



# 计算机科学

COMPUTER SCIENCE

## 基于国密算法SM9的环签名方案

谢振杰, 张耀, 杨启超, 宋恩舟

引用本文

谢振杰, 张耀, 杨启超, 宋恩舟. [基于国密算法SM9的环签名方案](#)[J]. 计算机科学, 2025, 52(12): 384-390.

XIE Zhenjie, ZHANG Yao, YANG Qichao, SONG Enzhou. [Ring Signature Scheme Based on Domestic Cryptographic Algorithm SM9](#) [J]. Computer Science, 2025, 52(12): 384-390.

---

## 相似文章推荐 (请使用火狐或 IE 浏览器查看文章)

Similar articles recommended (Please use Firefox or IE to view the article)

### [基于国密算法SM9的签密方案](#)

Signcryption Scheme Based on SM9 Domestic Cryptographic Algorithm

计算机科学, 2025, 52(11A): 241200049-8. <https://doi.org/10.11896/jsjcx.241200049>

### [基于国密算法SM9的加法同态加密方案](#)

Additively Homomorphic Encryption Scheme Based on Domestic Cryptographic Algorithm SM9

计算机科学, 2025, 52(11): 408-414. <https://doi.org/10.11896/jsjcx.241100188>

### [国密算法SM9的性能优化方法](#)

Performance Optimization Method for Domestic Cryptographic Algorithm SM9

计算机科学, 2025, 52(6): 390-396. <https://doi.org/10.11896/jsjcx.240300141>

### [基于HotStuff的高效量子安全拜占庭容错共识机制](#)

Efficient Quantum-secure Byzantine Fault Tolerance Consensus Mechanism Based on HotStuff

计算机科学, 2024, 51(8): 429-439. <https://doi.org/10.11896/jsjcx.230600200>

### [基于符号执行优化的PDF恶意指标提取技术](#)

PDF Malicious Indicators Extraction Technique Based on Improved Symbolic Execution

计算机科学, 2024, 51(7): 389-396. <https://doi.org/10.11896/jsjcx.230300117>

# 基于国密算法 SM9 的环签名方案

谢振杰<sup>1,2</sup> 张耀<sup>1,3</sup> 杨启超<sup>1</sup> 宋恩舟<sup>1</sup>

1 信息工程大学网络空间安全教育部重点实验室 郑州 450001

2 中国人民解放军 78156 部队 重庆 400039

3 中国人民解放军新疆昌吉军分区 新疆 昌吉 831100

(jsonxie@126.com)

**摘要** 环签名具备自发性和匿名性,其在实现数字签名的同时保护了用户隐私,已被广泛应用于区块链、电子选举和数字货币交易等需要隐藏签名者真实身份的场景。基于标识的密码可避免复杂的公钥基础设施建设和公钥证书管理,具有更好的系统性能。以基于标识密码体制的国密算法 SM9 数字签名算法为基础,构造了满足一般系统模型和安全模型的环签名方案,在随机预言机模型下基于  $q$ -SDH 困难问题,证明了提出的方案具有 EUF-CMIA 安全性,即使在掌握系统主私钥的敌手面前也具备完全匿名性。理论分析和测试表明,该方案相较于现有同类方案具有明显性能优势,当环用户数量为 1024 时,签名和验证速率较同类方案分别提升 121% 和 111%,签名数据减少近 50%。

**关键词:** 国密算法; SM9; 环签名; 数字签名; 基于标识的密码

**中图分类号** TP309.7

## Ring Signature Scheme Based on Domestic Cryptographic Algorithm SM9

XIE Zhenjie<sup>1,2</sup>, ZHANG Yao<sup>1,3</sup>, YANG Qichao<sup>1</sup> and SONG Enzhou<sup>1</sup>

1 Key Laboratory of Cyberspace Security, Ministry of Education, Information Engineering University, Zhengzhou 450001, China

2 Troop 78156 of PLA, Chongqing 400039, China

3 Xinjiang Changji Military Subarea of PLA, Changji, Xinjiang 831100, China

**Abstract** Ring signatures possess spontaneity and anonymity, which can protect user privacy while implementing digital signatures. They have been widely used in scenarios requiring the concealment of the signer's true identity, such as blockchain, electronic voting, and digital currency transactions. Identity-based cryptography can avoid the complexity of public key infrastructure construction and public key certificate management, which offers better system performance. Based on the SM9 digital signature algorithm, an identity-based domestic cryptographic algorithm, this paper constructs a ring signature scheme that satisfies general system model and security model. In the random oracle model, it is proven that this scheme has EUF-CMIA security based on the  $q$ -SDH hard problem. It is also proven that this scheme maintains full anonymity even in the presence of adversaries with access to the system's master secret key. Theoretical analysis and testing indicates that this scheme has significant performance advantages over existing similar schemes. When the number of ring users is 1024, the signature and verification rates are improved by 121% and 111% respectively, and the signature data size is reduced by nearly 50%.

