定义为：

$$\mathrm{Adv}_{\Re,\Gamma}^{\mathrm{Blind}}(\lambda)=\Pr\left[\mathrm{Exp}_{\Re,\Gamma}^{\mathrm{Blind}}(\lambda)=1\right]-\frac{1}{2}$$

若$\mathrm{Adv}_{\Re,\Gamma}^{\mathrm{Blind}}(\lambda)$是一个可忽略的量，则称该方案满足盲性。

3.2　安全性证明

本文SM9协同盲签名方案的不可伪造性基于原始SM9签名方案的可证明安全性[26]，在方案的安全性证明中，本文借鉴文献[26]中的证明技术，不可伪造性由定理1保证，定理2保证本文方案的签名满足盲性。

定理1　在随机谕言机模型以及q-SDH假设下，本文所提基于SM9的两方协同盲签名方案是EUF-CMIA安全的。

证明　假定存在一个适应性选择消息和身份的攻击算法$\Re$，在询问q_{H_i}次随机谕言机$H_i(i=1,2)$后在概率多项式时间内以不可忽略的优势ε攻破方案，假设该攻击算法$\Re$访问私钥询问谕言机的次数为q_E，访问签名谕言机的次数为q_S，则存在一个模拟算法$\Im$可以和攻击算法$\Re$交互，并且在概率多项式时间t'内以不可忽略的优势ε'解决q-SDH问题。

假设给模拟算法$\Im$一个挑战问题，即双线性群$B=(G_1,G_2,G_T,e,N)$中的q-SDH问题：$P,Q,sQ,s^2Q,\cdots,s^qQ$，其中，P和Q分别为群G_1和G_2的生成元，模拟算法$\Im$通过调用攻击算法$\Re$成功找到q-SDH问题的一个解，即$\left(c,\frac{1}{c+s}P\right)$，其中，$c\in\mathbb{Z}_N^*$。为了方便描述，将攻击算法对谕言机$H_1$的询问次数简写为$q$。

1）初始化阶段。首先，模拟算法$\Im$隐式地设系统主私钥为$\mathrm{msk}=s$，即s是q-SDH问题中未知的随机数。其次，模拟算法从谕言机H_1的q次询问中随机选取$r^*\in[1,q]$，从空间$\mathbb{Z}_N^*$中选取q个不同的随机数$b^*,b_1,b_2,\cdots,b_{r^*-1},b_{r^*+1},\cdots,b_q$并生成如下多项式：

$$f(z)=\prod_{r=1,r\neq r^*}^{q}(z+b_r)=\sum_{r=0}^{q-1}c_rz^r$$

接着，模拟算法令$\varphi(Q)=P$，并计算群G_2和G_1的生成元，即：

$$P_2=f(s)Q=\sum_{r=0}^{q-1}c_r(s^rQ),P_1=\varphi(P_2)=f(s)P\in G_1$$

随后，模拟算法计算系统的主公钥参数$P_{\mathrm{pub}}=sP_2=\sum_{r=1}^{q}c_{r-1}(s^rQ)$以及$g=e(P_1,P_{\mathrm{pub}})$，令$f_r(z)=\frac{f(z)}{s+b_r}=\sum_{r=0}^{q-2}d_rz^r$。通过上述构造可以看出，除$r^*$外，对任意的$r\in[1,q]$有：

$$\sum_{r=0}^{q-2}d_r\cdot\varphi(s^{r+1}Q)=sf_r(s)P=\frac{sf(s)}{s+b_r}P=\frac{s}{s+b_r}P_1$$

因此，除了r^*，对于任意的$r\in[1,q]$，模拟算法都可以得到一组元素$\left(b_r,\frac{s}{s+b_r}P_1\right)$。

最后，模拟算法$\Im$选择两个密码杂凑函数H_1：$\{0,1\}^*\to\mathbb{Z}_N^*$和$H_2$：$\{0,1\}^*\times G_T\times N\to\mathbb{Z}_N^*$，令系统的主公钥为$\mathrm{mpk}=(P_1,P_2,g,P_{\mathrm{pub}})$，并将mpk发送给攻击算法。

2）哈希询问阶段。攻击算法$\Re$可以询问谕言机H_1、H_2，模拟算法$\Im$按照以下步骤给出回应：

（1）H_1询问。攻击算法$\Re$询问任意ID_r，模拟算法$\Im$创建二元组(ID,b)的列表L_1，若询问的$\mathrm{ID}_r\in L_1$，则返回b_r。若列表中没有询问的ID_r，则记ID_r为一个新的询问。若$r=r^*$，记ID_{r^*}为ID^*，设$H_1(\mathrm{ID}^*)=b^*$，发送b^*给攻击算法$\Re$，模拟算法$\Im$添加(ID^*,b^*)到L_1；若$r\neq r^*$，设$H_1(\mathrm{ID}_r)=b_r$，发送b_r给$\Re$并将(ID_r,b_r)

