# 基于国密 SM9 算法的门限环签名方案

邓浩明[1,2],彭长根[1,2,3],丁红发[4],叶延婷[1,2]
(1. 贵州大学 计算机科学与技术学院,贵州 贵阳 550025;
2. 贵州大学 公共大数据国家重点实验室,贵州 贵阳 550025;
3. 贵州大学 密码学与数据安全研究所,贵州 贵阳 550025;
4. 贵州财经大学 信息学院,贵州 贵阳 550025)

**摘 要**:环签名具有隐匿签名成员真实身份的优势,但现有环签名方案仍存在没有很好同时解决效率与安全性等问题。针对此问题,提出一种基于国密 SM9 算法的门限环签名方案(GMTRS)。首先,利用强抗碰撞性的 SM3 密码杂凑算法生成长度为 256 bit 的常数项值,利用安全冗余度更高的 SM4 分组密码算法对签名进行加解密处理,并在密文中嵌入具备时效性的时间戳,来提高签名算法的安全性;其次,在基于身份的环签名基础上利用门限参数提取算法引入门限值 $t$,使签名过程的效率得到提高,并将无需维护公钥证书和加解密速度快的 SM9 算法与门限环签名相结合,既保留了门限环签名的特性,又提高了签名算法的效率;最后,在随机预言模型下证明了 GMTRS 方案具有适应性选择消息攻击下的不可伪造性。与现有方案相比,该方案具备不可伪造性、匿名性、抗重放攻击性、前向后向安全性等优势。效率分析表明,GMTRS 方案在签名生成和验证阶段的效率分别提升约 52.38% 和 32.16%。并且门限值 $t$ 的变化,对方案总体计算开销影响较小。

**关键词**:国密算法;门限环签名;身份标识密码算法;不可伪造性;可证明安全
**中图分类号**:TP309 **文献标识码**:A **文章编号**:1673-629X(2022)12-0095-08
doi:10.3969/j.issn.1673-629X.2022.12.015

# A Threshold Ring Signature Scheme Based on GM SM9 Algorithm

DENG Hao-ming[1,2], PENG Chang-gen[1,2,3], DING Hong-fa[4], YE Yan-ting[1,2]
(1. School of Computer Science and Technology, Guizhou University, Guiyang 550025, China;
2. State Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China;
3. Institute of Cryptography and Data Security, Guizhou University, Guiyang 550025, China;
4. School of Information, Guizhou University of Finance and Economics, Guiyang 550025, China)

**Abstract**: Ring signature has the advantage of concealing the identity of the signature members in the ring, but the existing ring signature schemes have some problems such as low security and efficiency. To solve this problem, a threshold ring signature scheme based on SM9 algorithm is proposed. Firstly, the strong anti-collision SM3 cryptographic hash algorithm is used to generate the constant term value with a length of 256 bit, encrypt the signature with the more secure SM4 algorithm, and the time stamp with timeliness is embedded in the ciphertext to improve the security of the signature algorithm. Secondly, based on the identity based ring signature, the threshold parameter extraction algorithm is used to introduce the threshold value $t$, which improves the efficiency of the signature process. The SM9 algorithm, which does not need to maintain the public key certificate and has fast encryption and decryption speed, is combined with the threshold ring signature, which not only retains the characteristics of the threshold ring signature, but also improves the efficiency of the signature algorithm. Finally, it is proved that the proposed scheme has strong unforgeability under the random oracle model. Compared with most ring signature schemes, the proposed scheme has the advantages of strong unforgeability, anonymity, anti replay attack, forward and backward security and so on. Efficiency analysis shows that the efficiency of GMTRS scheme in the signature generation and verification stages is improved by about 52.38% and 32.16% respectively. The change of threshold value $t$ has little impact on the overall computational overhead of the scheme.

**Key words**: GM algorithms; threshold ring signature; identity-based cryptography; unforgeability; provably safe

**收稿日期**:2021-12-06 **修回日期**:2022-04-12
**基金项目**:国家自然科学基金项目(1836205);贵州省科技计划基金项目(黔科合平台人才[2020]5017);贵州省教育厅自然科学项目(黔教合 KY 字[2021]140)
**作者简介**:邓浩明(1998-),男,硕士,研究方向为密码学、国密算法;通讯作者:彭长根(1963-),男(侗),博导,教授,CCF 高级会员(48309S),研究方向为密码学、隐私保护。

## 0 引 言

当前,许多敏感隐私数据需依托网络进行传输,这对传输数据的安全提出了很高的要求。目前绝大多数传输系统利用密码技术来保证数据的隐私安全,但数据签名者的身份并没有得到很好的保护,这会导致数据发送方与接受方存在身份泄露的安全问题。

环签名[1]的提出能够解决签名者的身份隐私问题,可以确保环内签名者的身份实现匿名化。一个环签名方案包含 $n$ 个自发组成环的签名者,环中签名者首先使用私钥对消息进行签名,其次利用公钥验证签名的有效性。环签名已有广泛的应用,如车载物联网[2]、自动泊车系统[3]、第六代移动通信技术(6G)[4]、区块链[5]等场景。

在环签名的基础上,Bresson 等[6]提出第一个门限环签名方案,其主要原理是预先设置一个门限值 $t$,只要任意 $t$ 个环成员进行签名,就可得到最终签名结果。该方案利用公平拆分的思想将环成员进行公平拆分,在随机预言模型下证明了方案的安全性,但签名的效率随着签名者数量的增加而降低。文献[7]利用消息块共享技术提出了一种基于格的门限环签名方案,但该方案在消息比特长度较大时,签名生成与验证的效率较低。文献[8]通过将随机因子引入到用户的属性密钥中,提出了一个可变门限环签名方案,其实现了具有抗合谋攻击的安全特性,但方案的签名长度较长,验证效率较低。文献[9]提出一个利用分布式密钥生成协议解决属性密钥托管问题的门限环签名方案。巧妙利用身份标识的特性,使方案的安全性得到进一步的加强。此外,该方案提出了一种批验证方法,能够有效提高验证的效率。文献[10]将门限环签名应用于区块链上,提出了一种可以将过期区块数据删除的可删除区块链方案,利用门限值的特性,提高删除区块的效率。