**Keywords** Domestic cryptographic algorithm, SM9, Ring signature, Digital signature, Identity-based cryptograph

环签名是一种由群签名简化而来的数字签名方案,最早由 Rivest 等<sup>[1]</sup>于 2001 年提出。环签名允许一个实际的签名者代表一个潜在的签名者群体(称为环)对消息进行数字签名,同时该签名者在环中保持匿名性。相较于有群管理员的群签名,环签名的成员之间是平等的,签名过程不需要环成员间的协作。环签名最初因其签名数据按照一定的规则组成环状而得名,后来许多方案设计了非环状的签名结构,但只要签名满足自发性和匿名性,也可归入环签名的范畴。环签名的

安全特性包括不可伪造性和匿名性,非常适合应用于区块链<sup>[2]</sup>、电子投票、数字货币<sup>[3]</sup>和匿名投诉等需要隐藏签名者身份的领域。Rivest 等<sup>[1]</sup>最初提出的环签名方案是基于 RSA 算法的,自从环签名的概念被提出以后,研究人员陆续设计了基于离散对数<sup>[4]</sup>、双线性对<sup>[5]</sup>、格理论<sup>[6]</sup>等不同密码学原语的环签名方案。

传统的环签名方案依赖公钥基础设施(Public Key Infrastructure, PKI),但 PKI 体制面临较为复杂的证书管理问题,

到稿日期:2024-10-15 返修日期:2025-01-24

基金项目:装备预先研究项目(30603010601)

This work was supported by the Equipment Pre Research Project(30603010601).

通信作者:杨启超(yangqichaoo@foxmail.com)

而环签名的签名和验证都需要大量申请证书以获取环用户公钥,尤其是环用户数量较多时,易导致系统性能受限,从而增加时间开销。为此,研究人员设计了基于标识的环签名方案,在一定程度上解决了 PKI 体制的性能问题。

国密算法 SM9 是我国自主设计的基于标识的密码体制 (Identity-based Cryptography, IBC),包含数字签名算法、密钥交换协议、密钥封装机制和加密算法<sup>[7-8]</sup>。IBC 将用户身份信息作为公钥,公钥的真实性无需通过第三方颁发的证书来确认,不用建立复杂的 PKI,显著降低了密码系统的运维成本。另外,SM9 基于椭圆曲线,相对于 RSA 等类型的公钥密码,具有更强的安全性,在同等安全强度下,其所需的密钥更短、计算效率更高。国密算法 SM9 作为一款自主可控且性能优异的标识密码,能很好地适配各类公钥密码应用需求。近年来,基于 SM9 设计各类标识密码方案已成为研究热点,除环签名外,研究人员陆续提出了基于 SM9 设计的可搜索加密<sup>[9]</sup>、分层标识加密<sup>[10-12]</sup>、广播加密<sup>[12-13]</sup>和容错加密<sup>[14]</sup>等标识密码应用方案。

本文以国密算法 SM9 的数字签名算法为基础,设计了一种基于标识的环签名方案,其系统初始化和用户签名私钥生成过程与 SM9 数字签名算法一致,完全兼容 SM9 国标规定的公共参数。在随机预言机模型下,证明了该方案具有不可伪造性和完全匿名性,满足一般环签名方案安全模型所定义的安全需求。定量分析与实验测试结果表明,该方案相较于同类方案,环签名生成与验证算法都具有明显性能优势,同时显著压缩了签名数据大小。

## 1 相关工作

2002 年,文献[5]首次提出基于标识的环签名方案,之后提出的标识环签名方案大多使用双线性对作为数学工具<sup>[15-17]</sup>。2010 年,文献[18]提出一种使用现有数字签名方案构造环签名方案的通用方法,签名数据围绕环用户形成环状结构,生成 1 个环签名消息的计算开销相当于执行  $n$  次传统数字签名 ( $n$  为环用户数量)的开销,这为后续环签名方案设计提供了有益参考,但这种构造模式会导致计算和通信开销随环用户数量呈线性增长。时空效率问题始终是影响环签名方案应用的重要因素,故之后出现的环签名方案更加注重提高计算效率并降低通信开销。

文献[19]首次将基于标识的国密算法 SM9 应用于环签名方案设计,提出了一种基于 SM9 的环签名方案,并与 SM9 数字签名算法保持良好的兼容性,其通信开销优于此前提出的环签名方案,但计算开销更大。文献[20]针对车联网匿名认证需求,提出了 2 个基于 SM9 的环签名算法。文献[21]提出了基于 SM9 的门限环签名方案,将国密算法与门限环签名相结合,但其签名验证算法中的双线性对次数与门限值成正比,计算效率仍有较大优化空间。文献[22]设计了基于 SM9 盲签名与环签名的安全电子选举协议,然而其环签名验证算法的输入并不包含由签名者私钥产生的元素,故可通过重放攻击伪造签名。文献[23]提出了基于 SM9 和动态累加器的常数级签名大小的环签名方案,引入大小与最大环用户数量成正比的累加器元组,以扩充公共参数为代价实现了签名和

验证开销不随环用户数量变化。但其设计思路和计算过程相对复杂,当环用户数量大于 20 时才能体现出相对于文献[19]在通信开销上的优势;此外,其安全性证明尚不够充分。

对于环签名方案安全性的分析:文献[24]首次提出了用于证明数字签名方案安全性的分叉引理(Forking Lemma);文献[25]提出了在随机预言机模型下证明一般环签名方案安全性的分叉引理;文献[26]将分叉引理扩展到一般的基于身份的签名体制;文献[27]使用分叉引理,给出了对一般基于身份环签名体制的安全性证明;文献[28]基于  $q$ -SDH 假设和随机预言机模型,证明了 SM9 数字签名算法具有 EUF-CMIA 的安全性。

## 2 基于标识的环签名概述

本章介绍基于标识环签名所依赖的数学困难问题,以及一般的基于标识环签名方案的系统模型和安全模型。

### 2.1 困难问题

令  $P, Q$  分别为群  $G_1, G_2$  的生成元,且满足  $P = \psi(Q)$  ( $\psi$  为  $G_2$  到  $G_1$  的同态映射),群  $G_1, G_2$  的阶为  $N$ ,则在非对称双线性群上定义  $q$ -SDH 问题如下<sup>[28]</sup>:

**定义 1** ( $q$ -Strong Diffie-Hellman Problem,  $q$ -SDH 问题) 对于未知的正整数  $a \in [1, N-1]$ ,给定  $q+2$  个元素  $(P, Q, [a]Q, [a^2]Q, \dots, [a^q]Q) \in G_1 \times G_2^{q+1}$ ,计算  $(c, [\frac{1}{c+a}]P)$ ,其中  $c$  是  $[0, N-1]$  内的任意整数。

若在多项式时间内求解  $q$ -SDH 问题的概率是可忽略的,则称  $q$ -SDH 问题的困难性假设成立。

### 2.2 系统模型

一个典型的基于标识的环签名方案通常由系统建立 Setup、用户签名私钥生成 KeyGen、环签名生成 RingSign 和环签名验证 RingVerify 这 4 项算法构成<sup>[19]</sup>。方案包含 3 种角色:密钥生成中心(Key Generation Center, KGC)运行 Setup 算法完成系统初始化、运行 KeyGen 算法为用户生成签名私钥,签名者(Signer)和验证者(Verifier)分别运行 RingSign 和 RingVerify 算法。

1) 系统建立  $\text{Setup}(\lambda) \rightarrow (params, msk)$ :由 KGC 运行的概率多项式时间(Probabilistic Polynomial Time, PPT)算法,输入安全参数  $\lambda$ ,输出系统公开参数  $params$  和签名主私钥  $msk$ 。

以下算法的输入都包含  $params$ ,为简化描述不再额外标注。

2) 用户签名私钥生成  $\text{KeyGen}(ID, msk) \rightarrow ds$ :由 KGC 运行的确定性算法,输入用户身份标识  $ID$  和签名主私钥  $msk$ ,输出用户签名私钥  $ds$ 。

3) 环签名生成  $\text{RingSign}(M, U_n, ds) \rightarrow \sigma$ :由签名者(标识为  $ID_\pi, 1 \leq \pi \leq n, n$  为环用户数量)运行的 PPT 算法,输入待签名消息  $M$ 、环用户集合  $U_n = \{ID_1, ID_2, \dots, ID_n\}$  和签名私钥  $ds$ ,输出环签名消息  $\sigma$ 。

4) 环签名验证  $\text{RingVerify}(M, U_n, \sigma) \rightarrow \text{accept/reject}$ :由验证者运行的确定性算法,输入被签名消息  $M$ 、环用户集合  $U_n = \{ID_1, ID_2, \dots, ID_n\}$  和环签名消息  $\sigma$ ,验证通过则输出

accept, 否则输出 reject。

方案的正确性要求如下: 对于合法的签名, 验证通过的

$$\Pr \left[ \begin{array}{l} \text{RingVerify}(M, U_n, \sigma) = \text{accept} \\ \left[ \begin{array}{l} \text{Setup}(\lambda) \rightarrow (\text{params}, \text{msk}) \\ \text{KeyGen}(ID, \text{msk}) \rightarrow ds \\ \text{RingSign}(M, U_n, ds) \rightarrow \sigma \end{array} \right] = 1 \end{array} \right]$$

### 2.3 安全模型

基于标识的环签名方案, 须满足以下 2 个安全特性<sup>[29]</sup>:

1) 在自适应选择消息和身份攻击下的存在性不可伪造 (Existential Unforgeability under Adaptive Chosen-message-and-Identity Attack, EUF-CMIA); 2) 匿名性。

**定义 2 (EUF-CMIA)** 该性质由挑战者  $C$  与 PPT 敌手  $A$  之间的游戏来定义, 游戏过程分为以下 3 个阶段。

1) 初始化。挑战者  $C$  调用 Setup 生成系统公开参数  $\text{params}$  和签名主私钥  $\text{msk}$ , 将  $\text{params}$  发送给敌手  $A$ 。

2) 询问。A 以自适应的方式向  $C$  发起私钥询问和签名询问。

(1) 私钥询问。A 询问身份标识  $ID$ ,  $C$  调用 KeyGen 生成对应的用户签名私钥  $ds$  并返回。

(2) 签名询问。A 询问消息  $M$  和环用户集合  $U_n = \{ID_1, ID_2, \dots, ID_n\}$ ,  $C$  从  $U_n$  中随机选择标识  $ID_\pi (1 \leq \pi \leq n)$ , 调用 KeyGen 生成其签名私钥  $ds_\pi$ , 再调用 RingSign 生成  $U_n$  对  $M$  的环签名消息  $\sigma$  并返回。

(3) 伪造。A 伪造挑战用户集合  $U^* = \{ID_1^*, ID_2^*, \dots, ID_t^*\}$  对消息  $M^*$  的环签名消息  $\sigma^*$ , 要求 A 从未询问过  $U^*$  中任一用户的签名私钥, 也从未询问过  $U^*$  对  $M^*$  的签名。如果 A 伪造的签名  $\sigma^*$  能在 RingVerify 算法下通过验证, 则 A 赢得游戏。

定义 A 赢得该游戏的优势为  $\text{Adv}_A^{\text{EUF}} = \Pr[\text{RingVerify}(M^*, U^*, \sigma^*) = \text{accept}]$ 。如果对于任意 PPT 敌手  $A$ , 该优势是可以忽略的, 则称该环签名方案是 EUF-CMIA 安全的。

**定义 3 (匿名性)** 该性质由挑战者  $C$  与 PPT 敌手  $A$  之间的游戏来定义, 游戏过程分为以下 4 个阶段。

1) 初始化。挑战者  $C$  调用 Setup 生成系统公开参数  $\text{params}$  和签名主私钥  $\text{msk}$ , 将  $\text{params}$  发送给敌手  $A$ 。