更新到L_1。

(2)H_2询问。攻击算法$\mathfrak{R}$询问任意(M_r,w_r'),模拟算法$\mathfrak{I}$创建二元组(M,w',h)的列表L_2,若询问的$M_r,w_r'\in L_2$,则返回w_r'。若列表中没有询问的ID_r,随机选取$h_r\in\mathbb{Z}_N^*$,设$H_2(M_r,w_r')=h_r$,发送h_r给攻击算法$\mathfrak{R}$,模拟算法$\mathfrak{I}$添加(M_r,w_r',h_r)到L_2。

3)私钥生成询问。若$\mathrm{ID}_r=\mathrm{ID}^*$,模拟算法$\mathfrak{I}$输出失败,停止模拟;若$\mathrm{ID}_r\neq\mathrm{ID}^*$,模拟算法$\mathfrak{I}$令$d_r=\frac{s}{s+b_r}P_1$作为$\mathrm{ID}_r$的完整私钥。模拟算法随机选取$c_r\in[1,N-1]$,并计算$Q_r=[c_r^{-1}]\cdot d_r$。令第一签名者的部分私钥为$D_{\mathrm{ID}_{r,\mathrm{A}}}=c_r$,第二签名者的部分私钥为$D_{\mathrm{ID}_{r,\mathrm{B}}}=Q_r$。最后,模拟算法将$D_{\mathrm{ID}_{r,\mathrm{A}}}$和$D_{\mathrm{ID}_{r,\mathrm{B}}}$发送给攻击者。

4)挑战私钥询问。攻击者$\mathfrak{R}$选择一个挑战身份ID^*并发送给模拟算法$\mathfrak{I}$。若$\mathrm{ID}^*\neq\mathrm{ID}_{r^*}$,则模拟算法$\mathfrak{I}$输出失败,停止模拟;否则,模拟算法$\mathfrak{I}$随机猜测攻击者$\mathfrak{R}$要攻击的参与者$\mathrm{I}\in\{\mathrm{A},\mathrm{B}\}$并模拟构造协议第一签名者A的私钥或第二签名者B的私钥。具体过程如下:

(1)当$\mathrm{I}=\mathrm{A}$时,$\mathfrak{I}$随机选取$c_1\in[1,N-1]$,令$D_{\mathrm{ID}_{\mathrm{A}}}=c_1$作为第一签名者A的私钥。

(2)当$\mathrm{I}=\mathrm{B}$时,类似前一种情况,$\mathfrak{I}$随机选取$c_1\in[1,N-1]$,计算$Q_0=[c_1]\cdot P_1$作为B的私钥$D_{\mathrm{ID}_{\mathrm{A}}}$。

5)腐化询问。攻击者选择一个腐化对象$\mathrm{I}'\in\{\mathrm{A},\mathrm{B}\}$。若$\mathrm{I}'\neq\mathrm{I}$,则$\mathfrak{I}$终止游戏;否则,$\mathfrak{I}$将相应的部分签名私钥发送给攻击者。

由模拟算法选取系统参数和公钥的方式可知,该过程与不可伪造性实验初始化系统的方式一致,并且该过程与攻击者的视角完全独立。因此,模拟算法猜对攻击者腐化对象的概率(即$\Pr[\mathrm{I}'=\mathrm{I}]$)至少为1/2。

6)签名询问。记(M_r,ID_r)为第r个消息-身份标识对。若$r\neq r^*$,则模拟算法$\mathfrak{I}$能根据获得的与消息身份标识相对应的签名私钥来运行协同盲签名方案生成合法的签名;否则,模拟算法$\mathfrak{I}$仅知道挑战身份ID_{r^*}的部分私钥。不妨假设模拟算法知道第一签名者A的私钥,根据挑战私钥询问可知$D_{\mathrm{ID}_{\mathrm{A}}}=c_1$。下面证明在不知道第二签名者私钥的情况下,对于攻击者针对挑战身份ID^*任意消息M的签名询问,模拟算法可以按照如下方式完美地模拟方案的每个执行过程。在模拟方案执行前,$\mathfrak{I}$随机选取$\sigma\in G_1$和$h\in\mathbb{Z}_N^*$,计算$P^*=b^*P_2+P_{\mathrm{pub}}$和$w'=e(\sigma,P^*)e(P_1,P_{\mathrm{pub}})^h$,并定义$H_2(M\|w',N)=h$。如果$(M,w')$已经被询问过,$\mathfrak{I}$输出失败。由于$(M,w')$已经被询问过的概率为$\frac{q_{H_2}+q_s}{2^\lambda}$,是一个可忽略的量,因此$\mathfrak{I}$输出失败的概率是可忽略的。接下来,$\mathfrak{I}$模拟每个实体的过程如下:

(1)$\mathfrak{I}$模拟第二签名者B。随机选择$k_1',k_2',k_3,k_4,h'\in[1,N-1]$,并隐式定义$k_1=(s+b^*)\cdot k_1'\bmod N$和$k_2=(s+b^*)\cdot k_2'-(k_4-h')\bmod N$。利用$k_1'$和$k_2'$的随机性可知$k_1$和$k_2$相当于是从$[1,N-1]$中随机选取的。由于$P_{\mathrm{pub}}=sP_2$,$sP_1=\varphi(P_{\mathrm{pub}})$,因此$\mathfrak{I}$可以计算$g^s=e(sP_1,P_{\mathrm{pub}})$,继而可以计算$w_1=g^{k_1}$和$w_2=g^{k_2}$并将$w_1$和$w_2$发送给第一签名者。

(2)$\mathfrak{I}$模拟第一签名者A。计算$w=w_1^{c_1^{-1}k_3}\cdot w_2\cdot g^{k_4}$并将$w$发送给用户。

(3)$\mathfrak{I}$模拟用户U。首先,隐式地选取$\alpha,\beta\in[1,N-1]$使得$w^\alpha\cdot g^\beta=w'$,因此,$H_2(M\|w',N)=h$;然后,令$\alpha^{-1}(h-\beta)=h'\bmod N$;最后,将$h'$发送给第一签名者。由于$h'$是随机选取的,因此$h'=\log_g(w)\bmod N$的概率是可忽略的。由下列方程式可以唯一确定一组参数α和β,使得$w^\alpha\cdot g^\beta=w'$和$\alpha^{-1}(h-\beta)=h'\bmod N$同时成立:

$$\begin{cases}\log_g(w)\cdot\alpha+\beta=\log_g(w')\bmod N\\ h'\cdot\alpha+\beta=h\bmod N\end{cases}$$

因此,$\mathfrak{I}$模拟用户的行为和实际方案相一致。

(4)$\mathfrak{I}$模拟第一签名者A。计算$h''=k_4-h'\bmod N$并发送给第二签名者。

(5)$\mathfrak{I}$模拟第二签名者B。利用第(1)步中选取的k_1'和k_2'计算$Q_1=[c_1^{-1}k_1']\cdot sP_1$和$Q_2=[c_1^{-1}k_2']\cdot sP_1$。由于第二签名者的私钥隐式地定义为$Q_0=\left[c_1^{-1}\cdot\frac{s}{s+b^*}\right]\cdot P_1$,因此$Q_1=[k_1]\cdot Q_0$,$Q_2=[k_2+h'']\cdot Q_0$,与第二签名者实际计算过程一致。$\mathfrak{I}$将$Q_1$和$Q_2$发送给第一签名者。

(6)$\mathfrak{I}$模拟第一签名者A。利用k_3和c_1计算$S=[k_3]\cdot Q_1+[c_1]\cdot Q_2$并发送给用户。

(7)$\mathfrak{I}$模拟用户U。模拟算法令$[\alpha]\cdot S=\sigma$,并将(h,σ)作为盲签名解盲后的结果发送给攻击者。

通过上述分析可知,针对挑战身份的签名询问,模拟算法$\mathfrak{I}$可以模拟方案执行的每个步骤。

7)伪造阶段。攻击算法$\mathfrak{R}$输出挑战身份ID^*对应的$m+1$个消息-签名对(M_i,δ_i)。不妨假设前m个消息-签名对是通过签名询问而得到的,第$m+1$个消息-签名对是成功伪造的,记作(M^*,δ^*),则对于任意$i\in[1,m]$,有$M_i\neq M^*$且$\mathrm{Verify}(\mathrm{mpk},\mathrm{ID}^*,M^*,\delta^*)=1$。

8)输出阶段。令ID^*的下标为r。若$r\neq r^*$,模拟算法$\mathfrak{I}$输出失败并终止;否则,$\mathfrak{I}$执行以下步骤:令(M,w',h,σ)表示该方案的签名结果,其中,w'是内部状态参数,根据分叉引理,若存在一个攻击算法$\mathfrak{R}$能够在时间t内以$\varepsilon>\frac{10(q_s+1)(q_s+q_H)}{2^\lambda}$的概率伪造一个签名$(M,w',h,\sigma)$且不知道相应签名私钥,则存在一个图灵机算法以相同的输入(M,ID)在时间$t'<$

120 686 $q_H t/\varepsilon$内输出两个有效的签名(M,w',h_1,σ_1)和(M,w'',h_2,σ_2)，并且$h_1\neq h_2,\sigma_1\neq\sigma_2$。由此可知，模拟算法$\Im$可以借助攻击算法$\Re$获得两个关于挑战身份$\mathrm{ID}^*$的有效签名$(M^*,h_1^*,\sigma_1^*)$和$(M^*,h_2^*,\sigma_2^*)$，满足$h_1^*\neq h_2^*,\sigma_1^*\neq\sigma_2^*$以及下列验证等式：

$$e\left(\sigma_1^*,H_1(\mathrm{ID}^*)P_2+P_{\mathrm{pub}}\right)\cdot e\left(P_1,P_{\mathrm{pub}}\right)^{h_1^*}=$$
$$e\left(\sigma_2^*,H_1(\mathrm{ID}^*)P_2+P_{\mathrm{pub}}\right)\cdot e\left(P_1,P_{\mathrm{pub}}\right)^{h_2^*}$$