Shamir 首次提出基于身份的密码体制(IBC)[11],IBC 可以将用户的身份标识作为公钥,同时也不需要额外的数字证书,因此在不同场景下得到了广泛的应用。文献[12]首先提出一种基于身份的环签名方案,该方案的双线性配对运算较多,因此在计算效率上有一定的劣势。文献[13]基于公平拆分的思想,提出了一种基于身份的 $(t,n)$ 门限环签名方案,但在签名生成与验证阶段需要多次使用双线性对运算,所以效率较低。文献[14]提出两种基于身份的门限环签名方案,在该方案中,任何 $t$ 个环成员可以代表 $n$ 个环成员生成一个合法的门限环签名。但该方案需要 $n$ 倍次数的双线对运算,其总效率具有的优势并不明显。文献[15]提出一种可以利用基于原始消息生成的环签名,去派生原始消息子串上的新环签名的方案,由于该方案需要多次指数运算,其在总体计算开销上效率较低。文献[16]将门限环签名与可否认认证协议相结合提出一种非交互式可否认 $(t,n)$ 门限环签名方案,其可以确保签名的真实身份不被泄露,但无法抵御选择消息攻击。文献[17]提出一个在格上基于模糊身份的环签名方案,该方案可以实现对真实签名者的身份进行审计与监督,并在随机预言模型下证明了方案的安全性,但仍存在签名效率不高的问题。文献[18]提出一个基于 SM9 算法的环签名方案,但在签名生成和验证阶段需 $n$ 倍次数的双线对运算,方案总体计算开销效率较低。

综上所述,现有方案没有很好地同时解决环签名的效率与方案的安全性等问题。为了解决上述问题,该文利用强抗碰撞性的 SM3 算法[19]对 $n-t$ 次多项式的常数项进行优化处理,并生成 256 bit 的杂凑值;利用 SM4 算法[20]资源消耗率较低和加解密效率高的优势,对门限环签名进行对称加密,并在密文中嵌入具有时效性的时间戳,提高了签名的安全性;最后,将文献[7]中的门限参数提取算法进行改进,并把生成的门限值 $t$ 引入 SM9 签名算法中,使得签名效率得到提高,并利用 SM9 算法[21]加密强度大、系统资源消耗率较低、无需申请数字证书和广泛应用性[22-23]等优势,将 SM9 数字签名算法作为底层密码技术基础,最终生成安全高效的门限环签名。

在随机预言模型下证明了 GMTRS 方案具有适应性选择消息攻击下的不可伪造性,并具有匿名性、抗重放攻击性和前向后向安全性等优势。效率分析表明,GMTRS 方案相较于现有环签名方案,在签名生成和验证效率上分别具有约 52.38% 和 32.16% 的效率提升。同时所提方案的门限值 $t$ 的变化,对方案的总开销影响基本可忽略,故 GMTRS 方案在安全性与效率上具有一定的优势。

## 1 基础知识

### 1.1 双线性对

设 $G_1$ 和 $G_2$ 是阶为素数 $N$ 的加法循环群,$G_T$ 是阶为素数 $q$ 的乘法循环群,$P_1$ 和 $P_2$ 分别为 $G_1$ 和 $G_2$ 的生成元。定义在群上的一个双线性映射关系 $e:G_1 \times G_2 \rightarrow G_T$,并且满足以下的性质:

(1)双线性:对 $\forall U \in G_1, \forall V \in G_2$ 和随机数 $x,y \in Z_q^*$,都满足 $e(U^x,V^y)=e(U,V)^{xy}$。

(2)非退化性:对 $\exists U \in G_1, \exists V \in G_2$,满足 $e(U,V) \neq 1$。

(3)可计算性:对 $\forall U \in G_1, \forall V \in G_2$,存在一个有效的算法在多项式时间内计算 $e(U,V)$ 的值。

### 1.2　困难问题假设

定义 1:离散对数问题(DLP)。给定椭圆曲线 $E$ 上任意两点 $P,Q$,给定等式 $aP = Q$,在多项式时间内 $a$ 是不可解的。

### 1.3　环签名相关概念

门限环签名方案[6]的一般模型由以下 4 个阶段组成。

初始化:输入安全参数 $\gamma$,输出公共参数 $P$ 和系统主密钥 $K_{\text{pub}}$。

密钥生成:输入 $(P,K_{\text{pub}})$,输出签名者的公私钥对 $(\text{pk}_i,\text{sk}_i)$,$i \in [1,N]$。

签名生成:输入公共参数 $P$,消息 $m$,门限值 $t$,$n$ 个环成员的公钥集合 $P = \{\text{pk}_1,\text{pk}_2,\cdots,\text{pk}_n\}$ 和所对应的私钥集合 $\varepsilon = \{\text{sk}_1,\text{sk}_2,\cdots,\text{sk}_n\}$,输出环签名 $\sigma$。

签名验证:输入公共参数 $P$,消息 $m$,门限值 $t$,$n$ 个环成员的公钥集合 $P = \{\text{pk}_1,\text{pk}_2,\cdots,\text{pk}_n\}$ 和所对应的私钥集合 $\varepsilon = \{\text{sk}_1,\text{sk}_2,\cdots,\text{sk}_n\}$ 以及环签名 $\sigma$,返回验证结果接受或拒绝。

基于身份的门限环签名方案[13]的一般模型由以下 4 个阶段组成。

初始化:输入随机数 $\pi$,输出主密钥 $K$ 和系统参数 Para。

密钥生成:输入系统参数 $\overline{\omega}$,签名者的身份标识 $\text{ID} \in \{0,1\}^*$ 和主密钥 $K$,输出签名者的公钥 PK 和私钥 SK。