2) 询问。A 以自适应的方式向  $C$  发起私钥询问和签名询问。

(1) 私钥询问。A 询问身份标识  $ID$ ,  $C$  调用 KeyGen 生成对应的用户签名私钥  $ds$  并返回。

(2) 签名询问。A 询问消息  $M$  和环用户集合  $U_n = \{ID_1, ID_2, \dots, ID_n\}$ ,  $C$  从  $U_n$  中随机选择标识  $ID_\pi (1 \leq \pi \leq n)$ , 调用 KeyGen 生成其签名私钥  $ds_\pi$ , 再调用 RingSign 生成  $U_n$  对  $M$  的环签名消息  $\sigma$  并返回。

3) 挑战。A 向  $C$  提供挑战用户集合  $U^* = \{ID_1^*, ID_2^*, \dots, ID_t^*\}$ 、消息  $M^*$  和 2 个标识  $ID_{\pi_1}, ID_{\pi_2} \in U^*$ ,  $C$  随机选择  $b \in \{0, 1\}$ , 调用 KeyGen 生成  $ID_{\pi_b}$  对应的签名私钥  $ds_{\pi_b}$ , 再调用 RingSign 生成  $U^*$  对  $M^*$  的环签名消息  $\sigma^*$  并返回给  $A$ 。

4) 猜测。A 输出  $b' \in \{0, 1\}$ , 如果  $b' = b$ , 则 A 赢得游戏。

定义 A 赢得该游戏的优势为  $\text{Adv}_A^{\text{ANON}} = \left| \Pr[b' = b] - \frac{1}{2} \right|$ 。如果对于任意 PPT 敌手  $A$ , 该优势是可以

忽略的, 则称该环签名方案满足匿名性。

## 3 基于 SM9 的环签名方案构造

本章对所设计环签名方案的各项算法进行详细描述。本文的符号含义与 SM9 国标<sup>[7-8]</sup>一致。  $G_1, G_2$  是椭圆曲线加法循环群;  $P_1, P_2$  分别是群  $G_1, G_2$  的生成元;  $G_T$  是乘法循环群 (其元素均为有限域 12 次扩域上的元素);  $e(a, b)$  表示从  $G_1 \times G_2$  到  $G_T$  的双线性对;  $[k]P$  表示椭圆曲线点  $P$  的  $k$  倍 (即椭圆曲线标量乘);  $x \parallel y$  表示  $x$  与  $y$  的字节串拼接;  $H_1, H_2$  是将任意长度比特串映射到  $[1, N-1]$  内整数的哈希函数。

### 3.1 系统建立 Setup

首先, 由 KGC 产生随机数  $ks \in [1, N-1]$  作为签名主私钥, 计算群  $G_2$  中的元素  $P_{\text{pub-s}} = [ks]P_2$  作为签名主公钥, 则签名主密钥对为  $(ks, P_{\text{pub-s}})$ 。KGC 秘密保存  $ks$ , 公开  $P_{\text{pub-s}}$ 。KGC 选择并公开大小为 1 B 的签名私钥生成函数识别符  $hid$ 。

### 3.2 用户签名私钥生成 KeyGen

用户  $A$  的标识为  $ID_A$ , 为产生用户  $A$  的签名私钥  $ds_A$ , KGC 首先在有限域  $F_N$  上计算  $t_1 = H_1(ID_A \parallel hid, N) + ks$ 。若  $t_1 = 0$ , 则需重新产生系统签名主密钥, 并更新已有用户的签名私钥; 否则计算  $t_2 = ks \cdot t_1^{-1}$ , 再计算  $ds_A = [t_2]P_1$ 。最后将签名私钥  $ds_A$  通过安全途径传递给用户  $A$ 。

### 3.3 环签名生成 RingSign

设环用户集合  $U_n = \{ID_1, ID_2, \dots, ID_n\}$ , 待签名的消息为比特串  $M$ , 签名者的标识为  $ID_\pi (1 \leq \pi \leq n)$ , 生成环签名消息  $\sigma$  的运算步骤如下。

1) 计算群  $G_T$  中的元素  $g_0 = e(P_1, P_{\text{pub-s}})$ ,  $g_1 = e(ds_\pi, P_2)$ ,  $g_2 = e(ds_\pi, P_{\text{pub-s}})$ 。

2) 产生随机数  $r, r_0 \in [1, N-1]$ , 计算群  $G_T$  中的元素  $\omega_{\pi+1} = g_0^{r_0}$ 。

3) 计算整数  $h_{\pi+1} = H_2(U_n \parallel M \parallel \omega_{\pi+1}, N)$ 。

4) 令  $i = \pi + 1$ , 以下步骤循环执行  $n-1$  次:

(1) 若  $i > n$ , 则令  $i = 1, h_1 = h_{n+1}$ ;

(2) 计算整数  $v_i = H_1(ID_i \parallel hid, N)$ ;

(3) 产生随机数  $r_i \in [1, N-1]$ , 计算群  $G_T$  中的元素

$$\omega_{i+1} = g_1^{r_i v_i} \cdot g_2^{r_i} \cdot g_0^{h_i};$$

(4) 计算整数  $h_{i+1} = H_2(U_n \parallel M \parallel \omega_{i+1}, N)$ ;