将上式化简整理得：

$$e\left(\left(s^{-1}\left(h_2^*-h_1^*\right)^{-1}\right)\left(\sigma_1^*-\sigma_2^*\right),(b^*+s)P_2\right)=e\left(P_1,P_2\right)$$

令$Y^*=\dfrac{1}{h_2^*-h_1^*}\left(\sigma_1^*-\sigma_2^*\right)=\dfrac{s}{s+b^*}P_1$。因为$P_1=f(s)P$，所以有等式：

$$Y^*=\frac{s}{s+b^*}P_1=\frac{sf(s)}{s+b^*}P=\frac{\gamma}{s+b^*}P+\sum_{r=0}^{q-1}\gamma_r s^r P$$

其中：γ、γ_r是可以求得的系数，且$\gamma\neq 0$。又因为$\varphi(Q)=P$，则有下列等式：

$$B^*=\frac{1}{\gamma}\left(Y^*-\sum_{r=0}^{q-1}\gamma_r\varphi\left(s^rQ\right)\right)=$$
$$\frac{1}{\gamma}\left(Y^*-\sum_{r=0}^{q-1}\gamma_r s^r\varphi\left(Q\right)\right)=\frac{1}{s+b^*}P$$

因此，(b^*,B^*)是q-SDH困难问题的一个解。最后，模拟算法输出(b^*,B^*)。

通过上述分析可知，在伪造签名阶段，如果$\Re$成功伪造出$\mathrm{ID}^*=\mathrm{ID}_{r^*}$对应的签名，那么$\Re$没有询问身份标识$\mathrm{ID}_{r^*}$的概率为$1/q_{H_1}$，等同于模拟算法$\Im$成功猜对挑战身份的概率。因此，如果$\Re$在多项式时间内能以不可忽略的概率$\varepsilon$伪造出合法的签名，那么模拟算法$\Im$能以概率$\varepsilon/q_{H_1}$成功求解$q$-SDH问题。

证毕。

定理2　在随机谕言机模型下，本文所提两方协同盲签名方案具有盲性。

证明　假设$\Re$是一个攻击算法，该算法利用系统参数生成算法Setup(λ)和密钥生成算法$\mathrm{KeyGen}(\mathrm{msk},\mathrm{ID}^*)$分别生成系统主公钥mpk和主私钥以及第一签名人和第二签名人的私钥D_{ID_A}和D_{ID_B}。$\Re$将主公钥mpk和挑战身份ID^*发送给挑战算法$\Im$。模拟算法$\Im$选择任意两个消息$M_0,M_1\in\{0,1\}^*$，并通过盲签名方案获得相应的签名结果(M_0,h_0,σ_0)和(M_1,h_1,σ_1)。$\Im$随机选择1 bit的$b\in\{0,1\}$，并将(M_0,M_1,h_b,σ_b)发送给攻击算法$\Re$。$\Re$输出猜测的1 bit $b'\in\{0,1\}$。下面证明在随机谕言机模型下，攻击算法成功的优势$\Pr[b=b']-1/2$是可忽略的。

将消息M_0和M_1在签名过程中的内部参数w、w'和h'分别记为$w[0]$和$w[1]$、$w'[0]$和$w'[1]$以及$h'[0]$和$h'[1]$。对于攻击者来说，在签名过程中，内部状态$w[0]$和$w[1]$以及$h'[0]$和$h'[1]$是可知的，而$w'[0]$和$w'[1]$是未知的。下面证明对于任意一组给定的内部状态$w[i]$和$h'[i]$以及$w'[j]$和h_j，其中，$i,j\in\{0,1\}$，都存在一组参数$\alpha,\beta\in[1,N-1]$使得下列等式成立：

$$\begin{cases}w'[i]=w[j]^{\alpha}\cdot g^{\beta}\\ h'[i]=\alpha^{-1}(h_j-\beta)\bmod N\end{cases}$$

当$i=j$时，上述等式显然成立；当$i\neq j$时，由于$\log_g w[j]=h'[i]\bmod N$的概率是可忽略的，因此上述等式存在唯一一组解。在随机谕言机模型下，模拟算法可以随机选择1 bit的$b\in\{0,1\}$，并令$H_2(M_b\|w'[b])=h_i$，也就是说，签名结果(h_i,σ_i)对应的消息取决于模拟算法的随机谕言机输出结果。因此，攻击算法成功的优势是可忽略的。

证毕。

4　效率分析

4.1　理论分析

为了评估基于SM9协同盲签名方案的性能，将其与SM9相关签名方案（包括文献[8]方案、文献[10]方案、文献[11]方案、文献[19]方案、文献[20]方案这5种方案）的参数大小和功能进行对比，其中，文献[8]方案、文献[10]方案、文献[11]方案是盲签名方案，文献[19]方案、文献[20]方案是两方协同签名方案，对比结果如表1所示，其中，$|G_1|$、$|G_2|$及$|G_T|$分别代表SM9签名方案中群G_1、G_2及G_T的元素大小，$|N|$表示群元素阶的长度，ROM是随机谕言机模型。