签名生成:输入消息 $m$,$n$ 个签名者的身份标识 $\text{ID}_i \in \{0,1\}^*$,$i \in [1,n]$,$t$ 个签名者的私钥 $\text{SK}_i$,输出一个关于消息 $m$ 的基于 $(t,n)$ 门限值的环签名 $\sigma$。

签名验证:输入环签名 $\sigma$,消息 $m$,门限值 $t$ 和 $n$ 个签名者身份标识 $\text{ID}_i \in \{0,1\}^*$,如果 $n$ 个签名者中至少有 $t$ 个成员对消息 $m$ 签名,则返回验证结果为有效;否则,返回结果为无效。

### 1.4　门限环签名安全性定义

本节主要介绍门限环签名的安全模型,门限环签名方案必须满足以下条件。

定义 2:正确性。如果 $t$ 个以上的签名者按照签名步骤生成环签名 $\sigma$,则环签名 $\sigma$ 能通过验证。

定义 3:强不可伪造性。假如有 $n$ 个环成员,在其中任意选取个数不小于 $t$ 个的环成员,就可代表环进行签名。如果攻击者 $A$ 在概率多项式时间内选择任意消息 $M$(除 $M'$ 以外)并询问相应的签名结果后,成功伪造一个签名的概率仍是可忽略的,则门限环签名方案满足适应性选择消息攻击下的不可伪造性。

定义攻击者 $A$ 成功伪造门限环签名的优势为:

$$\text{Adv}_A^{\text{UNF}} = \Pr[A \text{ wins}]$$

GMTRS 方案的不可伪造性可以通过以下游戏进行正式定义:

初始化阶段:已知 $n$ 个环成员的身份标识集合 $\text{ID} = \{\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_n\}$,$i \in [1,n]$,其中挑战者 $C$ 运行 KeyGen 算法获得 $n$ 个环成员的公私钥对 $\text{MK}_1 = (\text{sk}_i,\text{pk}_i)$,$i \in [1,n]$,并将环成员的公钥 $\text{pk}_i$ 发给攻击者 $A$。

询问阶段:攻击者 $A$ 可以自适应地执行哈希询问、私钥询问、签名询问。

(1)哈希询问:攻击者 $A$ 向挑战者 $C$ 要求获取关于消息 $M$ 的哈希值。

(2)私钥询问:攻击者 $A$ 选择任意环成员的身份标识 $\text{ID}_i$ 发送给挑战者 $C$,挑战者 $C$ 计算相应的私钥 $\text{sk}_i$ 返回给攻击者 $A$。

(3)签名询问:攻击者 $A$ 选择消息 $M$,门限值 $t$,发送给挑战者 $C$,挑战者 $C$ 运行 Sign 并生成消息 $M$ 相应的门限环签名 $\sigma$。

伪造阶段:假设攻击者 $A$ 能以不可忽略的优势 $\text{Adv}_A^{\text{UNF}}$ 成功伪造出门限环签名,并将消息 $M'$ 相应的环签名 $\sigma'$ 发送给挑战者 $C$。如果下列条件成立,则攻击者 $A$ 获胜。

(1)验证 $(M',\sigma') = \text{true}$。

(2)签名伪造者的身份标识 $\text{ID}_i \in \text{ID}$,$i \in [1,t]$。

(3)没有执行签名算法而生成 $(M',\sigma')$。

定义 4:匿名性。在门限环签名方案中,超过 $t$ 个以上的签名者参与签名,并最终生成门限环签名 $\sigma$。但攻击者不知道是哪 $t$ 个签名者参与了门限环签名的生成。

## 2　基于国密 SM9 算法的门限环签名方案

GMTRS 方案包括初始化、密钥生成、环签名生成、环签名加密、环签名验证五个阶段。在初始化阶段之前,GMTRS 方案使用 Choi 和 Kim 提出的门限参数提取算法[7],生成环 $n$ 和门限 $t$ 的值。但该算法在消息长度很短时,无法生成相应的参数,从而导致无法生成门限环签名。因此,先对消息的位长进行处理,将短消息用 0 bit 填充到 $\lambda$bit 宽度,将长消息压缩到 $\lambda$ bit 宽度。其中,由于方案选取的曲线是阶为 256 bit 的 BN 曲线,所以方案的 $\lambda$ 长度设置为 256 bit。最后,输入填充后的消息,生成环 $n$ 和门限值 $t$ 的值。

### 2.1　初始化

$$\text{Setup}(\lambda) \rightarrow (\text{MK},\text{Para})$$

首先,获取环 $n$ 的大小,门限值 $t$ 的大小,其中 $t < n$。其次,设定并输入安全参数 $\lambda$,KGC 定义 $G_1$、$G_2$ 和 $G_T$ 是阶为素数 $N$ 的循环群,并且 $P_1$ 为 $G_1$ 的生成元和 $P_2$ 为 $G_2$ 的生成元;并定义一个双线性映射关系 $e$:$G_1 \times G_2 \rightarrow G_T$;从 SM3 密码杂凑算法中选取哈希函数

$H_0, H_1: \{0,1\}^* \to Z_q^*$，$H_2: \{0,1\}^* \to G_1$，伪随机函数 $F: \{0,1\}^K \times \{0,1\}^* \to \{0,1\}^l$；KGC 随机选择 ran $\in [1, N-1]$ 作为主私钥。计算 $P_{mpk} = [ran]P_2$ 作为主公钥。最后，输出公共参数 Para $= (N, G_1, G_2, G_T, P_1, P_2, e, ran, H_0, H_1, H_2, F)$，主密钥对 MK $= (ran, P_{mpk})$。