(5) 令  $i = i + 1$ 。

5) 计算整数  $r_\pi = (r r_0 - h_\pi) r^{-1}$ , 若  $r_\pi = 0$  则返回步骤 2)。

6) 计算群  $G_1$  中的元素  $S = [r]ds_\pi$ 。

7) 输出环签名消息  $\sigma = (h_1, S, r_1, r_2, \dots, r_n)$ 。

上述环签名步骤中, 由于签名主公钥和用户签名私钥是固定的, 因此步骤 1) 产生的  $g_0, g_1, g_2$  是常量, 可预先计算并保存, 故实际运行过程可省略步骤 1)。

### 3.4 环签名验证 RingVerify

验证者收到环用户集合  $U_n$  对消息  $M'$  的环签名消息  $\sigma' = (h_1', S', r_1', r_2', \dots, r_n')$  后, 执行以下运算步骤。

1) 检验  $h_1', r_1', r_2', \dots, r_n' \in [1, N-1]$  和  $S' \in G_1$  是否完全成立, 若不完全成立则验证不通过。

2) 计算群  $G_T$  中的元素  $g_0 = e(P_1, P_{\text{pub-s}}), g_3 = e(S', P_2), g_4 = e(S', P_{\text{pub-s}})$ 。

3) 令  $i=1$ , 以下步骤循环执行  $n$  次:

(1) 计算整数  $v_i = H_1(ID_i \parallel hid, N)$ ;

(2) 计算群  $G_T$  中的元素  $\omega'_{i+1} = g_3^{v_i} \cdot g_4^{r_i'} \cdot g_0^{h_i'}$ ;

(3) 计算整数  $h'_{i+1} = H_2(U_n \parallel M' \parallel \omega'_{i+1}, N)$ ;

(4) 令  $i=i+1$ 。

4) 检验  $h_1' = h'_{n+1}$  是否成立, 若成立则验证通过, 否则验证不通过。

同理, 步骤 2) 的  $g_0$  可预先计算并保存。

## 4 方案性质推导与证明

本章通过理论推导, 证明本文方案的正确性, 并以形式化的安全分析证明本文方案具有不可伪造性和匿名性。

### 4.1 正确性

如果签名者和验证者诚实地执行上述运算步骤, 且环用户集合  $U_n$ 、消息  $M'$  和环签名消息  $\sigma'$  在传输过程中未被篡改, 即  $M=M', h_1=h_1', S=S', r_i=r_i' (1 \leq i \leq n)$ , 则方案的正确性来自以下推导。

1) 当  $1 \leq i < \pi$  时, 由于  $h_1 = h_1'$ , 则有  $h_{i+1} = h'_{i+1}$ 。

2) 当  $i = \pi$  时, 由于  $h_\pi = h_\pi', rr_\pi = rr_0 - h_\pi$ , 则下式成立:

$$\begin{aligned} \omega'_{\pi+1} &= g_3^{r_\pi' v_\pi} \cdot g_4^{r_\pi'} \cdot g_0^{h_\pi'} \\ &= e(S, P_2)^{r_\pi v_\pi} \cdot e(S, P_{\text{pub-s}})^{r_\pi} \cdot g_0^{h_\pi} \\ &= e([rr_\pi v_\pi] ds_\pi, P_2) \cdot e([rr_\pi] ds_\pi, [ks] P_2) \cdot g_0^{h_\pi} \\ &= e([rr_\pi (v_\pi + ks)] ds_\pi, P_2) \cdot g_0^{h_\pi} \\ &= e([(rr_0 - h_\pi)(v_\pi + ks) ks (v_\pi + ks)^{-1}] P_1, P_2) \cdot g_0^{h_\pi} \\ &= e([(rr_0 - h_\pi) ks] P_1, P_2) \cdot g_0^{h_\pi} \\ &= g_0^{rr_0 - h_\pi} \cdot g_0^{h_\pi} = g_0^{rr_0} = \omega_{\pi+1} \end{aligned}$$

故  $h_{\pi+1} = h'_{\pi+1}$ 。

3) 当  $\pi < i \leq n$  时, 由于  $h_i = h_i'$ , 则有  $h_{i+1} = h'_{i+1}$ , 故  $h_{n+1} = h'_{n+1}$ 。又因  $h_1 = h_{n+1}$ , 最终可得  $h_1' = h'_{n+1}$ 。

因此, 本文提出的环签名方案是正确的。

### 4.2 不可伪造性

下文运用形式化的安全规约方法证明所提环签名方案具有 EUF-CMIA 安全性。

**定理 1** 假设哈希函数  $H_1$  和  $H_2$  是随机预言机, 如果  $q$ -SDH 问题是困难的, 则本文所提环签名方案在 EUF-CMIA 安全模型下是安全的。

证明: 假设在 EUF-CMIA 安全模型下, 存在一个 PPT 敌手  $A$  能以不可忽略的优势  $\epsilon$  伪造本文方案签名, 则可构建模拟器  $B$  解决  $q$ -SDH 问题。  $B$  以 1 个  $q$ -SDH 问题实例  $(P, Q, [a]Q, [a^2]Q, \dots, [a^q]Q) \in G_1 \times G_2^{q+1}$  作为输入, 控制随机预言机并运行  $A$ , 进行以下操作。

1) 初始化。令  $\psi$  为  $G_2$  到  $G_1$  的同态映射, 满足  $[a^i]P = \psi([a^i]Q), 0 \leq i \leq q$ ; 模拟器  $B$  随机选择  $q+1$  个互不相同的数

$\omega^*, \omega_1, \omega_2, \dots, \omega_q \in [1, N-1]$ , 令  $f(x) = \prod_{i=1}^q (\omega_i + x), f(x)$  是  $Z_N[x]$  中次数为  $q$  的多项式; 设  $P_1 = [f(a)]P, P_2 = Q, P_{\text{pub-s}} = [a]Q$ 。除了签名主私钥  $ks = a$  是隐式的, 其余公开参数可通过问题实例和所选参数计算得到。

