

基于SM9的广播多重签名

陶金玲

(南京邮电大学 计算机学院, 江苏 南京 210023)

摘要: 广播多重签名是多个用户在同一时间对文件进行签名和认证。在传统的公钥密码系统中, 证书颁发机构(CA)需要生成并签署用户身份与其公钥绑定在一起的数字证书。然而, 公钥证书操作和存储会给CA带来沉重的证书管理负担, 而通过用户身份派生公钥能使方案在应用部署时的密钥管理操作得到简化。SM9标识密码算法作为我国自主设计的商用密码标准, 已由ISO/IEC标准化并被广泛使用且基于身份密码体制。为了结合身份基密码体制与多重签名的优势, 推动我国自主研发的密码体制发展, 提出一种基于SM9的广播多重签名方案。首先, 在签名聚合前验证了所有部分签名的有效性; 其次, 在签名聚合后对整体签名结果进行验证; 最后, 对该方案进行安全性证明与仿真实验。实验表明, 所提方案相较于传统公钥密码与国外密码体制下的方案, 在签名人数增加时仍具有较高的效率。

关键词: 广播多重签名; SM9标识密码算法; 证书管理; 身份基密码体制; 随机预言模型

DOI: 10.11907/rjtk.241202

开放科学(资源服务)标识码(OSID):

中图分类号: TP309

文献标识码: A

文章编号: 1672-7800(2025)004-0130-06



Broadcast Multi-Signature Based on SM9

TAO Jinling

(School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Broadcast multi signature refers to multiple users signing and authenticating a file at the same time. In traditional public key cryptography systems, certificate authorities (CAs) need to generate and sign digital certificates that bind user identities to their public keys. However, the operation and storage of public key certificates can impose a heavy certificate management burden on CAs, while deriving public keys through user identities can simplify key management operations during application deployment. The SM9 identification password algorithm, as a commercial password standard independently designed by China, has been standardized by ISO/IEC and widely used based on identity system. In order to combine the advantages of identity based cryptography and multi signature, and promote the development of independently developed cryptography in China, a broadcast multi signature scheme based on SM9 is proposed. Firstly, the validity of all partial signatures was verified before signature aggregation; Secondly, the overall signature result is verified after signature aggregation; Finally, the security of the scheme is demonstrated and simulated through experiments. The experiment shows that the proposed scheme still has high efficiency compared to traditional public key cryptography and schemes under foreign cryptographic systems, even when the number of signatures increases.

Key Words: broadcast multi-signatures; SM9 identification cryptography algorithm; certificate management; identity-based cryptography; random oracle model

0 引言

近年来,随着云计算技术和5G通信的迅猛发展,多重签名技术在各领域都有了更广泛的应用。在云计算环境下,多重签名在访问、共享云存储中的数据时需要多方确认,有助于提升数据安全性和隐私保护。目前实际应用

中,云中的多方协作平台(文档编辑、项目管理等)可使用多重签名来确保重要操作的合法性,例如文件修改、项目资金调配等。在5G通信环境下,支持区块链和智能合约的应用更普及,多重签名可确保执行智能合约时需要多方共同授权,即在实际应用中许多签署人需要签署一份文件^[1,2]。例如,一个重要合同需要同时由财务、营销和仓库经理批准和签署,再由客户验证。此外,多重签名认证可

收稿日期: 2024-03-05

扫描二维码阅读全文:

作者简介: 陶金玲(2000-),男,南京邮电大学计算机学院硕士研究生,研究方向为密码学与信息安全。



用于智慧电子医疗信息系统、物联网、智能电网系统和电子合同等^[3-6]。Itakura等^[7]首次提出多重签名的概念,指多个签名人合作产生同一个消息的签名,签名验证人可验证这些签名人是否参与了对该消息的签名。

根据签名过程是否需要一定的顺序,多重签名可分为有序多重签名和广播多重签名。张亚玲等^[8]对文献^[9]的方案进行了改进,提出一个基于身份和RSA的多重签名方案。在方案中增添了一个签名收集者,减少了签名者之间的交互过程,签名验证过程的效率也得到了提升。由于基于身份的多重签名具有通信效率高、简化密钥管理等特点,所以该方向的学者不断增多^[10-13]。Park等^[14]提出一种安全严密的多重签名方案,减少了文献^[9]在签名验证阶段的双线性对计算,但涉及较多双线性对计算,签名效率较低,并未给出严格的形式化安全性证明。Boneh等^[15]引入BLS签名替换Schnorr签名,提出一个基于配对的多重签名方案。Galindo等^[16]使用子分组参与多重签名的生成,以提升多重签名的安全性,但并非身份基签名方案,需要较大的密钥管理开销。Lai等^[17]基于SM9签名方案提出一个可证安全的在线/离线签名方案,但并未实现多重签名,在多参与者签名条件下并不适用。Liu等^[18]提出一种基于Schnorr方案的身份基多重签名,虽有效解决了多用户情景下的签名开销问题,但并非基于我国自主研发的密码体制为基础。