### 2.2 密钥生成

KeyGen$(\lambda, ID, ran) \to (K_e, MK_1)$

输入安全参数 $\lambda$，$n$ 个环成员的身份标识集合 ID $= \{ID_1, ID_2, \cdots, ID_n\}$，主私钥 ran。

(1)KGC 选择 $K_e \leftarrow \{0,1\}^\lambda$ 作为 SM4 分组密码算法的对称密钥。

(2)KGC 选择私钥生成函数识别符 $\chi$，并计算 $t_1 = H_1(ID_i \| \chi, N) + ran$，如果 $t_1$ 为 0，KGC 重新选择新的随机数来产生主私钥，并需要重新计算主公钥；否则计算 $t_2 = ran \cdot t_1^{-1}$。最后计算环成员的私钥 $sk_i = [t_2]P_1 = [ran/(H_1(ID_i \| \chi, N) + ran)]P_1$ 和公钥 $pk_i = [H_1(ID_i \| \chi)]P_2$。

(3)输出对称加密密钥 $K_e$，环成员的公私钥对 $MK_1 = (pk_i, sk_i)$。

### 2.3 环签名生成

Sign(Para, $M, t, P_{mpk}, R, U) \to (\sigma)$

输入公共参数 Para，消息 $M$，门限值 $t$，主公钥 $P_{mpk}$，环签名成员的私钥集合 $R = \{sk_i\}$，$i \in [1, n]$，其私钥所对应的公钥集合 $U = \{pk_i\}$，$i \in [1, n]$，设 $\{1, 2, \cdots, t\}$ 为参与签名的环成员索引，不参与签名的环成员索引为 $d \in \{t+1, t+2, \cdots, n\}$，签名生成具体的步骤如下：

(1)计算 $g = e(P_1, P_{mpk})$；

(2)对于 $d \in \{t+1, t+2, \cdots, n\}$，随机选择 $r_d, h_d \in [1, N-1]$；计算 $Z_d = g^{r_d}$，$T_d = [Z_d]sk_d$；

(3)对于 $j \in \{1, 2, \cdots, t\}$，随机选择 $u_j \in [1, N-1]$，计算 $Z_j = g^{u_j}$；

(4)将 $Z_d, Z_j$ 的数据类型转换为比特串，并计算 $h_0 = H_0(U \| t \| M \| Z_1 \| Z_2 \cdots \| Z_n, N)$；

(5)计算 $L = (u_j - h_0) \bmod N$，若 $L = 0$ 则返回步骤(2)，重新选择随机数；

(6)对于 $d \in \{t+1, t+2, \cdots, n\}$，构造一个 $n-t$ 次多项式 $f_d(x) = h_d x^{n-t} + \cdots + h_2 x^2 + h_1 x + h_0$，其中，

$h_d = H_0(pk_d \| n - t \| M \| Z_{t+1} \| Z_{t+2} \cdots \| Z_n, N)$，

$f(0) = h_0$，$f(d) = h_d$；

(7)当 $j \in \{1, 2, \cdots, t\}$，计算 $h_j = f(j)$，$S_j = [u_j - h_j]sk_j$；

(8)输出关于消息 $M$ 的 $(t, n)$ 门限环签名 $\sigma = (t, S_1, S_2, \cdots, S_t, T_{t+1}, T_{t+2}, \cdots, T_n, f)$。

### 2.4 环签名加密

Enc$_1(\sigma, M, K_e, \eta) \to (E\sigma, EM)$

输入环签名 $\sigma$，对称密钥 $K_e$，时间戳 $\eta$，使用 SM4 分组加密算法，对消息 $M$ 和环签名 $\sigma$ 进行加密，并嵌入时间戳 $\eta$，输出密文消息 EM 和加密环签名 E$\sigma$。

Enc$_2(pk_i, K_e) \to (EK_e)$

输入环成员的公钥 $pk_i$，对称密钥 $K_e$，输出加密的密钥 $EK_e$。

### 2.5 环签名验证

Dec$_1(EK_e, sk_i) \to (K_e)$

输入环成员的私钥 $sk_i$，加密的密钥 $EK_e$，输出对称密钥 $K_e$。

Dec$_2(K_e, EM, E\sigma) \to (M', \sigma')$

输入对称密钥 $K_e$，密文消息 EM 和加密环签名 E$\sigma$，输出均包含时间戳的消息 $M'$ 和环签名 $\sigma' = (t, S_1', S_2', \cdots, S_t', T_{t+1}', T_{t+2}', \cdots, T_n', f')$。

Verify (Para, $P_{mpk}, M', \sigma', t, U, ID) \to$ (accept, reject)

输入公共参数 Para，消息 $M'$，门限值 $t$，主公钥 $P_{mpk}$，$n$ 个环成员公钥集合 $U$，环签名 $\sigma'$，$n$ 个环成员的身份标识集合 ID $= \{ID_1, ID_2, \cdots, ID_n\}$，签名验证具体的步骤如下：

(1)检查消息 $M'$ 和环签名 $\sigma'$ 中时间戳 $\eta$ 的时效性，如果无效则拒绝该消息验证失败；否则继续执行；

(2)验证多项式 $f$ 是否为 $n-t$ 次，如果不是，则验证失败；

(3)将 $f'(0)$ 的数据类型转换为整数，将 $T_d'$ 的数据类型转换为椭圆曲线上的点，并同时验证 $f'(0) \in [1, N-1]$ 和 $T_d' \in G_1$ 是否成立，如果验证不通过，则结束验证流程；

(4)计算 $g = e(P_1, P_{mpk})$，$v_j = g^{f(j)}$；

(5)计算 $c_j = H_1(ID_j \| \chi, N)$，$P_j = [c_j]P_2 + P_{mpk}$，$z_j = e(S_j', P_j)$；