2) 哈希询问。哈希函数  $H_1, H_2$  是由  $B$  控制的随机预言机, 询问次数 (相同询问不重复计数) 分别为  $q_{H_1}, q_{H_2}$ , 假设  $q = q_{H_1}$ 。为方便描述, 省略  $H_1, H_2$  中  $hid$  和  $N$  的输入。开始询问前,  $B$  随机选择  $i^* \in [1, q_{H_1}]$ , 并建立 2 个初始为空的哈希列表  $L_1, L_2$ , 分别记录对  $H_1, H_2$  的询问和应答。  $A$  可以在任意阶段向  $B$  发起以下哈希询问:

(1)  $H_1$  询问。令第  $i$  个  $H_1$  询问为  $ID_i$ , 若  $L_1$  中已有  $ID_i$  对应项, 则  $B$  根据  $L_1$  的记录来应答。否则, 当  $i = i^*$  时, 设  $H_1(ID_i) = \omega^*$ ;  $i \neq i^*$  时, 设  $H_1(ID_i) = \omega_i$ 。  $B$  将  $H_1(ID_i)$  作为该询问的应答, 并在  $L_1$  中记录  $(i, ID_i, H_1(ID_i))$ 。

(2)  $H_2$  询问。令第  $i$  个  $H_2$  询问为环用户集合  $U_i$ 、消息  $M_i$  和群  $G_T$  中的元素  $y_i$ , 若  $L_2$  中已有其对应项, 则  $B$  根据  $L_2$  的记录来应答。否则,  $B$  随机选择  $Y_i \in [1, N-1]$ , 将  $H_2(U_i \parallel M_i \parallel y_i) = Y_i$  作为该询问的应答, 并在  $L_2$  中记录  $(i, U_i, M_i, y_i, Y_i)$ 。

3) 询问。在此阶段,  $A$  以自适应的方式向  $B$  发起私钥询问和签名询问。

(1) 私钥询问。  $A$  询问身份标识  $ID_i$  的签名私钥, 令  $(i, ID_i, H_1(ID_i))$  为  $L_1$  中对应的记录。若  $i = i^*$ , 则中止; 否则, 有  $H_1(ID_i) = \omega_i$ 。令  $f_i(x) = x \prod_{j=1, j \neq i}^q (\omega_j + x)$ , 则  $f_i(x)$  是  $Z_N[x]$  中次数为  $q$  的多项式, 利用问题实例和所选参数可计算签名私钥  $ds_i = [f_i(a)]P$ 。由于:

$$ds_i = [f_i(a)]P = \left[ \frac{a \cdot f(a)}{\omega_i + a} \right] P = \left[ \frac{a}{\omega_i + a} \right] P_1$$

因此  $ds_i$  是一个有效的签名私钥。

(2) 签名询问。  $A$  询问环用户集合  $U_j$  对消息  $M$  的签名  $\sigma$ 。  $B$  从  $U_j$  中随机选择标识  $ID_\pi (\pi \neq i^*)$ , 生成其签名私钥  $ds_\pi$ , 再调用 RingSign 生成  $U_j$  对  $M$  的环签名消息  $\sigma$  并返回。

4) 伪造。  $A$  伪造挑战用户集合  $U^* = \{ID_1^*, ID_2^*, \dots, ID_n^*\}$  对消息  $M^*$  的环签名消息  $\sigma^*$ , 要求  $A$  从未询问过  $U^*$  中任一用户的签名私钥, 也从未询问过  $U^*$  对  $M^*$  的签名。若  $ID_i^* \notin U^*$ , 则中止; 否则, 根据分叉引理, 在不掌握  $U^*$  中任一用户签名私钥的情况下, 如果存在 PPT 敌手  $A$  能成功伪造环签名消息  $\sigma^*$ , 则  $B$  可构造一个图灵机  $A'$  通过多次运行  $A$ , 以相同的输入  $(M^*, U^*)$  得到 2 个有效的环签名消息  $\sigma_1^* (h_{1,1}^*, S^*, r_1^*, \dots, r_{\pi-1}^*, r_{\pi,1}^*, r_{\pi+1}^*, \dots, r_n^*)$  和  $\sigma_2^* (h_{1,2}^*, S^*, r_1^*, \dots, r_{\pi-1}^*, r_{\pi,2}^*, r_{\pi+1}^*, \dots, r_n^*)$ , 满足  $h_{1,1}^* \neq h_{1,2}^*, r_{\pi,1}^* \neq r_{\pi,2}^*$ 。若  $ID_\pi^* \neq ID_i^*$ , 则中止; 否则, 令  $\frac{x \cdot f(x)}{\omega^* + x} = F(x) + \frac{d}{\omega^* + x}$ 。其中  $F(x)$  是  $Z_N[x]$  中次数为  $q$  的多项式,  $d$  是非零整数,  $F(x)$  的各项系数和  $d$  均可通过所选参数计算。由于  $ID_\pi^* = ID_i^*$ , 则  $H_1(ID_\pi^*) = \omega^*$ 。  $B$  调用 RingVerify 计算得到  $h_{\pi,1}^*, h_{\pi,2}^*$ , 再计算  $W^* = \left[ \frac{1}{d} \right] \left( \left[ \frac{r_{\pi,1}^* - r_{\pi,2}^*}{h_{\pi,2}^* - h_{\pi,1}^*} \right] S^* - [F(a)]P \right)$ , 输出  $(\omega^*, W^*)$  作为  $q$ -SDH 问题实例的解。由于  $r_{\pi,1}^* = \frac{r^* r_0^* - h_{\pi,1}^*}{r^*}, r_{\pi,2}^* =$

$$\frac{r^* r_0^* - h_{\pi_2}^*}{r^*}, S^* = [r^*] d_{S\pi} = \left[ \frac{r^* a}{w^* + a} \right] P_1 = \left[ \frac{r^* a \cdot f(a)}{w^* + a} \right] P,$$