目前,绝大多数多重签名方案设计都以国外密码体制为基础,对以国家商用密码算法(SM2、SM9等)为基础的多重签名方案研究甚少。近年来,我国积极推动相关商用密码的研究,颁布了GM/T 0044-2016《SM9标识密码算法》密码行业标准^[19]。SM9是中国商用标识密码标准,包含数字签名、加密、密钥交换和密钥封装,SM9标识签名算法已被采纳为国际标准ISO/IEC的一部分,并于2020年成为中国国家标准GM/T 38 635.2—2020^[20,21]。

SM9密码算法的密钥长度为256 bit,采用R-ate双线性对,具备快速运算和高安全性能,应用嵌入度为12的椭圆曲线,旨在提升安全性和计算效率。SM9算法采用两个安全参数较小的非对称双线性对,相较于一般多重签名方案使用安全参数较大的对称双线性对的常规方法存在不同之处。国内学者在SM9算法的扩展应用方面已取得了一些研究进展,包括SM9盲签名、标识签密、SM9无证书签名、属性基签名等^[22-25]。虽然,这些研究成果促进了SM9的发展,但并未形成一个在多用户环境下SM9签名的有效多重签名方案。

本文贡献为:①构造了一个基于SM9的广播多重签名方案,相较于SM9标识密码算法标准中的单个数字签名而言,满足了其在需要多方参与和认证的业务场景中的需求;②算法结合基于身份的签名(Identity-Based Signature, IBS)与多重签名的优势,并以SM9标识密码为基础,致力于推动我国自主研发的密码体制发展,进一步完善了我国

密码体制。

1 基础知识

1.1 双线性映射

设 λ 为安全参数, G_1 、 G_2 为两个阶为 N 的循环加法群, G_T 为阶为 N 的循环乘法群,如果存在一个双线性映射 $e: G_1 \times G_2 \rightarrow G_T$ 满足以下性质,则称 (G_1, G_2, G_T) 为双线性映射群:

(1) 双线性。对于任意元素 $S \in G_1, Q \in G_2$, 整数 $a, b \in \mathbb{Z}_N^*$, 都有 $e(aS, bT) = e(S, T)^{ab}$ 。

(2) 非退化性。存在元素 $P \in G_1, Q \in G_2$, 满足 $e(P, Q) \neq 1$ 。

(3) 可计算性。 $\forall (S, T) \in G_1 \times G_2, e(S, T)$ 是容易计算的。

设 P, Q 分别为双线性群 G_1, G_2 上的生成元,那么在第二类双线性群中(非对称双线性群),存在着一种有效且公开的可计算同构映射 $\psi: G_2 \rightarrow G_1$,使得 $\psi(Q) = P$ 。

1.2 困难问题假设

定义 1 q -SDH 问题(q -Strong Diffie-Hellman Problem)

令 $P \in G_1, Q \in G_2$, 对未知的正整数 $a \in \mathbb{Z}_N^*$, 给定 $q+2$ 个元素 $(P, Q, aQ, a^2Q, \dots, a^qQ)$ 来找到一个二元组 $(c, \frac{1}{c+a}P)$ 是困难的。

2 方案定义与安全模型

本文基于SM9的广播多重签名方案,包含数据拥有者、密钥生成中心(Key Generation Center, KGC)、 n 个签名者 $N_i (i = 1, 2, \dots, n)$ 、签名收集者和签名验证者等主体,如图1所示。首先,数据拥有者发布签名消息 M ,签名者与密钥生成中心交互生成签名密钥;其次,签名者与签名收集者交互完成个体签名,并将个体签名发送给签名收集者;再次,签名收集者验证个体签名,若所有个体通过则计算输出多重签名给签名验证者;最后,签名验证者进行多重签名验证并返回验证结果^[26]。

2.1 方案定义

(1) 系统建立算法(Setup)。由KGC输入安全参数 λ ,

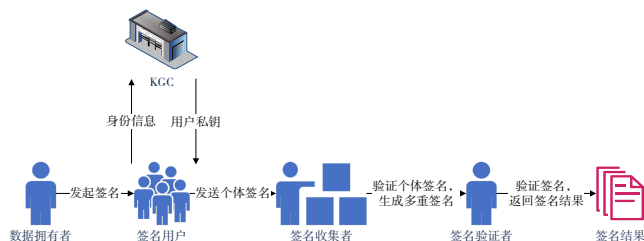


Fig. 1 Protocol workflow

图1 方案工作流程

输出主密钥 s 、主公钥 P_{pub} 及公共参数 $Params$ 。

(2)密钥生成算法(*KeyGen*)。首先输入签名用户身份 ID_i , KGC根据系统公共参数和主密钥为签名用户生成签名密钥,其次通过安全信道将用户签名密钥发送给签名用户。

(3)签名产生算法(*Multi-Sign*)。输入消息 m 、签名者 N_i 、签名密钥 d_i 和系统参数 $Params$,输出个体签名 S_i 并将 S_i 发送给签名收集者。签名收集者将先验证签名者的个体签名,当所有个体签名验证通过后进行聚合以输出多重签名。