(6)计算 $w_j' = v_j \cdot z_j$，将 $w_i'$ 转化为比特串类型；

(7)计算 $h' = H_0(U \| t \| M' \| w_1' \| w_2' \cdots \| w_j', N)$；

(8)验证 $h' = f'(0)$ 是否成立，若成立则签名合法，则输出“accept”；若不成立，则输出“reject”。

## 3 安全性分析

### 3.1 方案的正确性

定理 1：GMTRS 方案的门限环签名满足正确性。

证明：在门限环签名验证时，需要验证 $h' = f'(0)$ 是否成立。

因为 $h' = H_0(U \| t \| M' \| w_1' \| w_2' \cdots \| w_n', N)$，而 $f'(0) = H_0(U \| t \| M \| Z_1 \| Z_2 \cdots \| Z_n, N)$，则只需要验证 $w'$ 与 $Z$ 是否相等。

因为,

$$z_j = e(S_j', P_j) =$$
$$e([u_j - h_j]\mathrm{sk}_j, [c_i]P_2 + P_{\mathrm{mpk}}) =$$
$$e(([u_j - h_j][t_2]P_1), [c_i]P_2 + [\mathrm{ran}]P_2) =$$
$$e(P_1, P_2)^{(u_j - h_j)[t_2](c_i + \mathrm{ran})} =$$
$$e(P_1, P_2)^{(u_j - h_j)[\mathrm{ran} \cdot t_1^{-1}](H_1(\mathrm{ID}_i \| \chi, N) + \mathrm{ran})} =$$
$$e(P_1, P_2)^{(u_j - h_j)[\frac{\mathrm{ran}}{H_1(\mathrm{ID}_i \| \chi, N) + \mathrm{ran}}](H_1(\mathrm{ID}_i \| \chi, N) + \mathrm{ran})} =$$
$$e(P_1, P_2)^{(u_j - h_j)[\mathrm{ran}]} \tag{1}$$

又因为,

$$v_j = g^{f(j)} = e(P_1, P_{\mathrm{mpk}})^{h_j} =$$
$$e(P_1, [\mathrm{ran}]P_2)^{h_j} =$$
$$e(P_1, P_2)^{h_j[\mathrm{ran}]} \tag{2}$$

则:

$$w' = v_j \cdot z_j =$$
$$e(P_1, P_2)^{(u_j - h_j)[\mathrm{ran}]} \cdot e(P_1, P_2)^{h_j[\mathrm{ran}]} =$$
$$e(P_1, P_2)^{u_j[\mathrm{ran}]} = e(P_1, [\mathrm{ran}]P_2)^{u_j} =$$
$$e(P_1, P_{\mathrm{mpk}})^{u_j} = Z \tag{3}$$

根据签名验证结果可知, $w'$ 与 $Z$ 相等,因此 GMTRS 方案满足正确性。

### 3.2　方案的不可伪造性

定理 2:在随机预言模型中,如果 DLP 问题具有难解性,则 GMTRS 方案具有适应性选择消息攻击下的不可伪造性。

证明:给挑战者 $C$ 一个 DLP 问题的挑战实例 $(P_1, aP_1)$, $C$ 的目标是利用敌手 $A$ 的能力伪造出有效的门限环签名,并最终计算出 $a$。在随机预言模型下,密码杂凑函数 $H_0$, $H_1$ 被当作随机预言机。

初始化:挑战者 $C$ 执行 Setup 算法获得系统参数 Para 和主密钥对 MK,并将系统参数 Para 发送给攻击者 $A$。

询问阶段:攻击者 $A$ 执行自适应询问,挑战者 $C$ 设置 $L_0$、$L_1$、$L_2$ 和 $L_3$ 列表去存储询问结果。其中,列表 $L_0$ 中储存哈希 $H_0$ 询问结果,列表 $L_1$ 中储存哈希 $H_1$ 询问结果,列表 $L_2$ 中储存私钥询问结果,列表 $L_3$ 储存签名询问结果。

(1)哈希 $H_0$ 询问:当 $A$ 询问 $H_0(U \| t \| M \| Z_1 \| Z_2 \cdots \| Z_n, N)$ 时, $C$ 首先在 $L_0$ 中检查 $H_0$ 的询问记录。若询问记录不存在, $C$ 将随机选择 $c_i \in [1, N-1]$,并设置 $H_0(U \| t \| M \| Z_1 \| Z_2 \cdots \| Z_n, N) = c_i$,并以 $((U \| t \| M \| Z_1 \| Z_2 \cdots \| Z_n, N), c_i)$ 的格式存储到 $L_0$ 中。

(2)哈希 $H_1$ 询问:攻击者 $A$ 发送给挑战者 $C$ 一个环成员的身份标识 $\mathrm{ID}_i$,同时询问 $H_1(\mathrm{ID}_i \| \chi, N)$, $C$ 首先在 $L_1$ 中检查其询问记录。若记录不存在, $C$ 将随机选择 $y_i \in [1, N-1]$,设置 $H_1(\mathrm{ID}_i \| \chi, N) = x_i$,并将 $((\mathrm{ID}_i \| \chi, N), x_i)$ 存储到 $L_1$ 中。

(3)私钥询问:攻击者 $A$ 随机选择一个环成员的身份标识 $\mathrm{ID}_i$ 发送给挑战者 $C$,并要求返回相应的私钥。$C$ 首先随机选择 $y_i \in [1, N-1]$,并在到 $L_1$ 中找到 $\mathrm{ID}_i$ 所对应的 $x_i$ 值;随即计算 $t_1' = x_i + y_i$, $\mathrm{sk}_i = [y_i / t_1']P_1$,并将 $(\mathrm{ID}_i, \mathrm{sk}_i)$ 存储到 $L_2$ 列表中,最后 $A$ 收到私钥 $\mathrm{sk}_i$。

(4)签名询问:攻击者 $A$ 任意选择消息 $M$、门限值 $t$ 和主公钥 $P_{\mathrm{mpk}}$ 发送给挑战者 $C$, $C$ 执行 Sign 算法生成门限环签名 $\sigma$,并将 $(M, t, \sigma)$ 储存到 $L_3$ 列表中。如果生成签名过程中发生哈希碰撞,则需要重新执行生成门限环签名的步骤。