表1　签名方案性能对比

Table 1　Performance comparison of signature schemes

方案	主公钥长度	签名私钥长度		签名长度	ROM	盲性	协同签名
		A	B				
文献[8]方案	$\lvert G_T\rvert+\lvert G_1\rvert+2\lvert G_2\rvert$	$\lvert G_1\rvert$	—	$\lvert N\rvert+\lvert G_1\rvert$	√	√	×
文献[10]方案	$\lvert G_T\rvert+\lvert G_1\rvert+2\lvert G_2\rvert$	$\lvert G_1\rvert$	—	$\lvert N\rvert+\lvert G_1\rvert$	√	√	×
文献[11]方案	$\lvert G_T\rvert+\lvert G_1\rvert+2\lvert G_2\rvert$	$\lvert G_1\rvert$	—	$3\lvert N\rvert+\lvert G_1\rvert$	√	√	×
文献[19]方案	$\lvert G_T\rvert+\lvert G_1\rvert+2\lvert G_2\rvert$	$\lvert G_1\rvert$	$\lvert N\rvert+\lvert G_T\rvert$	$\lvert N\rvert+\lvert G_1\rvert$	√	×	√
文献[20]方案	$\lvert G_T\rvert+\lvert G_1\rvert+2\lvert G_2\rvert$	$\lvert N\rvert$	$\lvert G_1\rvert$	$\lvert N\rvert+\lvert G_1\rvert$	√	×	√
本文方案	$\lvert G_T\rvert+\lvert G_1\rvert+2\lvert G_2\rvert$	$\lvert N\rvert$	$\lvert G_1\rvert$	$\lvert N\rvert+\lvert G_1\rvert$	√	√	√

从表1可以看出：

1)从主公钥长度来看，本文方案与对比方案均采用原始SM9数字签名算法的主公钥，因此，均没有额外增加主公钥的长度。

2)从签名私钥长度来看，由于前3个对比方案只是纯粹的盲签名方案，并不具备协同特性，因此它们只考虑单方完整的签名私钥，在对比方案中，盲签名方案的签名私钥长度仍然与原始SM9签名私钥长度保持一致，而文献[19]方案、文献[20]方案以及本文方案都具备两方协同签名的特性，因此签名私钥长度应从两方各自私钥长度来分别考虑。文献[19]方案的两方分布式SM9数字签名生成方法中签名者A的私钥长度是群G_1中元素的大小，签名者B的私钥长度是群$\mathbb{Z}_N^*$中元素的大小和群G_T中元素大小之和。文献[20]的两方协同签名方案中，签名者A的签名私钥为群$\mathbb{Z}_N^*$中的一个元素，签名者B的私钥为群G_2中的一个元素。在本文SM9两方协同盲签名方案中，签名者A的私钥为群$\mathbb{Z}_N^*$中的一个元素，签名者B的私钥为群G_1中的一个元素。因此，在3个协同签名方案中，本文方案与文献[20]方案签名者的私钥长度之和一样且最短。

3)从最终签名长度来看，除了文献[11]方案是一个部分盲签名方案，在签名中嵌入了两个长度为$|N|$的时间戳信息从而增加了签名长度之外，本文方案和其余对比方案的签名长度与原始SM9签名方案保持一致。

4)本文方案与对比方案的安全性模型均满足随机谕言机下的不可伪造性。

5)从盲性角度分析，文献[8]方案将处理过(盲化)的待签名消息传送给签名者进行签名，达到了对原始消息进行隐私保护的目的，但该方案实际上得到的签名是盲化后消息的签名并非原始消息的签名。文献[10]方案是一种有效盲化消息的签名方法，文献[11]在文献[10]的基础上提出一种部分盲签名方案，其也是一种具有盲性的签名。文献[19]方案和文献[20]方案仅是两方协同签名方案，并不满足盲性。本文方案在签名过程中添加了消息盲化因子，具有盲性。

6)从是否满足协同特性角度来看，只有文献[19]方案和文献[20]方案是目前已公开发表的具有协同特性的SM9签名方案，本文对所提SM9协同盲签名方案进行了安全性证明，本文方案被证明是一个安全的、满足协同特性的签名方案。

综上所述，相较对比方案，本文方案在尽可能不增加原始SM9签名方案参数尺寸的基础上，同时满足了不可伪造性、盲性和协同特性，在功能上更加完善。

4.2 仿真分析

本节针对所提SM9协同盲签名方案，使用Java语言应用JPBC库实现编程仿真，其中采用的椭圆曲线是Type F曲线。仿真测试环境如下：CPU为3.20 GHz AMD R7-5800H；内存为16.0 GB；操作系统为Windows 11家庭中文版。