(4)签名验证算法(*Multi-Verify*)。签名验证者在接收到签名收集者发送的多重签名后,验证多重签名是否有效。

2.2 安全模型

定义2 不可伪造性

假设在参与生成多重签名的 n 个签名者中,只有一个诚实签名者,其他 $n-1$ 个签名者已被敌手攻破,意味着敌手知道 $n-1$ 个签名者的签名密钥,可伪造出他们的签名,攻击者的目标是塑造一个有效的多重签名,陷害这个诚实的签名者^[27]。

敌手 A 与挑战者 C 之间的交互过程为:

(1)初始化。挑战者 C 执行系统建立算法,获取系统安全参数 λ 、主密钥 a ,并将主公钥和系统公共参数发送给敌手 A 。

(2)敌手 A 与挑战者 C 的交互。敌手 A 自适应地向挑战者 C 发出请求,挑战者 C 返回对应的响应给敌手 A 。敌手 A 的请求和挑战者 C 对应的响应过程为:① H_1 询问:敌手 A 向挑战者 C 发出身份为 ID_i 的签名者 N_i 的 H_1 查询,挑战者 C 收到请求后生成相应值,作为响应返回给敌手 A ;② H_2 询问:敌手 A 向挑战者 C 发出消息 m 和 n 个签名者的承诺 $w_1, w_2, \dots, w_n$ 的 H_2 查询,第 i 个承诺为 w_i ,挑战者 C 收到请求后生成相应值返回给敌手 A ;③签名密钥询问:敌手 A 向挑战者 C 发出身份为 ID_i 的签名者 N_i 的签名密钥查询,除了身份为 ID_* 的诚实签名者在签名密钥时,挑战者 C 返回相应的签名密钥给敌手 A 。④签名询问:首先敌手 A 发送 $n-1$ 个签名者的承诺 w_i 给挑战者 C ,其次挑战者 C 对于诚实签名者选取随机数 $r_* \in \mathbb{Z}_N^*$,计算 $w_* = g^{r_*}$,返回诚实签名者的承诺 w_* 给敌手 A ,再次敌手 A 进行哈希查询生成 $n-1$ 个签名者的部分签名及签名消息 m 给挑战者 C ,最后挑战者 C 返回一个包含诚实签名者签名的有效多重签名。

(3)伪造阶段。在上述过程结束后,敌手 A 输出消息 m^* 和身份为 $ID_1, ID_2, \dots, ID_n$ 签名组的多重签名,包含用户身份为 ID_* 的诚实签名者。在没有对诚实签名者进行签名密钥询问和对消息 m^* 进行签名询问的情况下,如果敌手 A 成功伪造出一个合法的多重签名则敌手 A 获胜,否则敌手 A 失败,则代表其无法伪造合法的多重签名。

3 算法流程

本文提出一个基于SM9的广播多重签名方案,包括系统建立算法*Setup*、密钥生成算法*KeyGen*、多重签名生成算法*Multi-Sign*和多重签名验证算法*Multi-Verify*。

(1)*Setup*。 G_1, G_2, G_T 分别为阶数为素数 N 的两个循环加法群和一个循环乘法群,双线性映射 $e: G_1 \times G_2 \rightarrow G_T$ 。 P_1, P_2 分别为 G_1, G_2 的生成元,则存在 $P_1 = \psi(P_2)$ 。KGC选取一个随机数 $s \in [1, N-1]$ 作为系统主密钥,计算系统主公钥 $P_{pub} = sP_2$ 。首先,选择两个密码杂凑函数 $H_1: \{0, 1\}^* \rightarrow \mathbb{Z}_N^*, H_2: \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$;其次,计算群 G_T 上的元素 $g = e(P_1, P_{pub})$;最后,公开系统公共参数 $Params: (G_1, G_2, G_T, e, P_1, P_2, g, H_1, H_2)$ 。

(2)*KeyGen*。密钥生成算法由KGC为签名者生成签名密钥。首先,KGC根据身份为 ID_i 的签名者 N_i 计算 $t_1 = H_1(ID_i) + s, t_2 = t_1^{-1}s$;其次,计算签名者 N_i 的签名密钥 $d_i = t_2P_1$ 。

(3)*Multi-Sign*。数据拥有者发布签名消息 m 与签名者信息 $L = \{N_1, N_2, \dots, N_n\}$,签名者与签名收集者进行如下交互:

Round1. 每个签名者 $N_i \in L$:

- 选取一个随机数 $r_i \in \mathbb{Z}_q^*$;
- 计算个人的承诺 $w_i = g^{r_i}$;
- 发送 w_i 给签名收集者;

Round2. 签名收集者:

- 接收来自所有签名者的 w_i 之后,计算 $w = \prod_{i=1}^n w_i$;
- 计算 $h = H_2(m \| w)$;
- 广播 h 给每一个签名者;

Round3. 每个签名者 $N_i \in L$:

- 接收来自签名收集者的 h ;
- 计算 $h_i = H_2(w_i \| h)$;
- 计算 $S_i = (r_i - h_i)d_i$;
- 输出个体签名 (S_i, h_i) ;

当签名收集者接收到所有签名者的个体签名后,验证每个签名者的个体签名。首先,计算 $w'_i = e(S_i, H_1(ID_i)P_2 + P_{pub}) \cdot g^{h_i}$;其次,验证 $h'_i = H_2(w'_i \| h) = h_i$ 是否成立。当所有签名者的个体签名被签名验证者验证通过后,签名收集者将收集的个体签名进行聚合计算(见式(1));最后,签名收集者将生成的多重签名 (σ, U, Q, h) 通过安全信道发送给签名验证者。

$$\sigma = \sum_{i=1}^n S_i, U = \sum_{i=1}^n H_1(ID_i) \cdot S_i, Q = g^{\sum_{i=1}^n h_i} \quad (1)$$

(4)*Multi-Verify*。签名验证算法由签名验证者执行,在接收到签名收集者发来的多重签名 (σ, U, Q, h) 后,先计算 $w' = e(\sigma, P_{pub})e(U, P_2) \cdot Q$,再计算 $h' = H_2(m \| w')$,最后验证 $h = h'$ 是否成立。若等式成立则输出为真,表示多重

签名通过;否则输出为假,表示多重签名验证不通过。

本文给出上述多重签名方案的正确性证明:

如果签名者 $N_i \in L$ 发送给签名收集者的个体签名能通过签名收集者的验证,则输出正确的多重签名,代表多重签名验证通过。

单个签名验证的正确性验证方法为:

$$\begin{aligned}
 w_i' &= e(S_i, H_1(ID_i)P_2 + P_{pub}) \cdot g^{h_i} \\
 &= e((r_i - h_i)d_i, t_1P_2) \cdot e(P_1, P_{pub})^{h_i} \\
 &= e((r_i - h_i)t_2P_1, t_1P_2) \cdot e(P_1, P_{pub})^{h_i} \\
 &= e((r_i - h_i)P_1, sP_2) \cdot e(P_1, P_{pub})^{h_i} \\
 &= e((r_i - h_i)P_1, P_{pub}) \cdot e(P_1, P_{pub})^{h_i} \\
 &= e(P_1, P_{pub})^{r_i} \\
 &= g^{r_i}
 \end{aligned} \quad (2)$$

满足验证等式 $h_i = h_i' = H_2(w_i' || h)$ 。

多重签名验证的正确性验证方法为:

$$\begin{aligned}
 w_i' &= e(\sigma, P_{pub})e(U, P_2) \cdot Q \\
 &= e(\sum_{i=1}^n S_i, P_{pub})e(\sum_{i=1}^n U_i, P_2)g^{\sum_{i=1}^n h_i} \\
 &= \prod_{i=1}^n e(S_i, P_{pub})e(U_i, P_2)g^{h_i} \\
 &= \prod_{i=1}^n e(S_i, P_{pub})e(H_1(ID_i)S_i, P_2)g^{h_i} \\
 &= \prod_{i=1}^n e(S_i, H_1(ID_i)P_2 + P_{pub})g^{h_i} \\
 &= \prod_{i=1}^n e((r_i - h_i)d_i, H_1(ID_i)P_2 + P_{pub})g^{h_i} \\
 &= \prod_{i=1}^n e((r_i - h_i)P_1, P_{pub})g^{h_i} \\
 &= \prod_{i=1}^n g^{r_i} \\
 &= w'
 \end{aligned} \quad (3)$$

满足验证等式 $h = h' = H_2(m || w')$ 。

4 安全性分析

在随机预言模型下,假设存在一个敌手 A 在适应性选择消息攻击下,在多项式时间内发起 q_{H_1} 次哈希询问、 q_e 次签名密钥询问和 q_s 次签名询问后,可在时间 t 内以概率 ε 成功伪造签名,即存在一个多项式时间概率算法模拟挑战者 C 与敌手 A 之间的交互过程,在多项式时间 t' 内以 ε' 的概率解决 q -SDH 问题,如式(4)所示。

$$(1 - \frac{1}{q_e + 1})^{q_e} \frac{1}{q_s + 1} \varepsilon \geq \varepsilon', t = t' + O(q_{H_1} + 2q_{H_2} + q_e + 2q_s) \quad (4)$$

证明过程为:本文方案包含 n 个用户 $N_i (1 \leq i \leq n)$,假设除用户 N_* 外,其余 $n - 1$ 个用户都被敌手 A 攻破,挑战者 C 的目标是找到一个二元组 $(c, \frac{1}{c+a}P)$ 。那么,挑战者 C 与敌手 A 的交互为:

(1)初始化。挑战者 C 运行系统建立算法获取系统安全参数 λ 、系统主密钥 a ,执行以下步骤生成系统主公钥:
①随机选择 $i^* \in [1, q]$,从 Z_N^* 中随机选取 q 个两两不同的数 $x^*, x_1, x_2, \dots, x_{i^*-1}, x_{i^*+1}, \dots, x_q$,并定义多项式(见式(5));