伪造阶段:针对签名者 $\mathrm{ID}_i \in [1, t]$ 及消息 $M'$,如果 $A$ 能够从列表 $L_1$、$L_2$ 中获取正确记录,且不经过签名询问下成功伪造出一个能够通过验证的签名 $\sigma^*$。根据分叉引理[24], $A$ 以一个不可忽略的优势 $\mathrm{Adv}_A^{\mathrm{UNF}}$ 成功伪造 2 个有效的门限环签名 $\sigma^*$、$\sigma^{*'}$,且 $\sigma^*$、$\sigma^{*'}$ 未在签名询问时出现。其中 $u_j^* \neq u_j^{*'}$, $h_j^* \neq h_j^{*'}$,则由签名生成算法可以得到:

$$S_j^* = [u_j^* - h_j^*]\mathrm{sk}_j \tag{4}$$
$$S_j^{*'} = [u_j^{*'} - h_j^{*'}]\mathrm{sk}_j \tag{5}$$

所以,

$$\mathrm{sk}_j = \frac{S_j^{*'} - S_j^*}{[(u_j^{*'} - u_j^*) + (h_j^* - h_j^{*'})]} \tag{6}$$
$$a = \frac{S_j^{*'} - S_j^*}{P_1[(u_j^{*'} - u_j^*) + (h_j^* - h_j^{*'})]} \tag{7}$$

因此 DLP 问题的挑战实例 $(P_1, aP_1)$ 可解,由于 DLP 难解性可知其与假设相矛盾,所以 GMTRS 方案在随机预言模型中具有适应性选择消息攻击下的不可伪造性。

### 3.3　方案的匿名性

定理 3:GMTRS 方案具备匿名性。

证明:在签名生成算法中, $h_0$ 是单向密码杂凑函数 $H_0$ 生成的,而 $n-t$ 次多项式 $f$ 的常数项 $h_1, h_2, \cdots, h_d$ 是随机选取的,所以多项式 $f$ 也可以看成是随机选取且均匀分布的。在签名验证算法中,利用环成员的公钥 $\mathrm{pk}_i$ 对签名的合法性进行验证。根据 $S_j = (u_j - h_j)\mathrm{sk}_j$ 与 $T_d = [C_d]\mathrm{sk}_d$ 的生成过程可知,其包括单向哈希函数和椭圆曲线离散对数问题,这使得攻击者 $A$ 无法通过计算的方法确定签名者的真实身份。$A$ 无论是以随机选择的方式还是以计算的方式,都不能以超过 $\frac{t}{n}$ 的概率猜出签名者的真实身份,故 GMTRS 方案具备匿名性。

### 3.4　方案的前向与后向安全性

定理 4:GMTRS 方案满足前向与后向安全性。

证明:密钥生成中心(KGC)重新选择随机数 ran 来确定系统的主私钥,根据重新确定的主私钥来确定系统的主公钥 $P_{mpk}$,并将更新的主密钥对 MK = (ran, $P_{mpk}$) 发送给环成员,同时 KGC 也会记录之前的主密钥对,用来验证之前签名的有效性。因为 ran 是 KGC 随机选取的,所以 ran 具有随机性,从而系统参数 Para 也具有随机性,所以攻击者 $A$ 不能伪造出之前的主密钥对。即使 $A$ 成功伪造出主密钥对,其也无法融入到环成员中,也无法伪造出门限环签名,所以 GMTRS 方案满足前向与后向安全性。

### 3.5 方案的抗重放攻击性

定理 5:GMTRS 方案中的门限环签名具备可抗重放攻击性。

证明:GMTRS 方案在已签名的门限环签名 $\sigma$ 和消息 $M$ 的密文中嵌入一个时间戳 $\eta$。在验证签名之前,首先将检查时间戳 $\eta$ 的时效性。如果攻击者 $A$ 截获合法生成的门限环签名或消息两者其中的一个,在验证签名时,时间戳的新鲜度检查将失败,则该门限环签名 $\sigma'$ 或消息 $M'$ 将被拒绝,导致签名验证流程结束,故 GMTRS 方案生成的门限环签名具备可抗重放攻击性。

## 4 效率分析

将 GMTRS 方案与文献[12-14,16,18]进行计算开销对比,主要从私钥生成、签名生成和签名验证三个方面来比较,因为这三个部分所占的计算开销较大。其中主要比较双线性配对运算 $B$ 和幂运算 $E$ 的运算次数,因为双线性配对运算和幂运算所需要消耗的计算资源较多,同时忽略一些计算成本很小的运算。其中包括使用 SM4 算法对环签名进行对称加解密运算,GMTRS 方案只需要进行两次加密运算和两次解密运算,并且所需的计算开销与环成员个数 $n$ 和门限值 $t$ 的大小无关,根据表 3 中给出的单次加解密运算所消耗的时间大小,环签名加解密阶段所需的计算成本基本可以忽略。

GMTRS 方案使用嵌入度为 12 的 BN 曲线 $E: y^2 = x^3 + 5$,其中阶为 256 bit 的大素数 $N$。选择长度为 256 bit 的相应参数能保证方案具有与长度为 3 072 bit 的 RSA 密钥相当的安全强度。相关运算符号含义如表 1 所示,计算开销对比如表 2 所示。

表 1 运算符号含义

| 符号 | 含义 |
|---|---|
| $n$ | 环成员个数 |
| $t$ | 门限值 |
| $K_e$ | 对称加解密运算 |
| $B$ | 双线性配对运算 |
| $M$ | 椭圆曲线标量点乘运算 |
| $H$ | 哈希运算 |
| $E$ | 幂运算 |
| MI | 模逆运算 |
| MO | 取模运算 |