对本文方案运行20次，计算方案中参与者的平均时间开销，测试结果如图3所示。从图3可以看出：系统建立阶段耗时200.52 ms；在密钥生成阶段，由于签名者A的签名密钥只是进行了简单的随机数选取，因此签名者A的密钥生成耗时接近0 ms，签名者B由于进行了一个点乘运算，因此签名密钥生成耗时约为16.5 ms；在协同盲签名阶段，用户U盲化消息和对盲签名进行解盲共耗时76 ms，签名方A在交互过程中执行算法共耗时169 ms，签名方B执行算法共耗时115 ms；在签名验证阶段，验证者验证签名耗时267 ms。

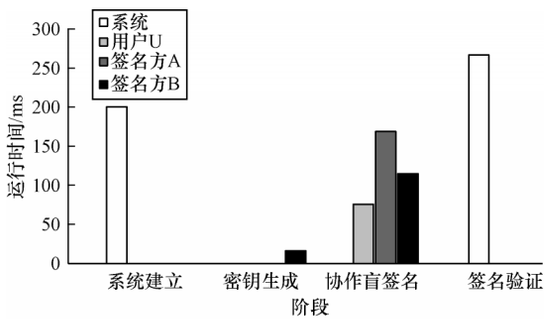

图3 方案各阶段的平均运行时间

Fig.3 Average running time of each phase of the scheme

统计本文方案整体运行时间并将其与原始SM9数字签名方案的耗时进行对比分析，结果如图4所示。从图4可以看出，本文方案对比原始SM9数字签名方案增加了187 ms的运行时间，原因是本文方案在原始SM9签名算法的基础上增加了协同特性以及消息盲化的过程，而在签名阶段增加一定的时间消耗是合理的。

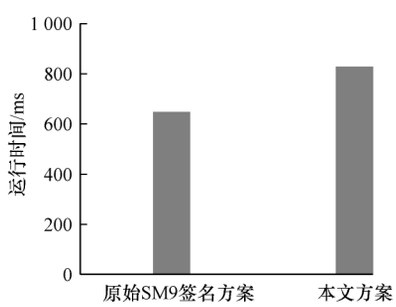

图4 2种方案整体运行时间对比

Fig.4 Comparison of overall operation time of two schemes

5 结束语

现有盲签名方案无法确保用户私钥安全，且难以解决由于签名者权力集中而导致的权力滥用问题，为此，本文提出一种基于国密SM9的协同盲签名方案。该方案允许签名私钥分散保存，增大了攻击者破译私钥时将签名私钥从移动设备导出的难度，

从而有效提高SM9盲签名系统的安全性。基于原始SM9签名的安全性分析能够保障该方案中待签消息的不可伪造性，方案的盲性也通过合理的盲化算法以及安全性高的单向哈希函数来保证。分析结果表明，与已有SM9盲签名方案相比，该方案具备协同特性，其增加的微小计算代价可忽略不计，计算效率较高，在用户隐私保护意识不断加强的大环境下，其具有良好的应用前景。但是本文方案目前仅具有两方协同的特征，下一步将研究并设计适用于多方协同场景的盲签名方案。

参考文献

[1] 中国互联网络信息中心. 第49次中国互联网络发展状况统计报告[EB/OL]. [2022-05-05]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202202/P020220311493378715650.pdf.
CNNIC. The 49th statistical report on Internet development in China[EB/OL]. [2022-05-05]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202202/P020220311493378715650.pdf. (in Chinese)

[2] 赖建昌，黄欣沂，何德彪，等. 基于商密SM9的高效标识签密[J]. 密码学报，2021，8(2)：314-329.
LAI J C，HUANG X Y，HE D B，et al. An efficient identity-based signcryption scheme based on SM9[J]. Journal of Cryptologic Research，2021，8(2)：314-329. (in Chinese)

[3] 秦宝东，张博鑫，白雪. 基于仲裁的SM9标识加密算法[J]. 计算机学报，2022，45(2)：412-426.
QIN B D，ZHANG B X，BAI X. Mediated SM9 identity-based encryption algorithm [J]. Chinese Journal of Computers，2022，45(2)：412-426. (in Chinese)

[4] 张博鑫，耿生玲，秦宝东. 高效的可撤销SM9标识签名算法[J]. 计算机应用研究，2022，39(9)：2837-2842，2849.
ZHANG B X，GENG S L，QIN B D. Efficient revocable SM9 identity-based signature algorithm[J]. Application Research of Computers，2022，39(9)：2837-2842，2849. (in Chinese)

[5] CHAUM D. Blind signatures for untraceable payments[EB/OL]. [2022-05-05]. https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

[6] 张学军. 2个改进的基于身份的代理盲签名[J]. 计算机工程，2009，35(3)：15-17.
ZHANG X J. Two improved ID-based proxy blind signatures[J]. Computer Engineering，2009，35(3)：15-17. (in Chinese)

[7] 曹素珍，戴文洁，王彩芬，等. 基于身份部分盲签名方案的分析与改进[J]. 计算机工程与科学，2018，40(12)：2193-2197.
CAO S Z，DAI W J，WANG C F，et al. Analysis and improvement of an ID-based partially blind signature scheme[J]. Computer Engineering & Science，2018，40(12)：2193-2197. (in Chinese)