因此有:

$$\begin{aligned} W^* &= \left[ \frac{1}{d} \right] \left( \left[ \frac{r_{\pi_1}^* - r_{\pi_2}^*}{h_{\pi_2}^* - h_{\pi_1}^*} \right] S^* - [F(a)] P \right) \\ &= \left[ \frac{1}{d} \left( \frac{(r^* r_0^* - h_{\pi_2}^*) - (r^* r_0^* - h_{\pi_2}^*)}{r^* (h_{\pi_2}^* - h_{\pi_1}^*)} \cdot \right. \right. \\ &\quad \left. \left. \frac{r^* a \cdot f(a)}{w^* + a} - F(a) \right) \right] P \\ &= \left[ \frac{1}{d} \left( \frac{a \cdot f(a)}{w^* + a} - F(a) \right) \right] P \\ &= \left[ \frac{1}{d} \left( F(a) + \frac{d}{w^* + a} - F(a) \right) \right] P \\ &= \left[ \frac{1}{w^* + a} \right] P \end{aligned}$$

故 $(w^*, W^*)$ 可作为 $q$ -SDH问题实例的一个解。

以下是对 $B$ 成功模拟概率和破解 $q$ -SDH问题优势的分析。只有当 $A$ 伪造签名私钥的标识 $ID_{\pi^*}$ 在 $L_1$ 中的序号恰好为 $i^*$ 时, $B$ 才能成功模拟并计算 $q$ -SDH问题实例的解,其概率为 $1/q_{H_1}$ ,而 $q_{H_1}$ 是多项式级别且有上界,所以此概率是不可忽略的。因此,若 $A$ 能以不可忽略的优势 $\epsilon$ 伪造本文方案签名,则 $B$ 能以 $\epsilon/q_{H_1}$ 的优势成功求解 $q$ -SDH问题,该优势同样是不可忽略的。然而,这与 $q$ -SDH问题的困难性假设相矛盾,故本文环签名方案在EUF-CMIA安全模型下是安全的。

### 4.3 匿名性

在匿名性方面,考虑KGC为恶意敌手的情况,保证即使敌手知道系统主私钥,也无法确认环签名消息的真实签名者,即本文方案具备完全匿名性。

**定理2** 如果方案采用的随机数源满足均匀分布,则本文环签名方案具有匿名性。

**证明:**假设 $\sigma$ 是环用户集合 $U_n = \{ID_1, ID_2, \dots, ID_n\}$ 对消息 $M$ 的环签名消息,且 $\sigma = (h_1, S, r_1, r_2, \dots, r_n)$ 由签名者 $ID_{\pi_1}$  ( $1 \leq \pi_1 \leq n$ )生成。令 $v_i = H_1(ID_i)$  ( $1 \leq i \leq n$ ),根据本文

环签名方案, $r_{\pi_1} = \frac{rr_0 - h_{\pi_1}}{r}$ ,  $S = [r] d_{S\pi_1} = \left[ \frac{r \cdot ks}{v_{\pi_1} + ks} \right] P_1$ 。而 $\sigma$

同样可视为由签名者 $ID_{\pi_2}$  ( $1 \leq \pi_2 \leq n$ 且 $\pi_2 \neq \pi_1$ )生成,这是因为

$S = \left[ \frac{r \cdot ks}{v_{\pi_1} + ks} \right] P_1 = \left[ \frac{r(v_{\pi_2} + ks)}{v_{\pi_1} + ks} \cdot \frac{ks}{v_{\pi_2} + ks} \right] P_1$ , 令 $r' =$

$\frac{r(v_{\pi_2} + ks)}{v_{\pi_1} + ks}$ , 则 $S = \left[ \frac{r' \cdot ks}{v_{\pi_2} + ks} \right] P_1$ , 此时 $r_{\pi_2}$ 可视为 $r_{\pi_2} =$

$\frac{r' r_0' - h_{\pi_2}}{r'}$ , 则 $r_0' = \frac{r_{\pi_2} r' + h_{\pi_2}}{r'}$ 。当方案采用的随机数源满足

均匀分布时,由签名者 $ID_{\pi_1}$ 在签名过程中产生的 $n+1$ 个随机数 $(r, r_0, r_1, \dots, r_{\pi_1-1}, r_{\pi_1+1}, \dots, r_n)$ 是随机且独立的;假设 $\sigma$ 的签名者是 $ID_{\pi_2}$ ,其在签名过程中产生的 $n+1$ 个随机数 $(r', r_0', r_1, \dots, r_{\pi_2-1}, r_{\pi_2+1}, \dots, r_n)$ 同样是随机且独立的。因此,即使在具有无限计算能力的敌手看来, $\sigma$ 由 $ID_{\pi_1}$ 或 $ID_{\pi_2}$ 生成的概率是相等的,即敌手在判断 $\sigma$ 的签名者是 $ID_{\pi_1}$ 还是 $ID_{\pi_2}$ 时无任何优势。进一步地, $\sigma$ 的实际签名者在集合 $U_n$ 内具有不可区分性,即本文环签名方案满足匿名性。