②计算群 G_2 的生成元: $P_2 = \sum_{i=0}^{q-1} c_i(a^i Q) = f(a)Q$,计算群 G_1 的生成元 $P_1 = \psi(P_2) = f(a)P \in G_1$;③根据生成元 P_2 计算系统主公钥 $P_{pub} = \sum_{i=0}^{q-1} c_i(a^{i+1} Q) = aP_2 \in G_2$,计算群 G_T 的元素 $g = e(P_1, P_{pub})$, $\psi(Q) = P$,并对任意 $i \in [1, q] \setminus i^*$,定义 $f_i(z) = \frac{f(z)}{z + x_i} = \sum_{i=0}^{q-2} d_i z^i$,以计算 $\sum_{i=0}^{q-2} d_i(a^{i+1} Q) = \frac{af(a)}{a + x_i} P = \frac{a}{a + x_i} P_1$,由此可知二元组 $(x_i, \frac{a}{a + x_i} P_1)$ 十分容易计算;④将系统主公钥 $P_{pub} = aP_2$ 与其他公共参数 $Params: (G_1, G_2, G_T, e, P_1, P_2, g, H_1, H_2)$ 发送给敌手 A , c_i 为多项式 $f(z)$ 的系数

$$f(z) = \prod_{i=1, i \neq i^*}^q (z + x_i) = \sum_{i=0}^{q-1} c_i z^i \mod N \quad (5)$$

(2)敌手 A 和挑战者 C 的交互。敌手 A 自适应地向挑战者 C 发出请求,挑战者 C 返回对应的响应给敌手 A 。其中,敌手 A 的请求和挑战者 C 响应过程为:① H_1 询问:挑战者 C 创建 $H_1 - List$ 列表保存元组 $(ID_i, k_i, H(ID_i))$,对每一个身份为 $(ID_i (ID_i \neq ID_*))$ 的签名者,如果 $H_1 - List$ 中没有存在关于 ID_i 的记录,则挑战者 C 随机选择一个 $k_i \in Z_q^*$ 作为 ID_i 的哈希值返回,并将元组 $(ID_i, k_i, H(ID_i))$ 记录在 $H_1 - List$ 中,若已存在此元组记录则挑战者 C 直接返回相应值,若敌手 A 询问诚实者 ID_* 的哈希值,则挑战者 C 选取一个随机数 $c \in Z_q^*$ 作为 ID_* 的哈希值返回给敌手 A ;② H_2 询问:挑战者 C 创建 $H_2 - List$ 列表保存元组 $(w_1, w_2, \dots, w_n, h_1, h_2, \dots, h_n, h)$,在接收到敌手 A 对 $w_1, w_2, \dots, w_n$ 元素和消息 m 进行哈希询问时,如果 n 个元素 $w_1, w_2, \dots, w_n$ 在表中没有记录,挑战者 C 选取 $h = v \in_R Z_N^*$ 、 $h_i = v_i \in_R Z_N^*$ 作为 $w = \prod_{i=1}^n w_i$ 和相应 w_i 的哈希值返回给敌手 A ,若表中存在相应记录则直接返回;③签名密钥询问:挑战者 C 创建一个 $E - List$ 列表模拟签名密钥询问,如果 $ID_i = ID_*$ 则终止游戏,否则挑战者 C 在 $E - List$ 列表查找相应记录并返回,如果表中没有相关记录则先对用户身份 ID_i 进行 H_1 询问,再使用 H_1 询问的值 $k_i \in Z_q^*$ 计算用户 ID_i 的签名密钥 $d_i = \frac{a}{k_i + a} P_1$,若表中存在相应记录则直接返回;④签名询问:对于消息 m 和签名组 $ID_1, ID_2, \dots, ID_n$ 的签名询问,敌手 A 发送 $n - 1$ 个签名者的 w_i 和诚实签名者的身份 ID_* 给挑战者 C ,挑战者 C 选取一个随机数 r_* ,计算 $w_* = g^{r_*}$ 、 $w = \prod_{i=1}^{n-1} w_i \cdot w_*$ 并返回给敌手 A ,敌手 A 通过相应的哈希询问及签名密钥询问,利用真实签名算法计算 $n - 1$ 个签名者的部分签名及签名消息 m 以发送给挑战者 C ,挑战者 C 再根据签名算法返回关于消息 m 的多重签名 (σ, U, Q, h) ,具体计算过程如式(6)一式(9)所示。