[8] 王方鑫. 一种基于RSA算法的盲签名方案[J]. 电脑知识与技术，2019，15(2)：271-272.
WANG F X. Blind signature scheme based on RSA algorithm [J]. Computer Knowledge and Technology，2019，15(2)：271-272. (in Chinese)

[9] 顾兆军，刘东楠. 基于身份的Elgamal盲签名方案及其应用[J]. 计算机工程与设计，2019，40(5)：1201-1204，1209.
GU Z J，LIU D N. Identity based Elgamal blind signature scheme and its application[J]. Computer Engineering and Design，2019，40(5)：1201-1204，1209. (in Chinese)

[10] 张雪锋，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(8)：61-67.
ZHANG X F，PENG H. Blind signature scheme based on SM9 algorithm[J]. Netinfo Security，2019(8)：61-67. (in Chinese)

[11] 王倩. 基于编码的盲签名在电子投票系统中的应用[J]. 数码世界，2020(9)：5-6.
WANG Q. Application based on coded blind signature in electronic vote system [J]. Digital Space，2020(9)：5-6. (in Chinese)

[12] 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：CN108551392B[P]. 2021-07-06.
HE D B，ZHANG Y D，ZHANG Y B，et al. Blind signature generation method and system based on SM9 digital signature：CN108551392B[P]. 2021-07-06. (in Chinese)

[13] 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.
LÜ Y，HOU J P，NIE C，et al. Partial blind signature scheme based on SM9 algorithm[J]. Chinese Journal of Network and Information Security，2021，7(4)：147-153. (in Chinese)

[14] 陈丽燕. Hash-RSA盲签名的数字货币方案[J]. 计算机时代，2021(6)：52-56.
CHEN L Y. Digital currency scheme with Hash-RSA blind signature[J]. Computer Era，2021(6)：52-56. (in Chinese)

[15] 姜昊堃，董学东，张成. 改进的具有前向安全性的无证书代理盲签名方案[J]. 计算机科学，2021，48(S1)：529-532.
JIANG H K，DONG X D，ZHANG C. Improved certificateless proxy blind signature scheme with forward security[J]. Computer Science，2021，48(S1)：529-532. (in Chinese)

[16] 唐卫中，张大伟，佟晖. 基于SM2的无证书盲签名方案[J]. 计算机应用研究，2022，39(2)：552-556.
TANG W Z，ZHANG D W，TONG H. Certificateless blind signature scheme based on SM2[J]. Application Research of Computers，2022，39(2)：552-556. (in Chinese)

[17] 符朕皓，林定康，姜皓晨，等. 大零币匿名技术及追踪技术综述[J]. 计算机科学，2021，48(11)：62-71.
FU Z H，LIN D K，JIANG H C，et al. Survey of anonymous and tracking technology in zerocash[J]. Computer Science，2021，48(11)：62-71. (in Chinese)

[18] JI Y P，SHEN C F，WANG Y B，et al. Design and implementation of SM9 digital signature algorithm [C]// Proceedings of the 15rd National Signal and Intelligent Information Processing and Application Academic Conference. Washington D. C.，USA：IEEE Press，2022：47-54.

[19] 何德彪，张语荻. 一种两方分布式SM9数字签名生成方法与系统：CN107566128A[P]. 2018-01-09.
HE D B，ZHANG Y D. A two-party distributed SM9 digital signature generation method and system：CN107566128A[P]. 2018-01-09. (in Chinese)

[20] MU Y H，XU H X，LI P L，et al. Secure two-party SM9 signing[J]. Science China Information Sciences，2020，63(8)：1-3.