表 2 不同环签名方案计算开销

| 方案 | 私钥生成 | 签名生成 | 签名验证 | 总开销 |
|---|---|---|---|---|
| 文献[12] | $H + M$ | $(2n-1)B + nH + (2n-1)M$ | $2nB + nH + nM$ | $(4n-1)B + (2n+1)H + 3nM$ |
| 文献[13] | $H + M$ | $(2n+2t)B + (n+2t)H + (2n+t)M$ | $(4n-t)B + (n+t)H$ | $(6n+t)B + (2n+3t+1)H + (2n+1+t)M$ |
| 文献[14] | $H + E$ | $(2n-t)B + nH + (2n-t)E + tM + tMO$ | $2nB + 2nH + 2nE$ | $(4n-t)B + (3n+1)H + (4n-t+1)E + tM + tMO$ |
| 文献[16] | $H + M$ | $nB + H + (3n+2t)M$ | $2nB + nH + 2nM$ | $3nB + (n+2)H + (5n+2t+1)M$ |
| 文献[18] | $H + MI + M$ | $nB + nH + (n-1)E + (3n-1)M$ | $nB + nH + nE + 2nM$ | $2nB + (2n+1)H + (2n-1)E + 5nM + MI$ |
| GMTRS | $H + M$ | $B + (n-t)H + nE + nM + tMO$ | $(t+1)B + (t+1)H + tE + 2tM$ | $(t+2)B + (n+2)H + (n+t)E + (n+2t+2)M + tMO + 2Ke$ |

由表 2 可知,GMTRS 方案只需进行一次计算成本可忽略的哈希运算 $H$ 和计算成本较小的一次标量点乘运算 $M$ 就可生成私钥;在签名生成阶段,GMTRS 方案需要进行一次双线性配对运算 $B$、$n$ 次幂运算 $E$ 和 $n$ 次标量点乘运算 $M$,同时相较于效率较高的文献[16],其所需要的双线性配对运算与标量点乘运算的运算次数明显均要多于本方案;在签名验证阶段,GMTRS 方案需要进行双线性配对运算、幂运算和标

量点乘运算的次数只与门限值 $t$ 有关,由门限环签名的特性可知 $t < n$ ,所以本方案在签名验证阶段具有一定的性能优势;从总开销来看,GMTRS 方案需要进行 $t + 2$ 次双线性配对运算 $B$ 、$n + t$ 次幂运算 $E$ 和 $n + 2t + 2$ 次标量点乘运算 $M$ ,与文献[12-14,16,18]对比来看,GMTRS 方案具有较高的性能优势。

为了进行更加直观的对比,本文在 3.20 GHz 的 8 核 64 位 Intel(R)Core(TM) i5-10210 处理器、8 GB RAM 和 Windows 10 操作系统的计算机上进行了实验。基于表 1 相同的数据设置,并采用 Miracl 密码函数库进行实验操作,得到表 1 中相关运算的单次运算所消耗的时间。同时调用 SM4 对称加解密算法对 1 024字节长度的字节串进行加解密实验操作,并以循环执行 1 000 次加解密取平均值的方式,得出 SM4 单次对称加解密所消耗的时间,实验结果如表 3 所示。

表 3　相关运算单次运算消耗时间

| 符号 | 运行时间 /ms |
|---|---|
| $K_e$ | 2.457 6 |
| $B$ | 20.235 5 |
| $M$ | 3.216 6 |
| $H$ | 0.006 1 |
| $E$ | 9.863 3 |
| MI | 1.966 1 |
| MO | 0.416 5 |

本文以群体医疗咨询背景为例,没有设置过大的环成员数,按照实际情况将 $n$ 设置为 10, $t$ 设置为 6。其中 $n$ 为专家医生的人数,在上述相同的实验环境下,分别进行了签名阶段和签名验证阶段的时间开销对比实验,实验结果如图 1 和图 2 所示。

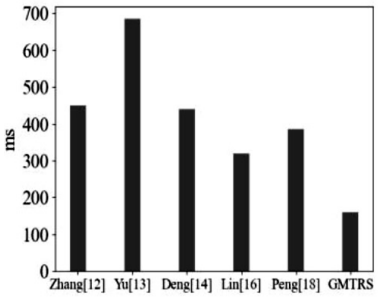


图 1　签名生成时间开销对比

由对比可得,GMTRS 方案对比文献[12-14,16,18]具有较高的签名生成效率,并且相较于耗时最短的文献[16],在签名阶段效率提升约 52.38% 。对比效率较高的文献[18],GMTRS 方案签名验证阶段效率得到约 32.16% 的提升。GMTRS 方案在签名生成阶段与签名验证阶段的效率均占有一定优势,具有更好的实用性。

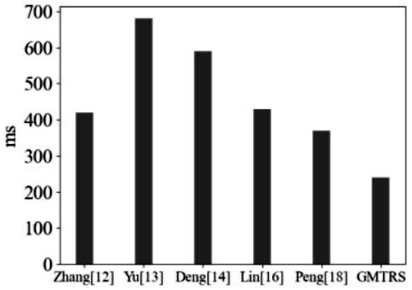


图 2　签名验证时间开销对比

由于签名效率会受到门限值 $t$ 和环成员 $n$ 大小变化的影响,所以以大规模签名场景为例,在相同的实验环境下,进行了 $n$ 与 $t$ 变化的对比实验,结果如图 3 和图 4 所示。