$$S_{i_*} = (r_{i_*} - h_{i_*})d_{i_*} \quad (6)$$

$$\sigma = \sum_{i=1, i \neq i_*}^n S_i + S_{i_*} \quad (7)$$

$$U = \sum_{i=1, i \neq i_*}^n k_i \cdot S_i + c \cdot S_{i_*} \quad (8)$$

$$Q = g^{\sum_{i=1, i \neq i_*}^n h_{i_*}} \cdot g^{h_{i_*}} \quad (9)$$

(4) 伪造阶段。上述过程结束后敌手 A 输出一个关于消息 m^* 与用户签名组 $ID_1, ID_2, \dots, ID_n$ 的多重签名 (σ_*, U_*, Q_*, h) , 包含身份为 ID_* 的诚实签名者。在没有对 ID_* 进行签名密钥询问和对消息 m^* 进行签名询问的情况下, 如果敌手 A 伪造的多重签名通过, 那么挑战者 C 就可查询到相应列表, 计算诚实签名者 ID_* 的部分签名信息 (S_{i_*}, h_{i_*}, w_*) 可通过签名验证, $S_{i_*} = \sigma_* - \sum_{i=1, i \neq i_*}^n S_i$, 即 $e(S_{i_*}, H(ID_*) \cdot P_2 + P_{pub}) \cdot g^{h_{i_*}} = e(S_{i_*}, (c + a)P_2) \cdot g^{h_{i_*}} = w_*$ 。

根据分叉引理, 挑战者 C 可通过敌手 A 获得另一个关于消息 m^* 和诚实签名者 ID_* 签名消息的签名信息 $(S'_{i_*}, h'_{i_*}, w_*)^{[28]}$ 。

$$\begin{aligned} & e(S_{i_*}, H(ID_*)P_2 + P_{pub}) \cdot e(P_1, P_{pub})^{h_{i_*}} \\ &= e(S'_{i_*}, H(ID_*)P_2 + P_{pub}) \cdot e(P_1, P_{pub})^{h'_{i_*}} \end{aligned} \quad (10)$$

式中: $S_{i_*} \neq S'_{i_*}, h_{i_*} \neq h'_{i_*}$ 。

将 $H(ID_*) = c, P_{pub} = aP_2$ 带入式 (10) 可得 $\frac{a}{a+c}P_1 = \frac{S_{i_*} - S'_{i_*}}{h'_{i_*} - h_{i_*}}$, 令 $Y^* = \frac{S_{i_*} - S'_{i_*}}{h'_{i_*} - h_{i_*}}$ 可得 $Y^* = \frac{a}{a+c}P_1$ 。又因为 $\frac{zf(z)}{z+c} = \frac{\gamma}{z+c} + \sum_{i=0}^{k-1} \gamma_i z^i, P_1 = f(a)P, \gamma, \gamma_i$ 为可求的系数且 $\gamma \neq 0$, 最终计算出 $X^* = \frac{1}{\gamma} (Y^* - \sum_{i=0}^{k-1} \gamma_i \psi(a^i Q)) = \frac{1}{c+a}P$, 即输出 $(c, \frac{1}{c+a}P)$ 为 q -SDH 困难问题实例的解, 这与定义 1 矛盾, 根据反证法可知本文方案满足定义 2。

由此可知, 挑战者 C 在通过敌手 A 的能力解决 q -SDH 困难问题时, 当且仅当没有对 ID_* 进行签名密钥询问和对消息 m^* 进行签名询问的情况下能成功伪造签名, 即 q -SDH 困难问题能被解决的概率 ε' 满足 $(1 - \frac{1}{q_e + 1})^{q_e} \frac{1}{q_s + 1} \varepsilon \geq \varepsilon'$, 上述敌手 A 与挑战者 C 交互的时间为 $t' + O(q_{H_1} + 2q_{H_2} + q_e + 2q_s)$ 。

此外, 如果签名者与签名收集者内部合谋伪造一个其他消息 m' 的签名, 那么签名验证者在验证签名时, 签名验证者会验证等式 $h' = H_2(m' || w) = H_2(m || w)$ 是否成立。此时, 哈希函数的单向性可使验证不通过, 以有效防止签名者内部合谋攻击。

5 性能分析

5.1 计算代价分析

本文对各方案中签名各阶段的计算量进行分析, 给出了方案总体开销, 如表 1 所示。其中, BP 表示群上双线性配对运算, SM 表示群上标量点乘运算。本文所提方案在多重签名阶段时, 即生成多重签名前, 每个签名者需计算 1 次双线性配对和 3 次标量点乘运算, 因此 n 名签名者在签

名计算阶段共需要 n 次双线性配对计算和 $3n$ 次双线性配对计算, 在多重签名验证阶段只需 2 次双线性配对计算验证签名结果。

本文方案在整个过程中使用 $n + 2$ 次双线性配对, $3n$ 次群上标量点乘运算, 相较于文献 [14] 在签名计算量上虽增加了 n 次标量点乘运算, 但整体上减少 $n+2$ 次双线性配对计算; 相较于文献 [16] 在签名计算上减少 $3n$ 次双线性配对计算, 但由于双线性的运算开销远大于标量点乘运算, 因此本文方案更高效。此外, 本文方案基于身份的密码体制, 减轻了复杂的公钥证书管理负担。

Table 1 Efficiency comparison of various schemes (n signed users)

表 1 各方案效率比较 (n 个签名用户)