（下转第161页）

convolutional layer[C]//Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. New York, USA: ACM Press, 2016: 5-10.
[8] HU X, ZHANG Z, JIANG Z, et al. SPAN: spatial pyramid attention network for image manipulation localization[C]// Proceedings of European Conference on Computer Vision. Berlin, Germany: Springer, 2020: 312-328.
[9] ZHOU P, HAN X T, MORARIU V I, et al. Learning rich features for image manipulation detection[C]//Proceedings of IEEE/CVF Conference on Computer Vision and Pattern Recognition. Washington D. C., USA: IEEE Press, 2018: 1053-1061.
[10] SALLOUM R, REN Y Z. Image splicing localization using a Multi-task Fully Convolutional Network (MFCN)[J]. Journal of Visual Communication and Image Representation, 2018, 51: 201-209.
[11] ZHOU P, CHEN B C, HAN X T, et al. Generate, segment, and refine: towards generic manipulation segmentation[C]// Proceedings of AAAI Conference on Artificial Intelligence. Palo Alto, USA: AAAI Press, 2020: 13058-13065.
[12] KWON M J, YU I J, NAM S H, et al. CAT-net: compression artifact tracing network for detection and localization of image splicing[C]//Proceedings of IEEE Winter Conference on Applications of Computer Vision. Washington D. C., USA: IEEE Press, 2021: 375-384.
[13] 路东生，张玉金，党良慧. 面向图像篡改取证的多特征融合U形深度网络[J]. 计算机工程，2022，48(4)：213-222.
LU D S, ZHANG Y J, DANG L H. Multi-feature fusion U-structure deep network for image tempering forensics[J]. Computer Engineering, 2022, 48(4): 213-222. (in Chinese)
[14] WANG J K, WU Z X, CHEN J J, et al. ObjectFormer for image manipulation detection and localization [C]// Proceedings of IEEE/CVF Conference on Computer Vision and Pattern Recognition. Washington D. C., USA: IEEE Press, 2022: 2354-2363.
[15] YIN Q, WANG J, LU W, et al. Contrastive learning based multi-task network for image manipulation detection[J]. Signal Processing, 2022, 201: 108709.
[16] 刘丽颖，王金鑫，曹少丽，等. 检测小篡改区域的U型网络[J]. 中国图象图形学报，2022，27(1)：176-187.
LIU L Y, WANG J X, CAO S L, et al. U-Net for detecting small forgery region[J]. Journal of Image and Graphics, 2022, 27(1): 176-187. (in Chinese)
[17] 朱叶，余宜林，郭迎春. HRDA-Net：面向真实场景的图像多篡改检测与定位算法[J]. 通信学报，2022，43(1)：217-226.
ZHU Y, YU Y L, GUO Y C. HRDA-Net: image multiple manipulation detection and location algorithm in real scene[J]. Journal on Communications, 2022, 43(1): 217-226. (in Chinese)
[18] DONG C B, CHEN X R, HU R H, et al. MVSS-Net: multi-view multi-scale supervised networks for image manipulation detection[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 4(3): 3539-3553.
[19] LIU X H, LIU Y J, CHEN J, et al. PSCC-Net: progressive spatio-channel correlation network for image manipulation detection and localization [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(11): 7505-7517.
[20] 朱昊昱，孙俊，陈祺东. 基于DeepLab v3+的多任务图像拼接篡改检测算法[J]. 计算机工程，2022，48(1)：253-259.
ZHU H Y, SUN J, CHEN Q D. Multi-task algorithm for image splicing forgery detection based on DeepLab v3+[J]. Computer Engineering, 2022, 48(1): 253-259. (in Chinese)
[21] WEI Q J, LI X R, YU W H, et al. Learn to segment retinal lesions and beyond [C]//Proceedings of the 25th International Conference on Pattern Recognition. Washington D. C., USA: IEEE Press, 2021: 7403-7410.
[22] DONG J, WANG W, TAN T N. CASIA image tampering detection evaluation database[C]//Proceedings of IEEE China Summit and International Conference on Signal and Information Processing. Washington D. C., USA: IEEE Press, 2013: 422-426.
[23] WEN B H, ZHU Y, SUBRAMANIAN R, et al. COVERAGE—a novel database for copy-move forgery detection[C]//Proceedings of IEEE International Conference on Image Processing. Washington D. C., USA: IEEE Press, 2016: 161-165.
[24] GUAN H Y, KOZAK M, ROBERTSON E, et al. MFC datasets: large-scale benchmark datasets for media forensic challenge evaluation [C]//Proceedings of IEEE Winter Applications of Computer Vision Workshops. Washington D. C., USA: IEEE Press, 2019: 63-72.
[25] HSU J, CHANG S F. Columbia uncompressed image splicing detection evaluation dataset[EB/OL]. [2022-07-12]. https://www.ee.columbia.edu/ln/dvmm/downloads/authsplcuncmp/.

编辑　陆燕菲

(上接第153页)

[21] MISHRA S, YADUVANSHI R, RAI A K, et al. An ID-based signature scheme from bilinear pairing based on ex-K-plus problem[J]. Advanced Materials Research, 2011, 403: 929-934.
[22] BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups [EB/OL]. [2022-05-05]. https://eprints.qut.edu.au/69199/2/Boyen_accepted_draft.pdf.
[23] 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 Z H. Overview on SM9 identity-based cryptographic algorithm [J]. Journal of Information Security Research, 2016, 2(11): 1008-1027. (in Chinese)
[24] CHAUM D L. Blind signature systems: EP, US4759063 (A)[P]. 1988-07-19.
[25] 彭聪，何德彪，罗敏，等. 基于SM9标识密码算法的环签名方案[J]. 密码学报，2021，8(4)：724-734.
PENG C, HE D B, LUO M, et al. An identity-based ring signature scheme for SM9 algorithm [J]. Journal of Cryptologic Research, 2021, 8(4): 724-734. (in Chinese)
[26] 赖建昌，黄欣沂，何德彪，等. 国密SM9数字签名和密钥封装算法的安全性分析[J]. 中国科学：信息科学，2021，51(11)：1900-1913.
LAI J C, HUANG X Y, HE D B, et al. Security analysis of SM9 digital signature and key encapsulation[J]. Scientia Sinica (Informationis), 2021, 51(11): 1900-1913. (in Chinese)

编辑　吴云芳