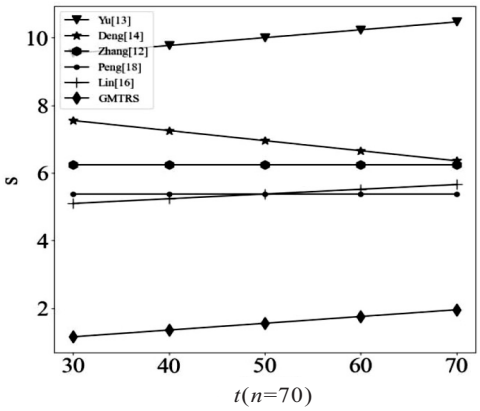


图 3　总开销下 $t$ 变化时间开销对比

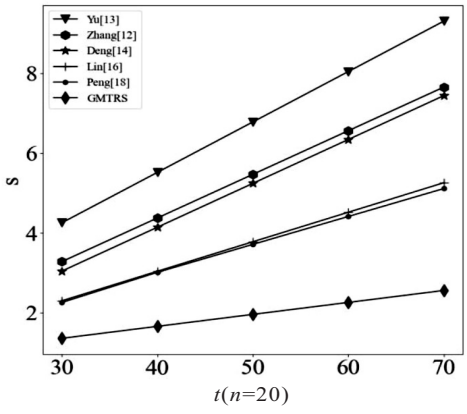


图 4　总开销下 $n$ 变化时间开销对比

图 3 和图 4 实验结果表明,GMTRS 方案的总开销与 $t$ 和 $n$ 的大小变化呈线性关系,但所提方案的曲线波动幅度较小。由图 3 可知,因为文献[12]与文献[18]是环签名方案,所以门限值 $t$ 的变化不会导致签名开销变化。但在 $n$ 和 $t$ 相等时,GMTRS 方案为全部环成员都参与签名的环签名方案,方案总体效率仍为最高。由如图 4 可知,当门限值 $t$ 大小固定 $n$ 增加时,方案的总体时间开销最小。综上,GMTRS 方案在签名生成阶段与验证阶段的效率均具有优势,具有更好的实用性。

## 5 结束语

在环签名的基础上,加入了 $(t,n)$ 门限值,利用国密算法作为底层密码技术支持,提出了一种基于国密 SM9 算法的门限环签名方案(GMTRS)。GMTRS 方案只需要 $t$ 个以上的签名者对消息进行签名,就可以代表所有环成员得到最终的签名。并将国密算法与门限环签名相结合,既保留了环签名的特性,又提高了签名的效率和安全性。在随机预言模型下证明了适应性选择消息攻击下的不可伪造性,同时 GMTRS 方案也具有不可匿名性和抗重放攻击性等优势。效率分析表明,GMTRS 方案在计算开销和效率上相较现有方案具有明显的优势。此外,该方案仍然需要计算成本高的双线性对运算,下一步需要考虑如何减少双线对运算次数等问题,使方案的效率更高。

**参考文献:**


[1] RIVEST R L,SHAMIR A,TAUMAN Y. How to leak a secret[C]//Proceedings of the 7th international conference on the theory and application of cryptology and information security. Berlin:Springer,2001:552-565.

[2] MUNDHE P,YADAV V K,VERMA S,et al. Efficient lattice-based ring signature for message authentication in VANETs[J]. IEEE Systems Journal,2020,14(4):5463-5474.

[3] XU S Y,CHEN X,WANG C,et al. A lattice-based ring signature scheme to secure automated valet parking[C]//7th international conference on wireless algorithms,systems,and applications. Nanjing:Springer,2021:70-83.

[4] LIU J H,YU Y,LI K,et al. Post-quantum secure ring signatures for security and privacy in the cybertwin-driven 6G[J]. IEEE Internet of Things Journal,2021,8(22):16290-16300.

[5] TA A T,KHUC T X,NGUYUE T N,et al. Efficient unique ring signature for blockchain privacy protection[C]//26th Australasian conference. Perth:Springer,2021:391-407.

[6] BRESSON E,STEM J,SZYDLO M. Threshold ring signatures and applications to ad-hoc groups[C]//International cryptology conference on advances in cryptology. California:Springer,2002:465-480.

[7] CHOI R,KIM K. Lattice-based threshold signature with message block sharing[C]//31st symposium on cryptography and information security. Kagoshima:[s. n.],2014:1-7.

[8] 陈 桢,张文芳,王小敏. 基于属性的抗合谋攻击可变门限环签名方案[J]. 通信学报,2015,36(12):212-222.

[9] 刘旭东,张文芳,王小敏. 分布式无中心授权的属性基可变门限环签名[J]. 软件学报,2018,29(11):3528-3543.

[10] 任艳丽,徐丹婷,张新鹏,等. 基于门限环签名的可删除区块链[J]. 通信学报,2019,40(4):71-82.

[11] SHAMIR A. Identity-based cryptosystem and signature scheme[C]//Advances in Cryptology-CRYPTO. Berlin:Springer,1984:47-53.

[12] ZHANG F G,KIM K. ID-based blind signature and ring signature from pairings[C]//International conference on the theory and application of cryptology and information security. Queenstown:Springer,2002:533-547.

[13] YU F C,WU Z,LAI F,et al. A novel ID-based threshold ring signature scheme competent for anonymity and Anti-forgery[C]//International conference on computational and information science. Guangzhou:Springer,2006: 502-512.

[14] DENG L Z,ZENG J W. Two new identity-based threshold ring signature schemes[J]. Theoretical Computer Science,2014,535:38-45.

[15] WANG K,MU Y,SUSILO W. Identity-based quotable ring signature[J]. Information Sciences,2015,321(C):71-89.

[16] LIN T C,YEH T Y,HWANG M S. Cryptanalysis of an ID-based deniable threshold ring authentication[J]. International Journal of Network Security,2019,21(2):298-302.

[17] CAO C T,YOU L,HU G R. Fuzzy identity-based ring signature from lattices[J]. Security and Communication Networks,2021,2021(5):1-9.

[18] 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.

[19] 王小云,于红波. SM3 密码杂凑算法[J]. 信息安全研究,2016,2(11):983-994.

[20] 吕述望,苏波展,王 鹏,等. SM4 分组密码算法综述[J]. 信息安全研究,2016,2(11):995-1007.

[21] GM/T 0044-2016. SM9 标识密码算法[S]. 2016.

[22] 杨亚涛,蔡居梁,张筱薇,等. 基于 SM9 算法可证明安全的区块链隐私保护方案[J]. 软件学报,2019,30(6):1692-1704.

[23] JI H,ZHANG H,SHAO L,et al. An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud[J]. Connection Science,2021,33(4):1-22.

[24] POINTCHEVAL D,STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology,2000,13(3):361-396.