方案	签名计算量	验证计算量	总开销	是否基于身份
文献 [14]	$2nBP+2nSM$	$3BP$	$(2n+3)BP+2nSM$	否
文献 [16]	$4nBP+3nSM$	$2BP$	$(4n+2)BP+3nSM$	否
本文方案	$nBP+3nSM$	$2BP$	$(n+2)BP+3nSM$	是

5.2 仿真结果与分析

本文利用 JPBC 密码库对所提方案进行实现, 由于文献 [14]、文献 [16] 和本文方案均建立在非对称群上, 根据国家 SM9 密码算法参数规范, 使用的曲线为嵌入度为 12, 阶为 256 bit 大素数的 BN 曲线方程 $E: y^2 = x^3 + 5$ 。实验配置为 Windows 11、AMD Ryzen 7 5800H with Radeon Graphics 3.20 GHz、32 GB RAM、JDK 11、JPBC 2.0.0。图 2 为同一条消息在不同签名人数时的计算开销, 横坐标表示签名者人数, 纵坐标表示系统运行时间单位, 将签名人数从 5 增加到 30, 每次增加 5 人。由此可见, 所选方案的系统计算时间随签名人数增加呈线性增长, 但在签名者人数相同时系统计算时间成本最小。

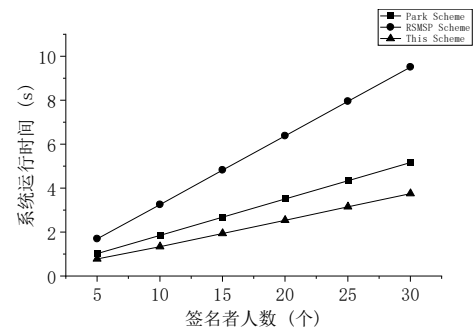


Fig. 2 System calculation time cost

图 2 系统计算时间成本

6 结语

多重签名是对单个数字签名的拓展, 涉及到多用户对同一份数据或交易进行签名。然而, 当前多重签名方案往往基于传统公钥密码系统与国外密码体制, 未能满足国内实际发展需求, 这使得国内在选择合适的多重签名方案

时,需更谨慎地均衡自主知识产权与信息安全性。

为了结合身份基密码体制与多重签名的优势,本文基于SM9标识签名密码算法设计了一种广播多重签名方案,并在随机预言模型下证明了该方案满足不可伪造性安全要求。同时,所使用的身份基签名算法能简化密钥管理,弱化对公钥证书的需求,计算代价分析与实验仿真也验证了所提方案的实用性和效率。未来,将围绕场景应用和国产密码体制,研究更多基于国产密码算法的功能性密码方案。

参考文献:

- [1] LI Y Q, LIU Z W. Design of security information sharing mechanism for Internet of vehicles based on blockchain[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(1): 103-110.
李永强, 刘兆伟. 基于区块链的车联网安全信息共享机制设计[J]. 郑州大学学报(工学版), 2022, 43(1): 103-110.
- [2] LIU X, LIU Y. Two-factor identity authentication scheme based on smart contract[J]. Computer and Modernization, 2023(10): 121-126.
刘鑫, 柳毅. 基于智能合约的双因素身份认证方案[J]. 计算机与现代化, 2023(10): 121-126.
- [3] YANG X, WEN H, DIAO R, et al. Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks[J]. IEEE Internet of Things Journal, 2023, 10(12): 10881-10892.
- [4] YANG X, WANG W, TIAN T, et al. Cryptanalysis and improvement of a blockchain-based certificateless signature for IIoT devices [J]. IEEE Transactions on Industrial Informatics, 2023, 20(2): 1844-1894.
- [5] LA Y, ZHAO J G, ZHANG W. Transactions of electric power science and technology, 2022, 37(4): 183-188, 226.
喇元, 赵继光, 张伟. 基于SM9门限签名的电力终端安全认证方案[J]. 电力科学与技术学报, 2022, 37(4): 183-188, 226.
- [6] LIU D, BI X H. Multi digital signatures and their application scenarios [J]. Information Technology and Informatization, 2022(8): 78-81.
刘丹, 毕晓红. 多重数字签名及其应用场景[J]. 信息技术与信息化, 2022(8): 78-81.
- [7] LTAKURA K, NAKAMURA K. A public-key cryptosystem suitable for digital multi-signatures [J]. NEC Research and Development, 1983, 71(71): 474-480.
- [8] ZHANG Y L, ZHANG J, WANG X F. An efficient identity and RSA based compact multiple digital signature scheme [J]. Journal of Electronics and Information Technology, 2008(9): 2246-2249.
张亚玲, 张璟, 王晓峰. 一个高效的基于身份和RSA的紧致多重数字签名方案[J]. 电子与信息学报, 2008(9): 2246-2249.
- [9] BELLARE M, NEVEN G. Identity-based multi-signatures from RSA [EB/OL]. <https://iacr.org/archive/pkc2010/60560484/60560484.pdf>.
- [10] HE Q Z, CAO S Z, WANG C F, et al. Identity-based auditable multiple intercept signature scheme [J]. Computer Engineering and Science, 2023, 45(2): 269-276.
何启芝, 曹素珍, 王彩芬, 等. 基于身份的可审计多重截取签名方案[J]. 计算机工程与科学, 2023, 45(2): 269-276.
- [11] TIAN C, WANG Z W. Identity-based multisig scheme based on subgrouping [J]. Computer Science, 2022, 49(12): 346-352.
田陈, 王志伟. 基于子分组的身份基多重签名方案[J]. 计算机科学, 2022, 49(12): 346-352.
- [12] SHIN Y A, JEONG I R, BYUN J W. Identity-based multi-proxy signature with proxy signing key for Internet-of-Drones [J]. IEEE Internet of Things Journal, 2023, 11(3): 4191-4205.
- [13] DE G M, MIYAJI A. Isogeny-based multi-signature scheme [C]// International Conference on Information Security Practice and Experience, 2023: 477-491.
- [14] PARK J H, PARK Y H. A tightly-secure multisignature scheme with improved verification [J]. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2016(2): 579-589.
- [15] BONEH D, DRIVERS M, NEVEN G. Compact multi-signatures for smaller blockchains [C]// International Conference on the Theory and Application of Cryptology and Information Security, 2018: 435-464.
- [16] GALINDO D, LIU J. Robust subgroup multi-signatures for consensus [EB/OL]. <https://eprint.iacr.org/2020/1478.pdf>.
- [17] LAI J, HUANG X, HE D, et al. Provably secure online/offline identity-based signature scheme based on SM9 [J]. The Computer Journal, 2022, 65(7): 1692-1701.
- [18] LIU H, HAN D, CUI M, et al. IdenMultiSig: identity-based decentralized multi-signature in Internet of Things [J]. IEEE Transactions on Computational Social Systems, 2023, 10(4): 1711-1721.
- [19] State Cryptography Administration. Announcement of the state cryptography administration (No. 30) [EB/OL]. http://www.sca.gov.cn/sca/xxgk/201603/28/content_1002815.shtml, 2016-3-28/2020-3-2.
国家密码管理局. 国家密码管理局公告(第30号) [EB/OL]. http://www.sca.gov.cn/sca/xxgk/201603/28/content_1002815.shtml, 2016-3-28/2020-3-2.
- [20] State Cryptography Administration. GM/T 0044-2016 SM9 Identification Password Algorithm [S]. Beijing: Standard Press of China, 2016.
国家密码管理局. GM/T 0044-2016 SM9 标识密码算法 [S]. 北京: 中国标准出版社, 2016.
- [21] Technical Committee for Standardization of Cryptography Industry. China's SM2 and SM9 digital signature algorithms officially became ISO/IEC international standards [EB/OL]. <http://www.gmbz.org.cn/main/postDetail.html?id=20180118171408>, 2017-11-17/2020-3-2.
密码行业标准化技术委员会. 我国SM2和SM9数字签名算法正式成为ISO/IEC国际标准 [EB/OL]. <http://www.gmbz.org.cn/main/postDetail.html?id=20180118171408>, 2017-11-17/2020-3-2.
- [22] ZHANG X F, PENG H. Research on a blind signature scheme based on SM9 algorithm [J]. Information Network Security, 2019, 19(8): 61-67.
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, 19(8): 61-67.
- [23] LAI J C, HUANG X Y, HE D B, et al. An efficient identity-based Sign-cryption scheme based on SM9 [J]. Journal of Cryptologic Research, 2021, 8(2): 314-329.
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.
- [24] TANG F, GAN N, YANG X G, et al. Anti malicious KGC certificateless signature scheme based on blockchain and domestic cryptographic SM9 [J]. Chinese Journal of Network and Information Security, 2022, 8(6): 9-19.
唐飞, 甘宁, 阳祥贵, 等. 基于区块链与国密SM9的抗恶意KGC无证书签名方案[J]. 网络与信息安全学报, 2022, 8(6): 9-19.
- [25] ZHU L F, LI J G, LAI J C, et al. Attribute-based online/offline signature scheme based on SM9 [J]. Journal of Computer Research and Development, 2023, 60(2): 362-370.
朱留富, 李继国, 赖建昌, 等. 基于商密SM9的属性基在线/离线签名方案[J]. 计算机研究与发展, 2023, 60(2): 362-370.
- [26] WANG X F, ZHANG J, WANG S P. Multi-signature scheme and its security proof [J]. Chinese Journal of Computers, 2008(1): 176-183.
王晓峰, 张璟, 王尚平. 多重数字签名方案及其安全性证明[J]. 计算机学报, 2008(1): 176-183.
- [27] GANGISHETTI R, GORANTLA M C, DAS M L, et al. Identity based multisignatures [J]. Informatica, 2006, 17(2): 177-186.
- [28] LAI J C, HUANG X Y, HE D B, et al. Security analysis of SM9 digital signature and key encapsulation [J]. Science in China (Information Sciences), 2021, 51(11): 1900-1913.
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.

(责任编辑: 刘嘉文)