## 5 性能分析与实验

本章通过理论分析和编程实验,对本文方案的计算和通

信开销与同类方案展开对比分析。

### 5.1 性能分析

首先定量分析本文方案的计算和通信开销,并与文献[16,17,19]提出的方案进行对比。对于计算开销,考虑用户签名私钥生成、环签名生成和环签名验证3项算法中各项耗时运算的次数(可预计算完成的步骤未计入),对比分析结果如表1所列。其中, $SM_1, SM_2$ 分别表示群 $G_1, G_2$ 上的标量乘运算, $BP$ 表示双线性对运算, $E$ 表示群 $G_T$ 上的幂运算, $HTP$ 表示将比特串通过哈希映射到椭圆曲线点的HashToPoint运算。经实测,其余运算(如有限域 $F_N$ 上的模逆、群 $G_1$ 和 $G_2$ 上的加法、群 $G_T$ 上的乘法以及哈希运算 $H_1, H_2$ 等)耗时与上述运算至少相差2个数量级,为突出分析重点已将它们忽略。

表1 环签名方案的计算开销

Table 1 Calculation overhead of ring signature schemes

方案	私钥生成	环签名生成	环签名验证
文献[16]	$HTP$	$SM_1 + (n-1)SM_2 + (n+1)BP$	$nSM_2 + 2BP$
文献[17]	$HTP$	$nHTP + 2nSM_2$	$nSM_2 + 2BP$
文献[19]	$SM_1$	$(n+1)SM_1 + (n-1)SM_2 + (n-1)E + nBP$	$nSM_2 + nE + nBP$
本文方案	$SM_1$	$SM_1 + (3n-2)E$	$3nE + 2BP$

相较于同样基于SM9的文献[19]方案,本文方案通过优化算法设计,更多使用 $G_T$ 上固定基的幂运算,在环签名生成过程中避免了耗时更大的双线性对运算,在环签名验证过程中将双线性对运算由 $n$ 次减少到2次。通过文献[30]所提优化方法, $G_T$ 上固定基的幂运算耗时可显著减少,而文献[19]方案耗时主要来自双线性对,优化效果有限(文献[31]体现了SM9双线性对运算优化的最新成果)。故本文方案在环签名生成和验证的计算性能上相较于文献[19]方案,具有较大优势。

对于通信开销,考虑系统公钥、用户私钥和环签名数据的比特位数,对比分析结果如表2所列。其中 $|G_1|, |G_2|, |G_T|, |F_N|$ 分别表示对应群(或域)元素的比特位数。具体而言,对于SM9国标规范使用的256b的BN曲线<sup>[7]</sup>, $|G_1| = 512b, |G_2| = 1024b, |G_T| = 3072b, |F_N| = 256b$ 。SM9国标已做规定的 $P_1, P_2$ 等公共参数未计入系统公钥。

表2 环签名方案的通信开销

Table 2 Communication overhead of ring signature schemes

方案	系统公钥	用户私钥	环签名数据
文献[16]	$ G_2 $	$ G_1 $	$n G_T  +  G_1  + n F_N $
文献[17]	$ G_2 $	$ G_1 $	$(n+1) G_2 $
文献[19]	$ G_2 $	$ G_1 $	$n G_1  +  F_N $
本文方案	$ G_2 $	$ G_1 $	$ G_1  + (n+1) F_N $

可见,各方案的系统公钥和用户私钥长度均相同。相较于文献[19]方案,本文方案的环签名数据以 $n$ 个 $F_N$ 元素代替 $n$ 个 $G_1$ 元素,当 $n$ 较大时,传递环签名数据的通信开销降低近一半。事实上,文献[19]方案和本文方案的系统建立与用户签名私钥生成2项算法与标准SM9数字签名算法是完全一致的,因此,这2个环签名方案均可在运行标准SM9数字签名算法的系统中直接应用,而不必重新生成系统公钥和用户私钥。

### 5.2 实验测试

本文基于国密算法开源Python库hggm<sup>[32]</sup>的SM9模

块,通过 Python 编程实现了文献[19]方案和本文方案,在对比测试中重点关注环签名生成和验证的计算效率,以验证本方案的有效性 with 性能优势。实验计算机的配置如表 3 所列。

当环用户数量分别为 4, 16, 64, 256, 1024 时,测试文献[19]方案和本文方案的环签名生成与环签名验证耗时,测试结果如表 4 所列。以文献[19]方案为基准,本文方案的相对速率(文献[19]方案耗时/本文方案耗时)如图 1 所示。预计算的步骤已提前完成,测试数据不含预计算耗时。两套方案均应用了文献[30,31]方法,尽可能优化  $G_T$  上固定基的幂和双线性对等运算。优化所需的额外数据在预计算阶段获取。

各项算法均执行 500 次,取平均值为有效数据。

表 3 实验计算机配置

Table 3 Configuration of experimental computer

项目	配置
设备类型	PC
操作系统	Windows 10 64 位
CPU	Intel Core i3-10110U(2 核心 4 线程)
内存	8 GB LPDDR3 2133 MHz
硬盘	SAMSUNG MZVLB512HBJQ-000L7
Python 版本	3.7.1

表 4 各项算法测试结果

Table 4 Test results of algorithms

(ms)

方案	算法	环用户数量				
		4	16	64	256	1024
文献[19]	环签名	118.33	491.86	2067.99	8377.71	33811.28
本文方案	生成	50.56	217.87	887.06	3736.40	15322.08
文献[19]	环签名	120.96	485.08	2025.57	8175.67	32848.66
本文方案	生成	195.70	364.03	1077.46	4104.04	15540.95

由表 4 和图 1 数据可知,本文方案环签名生成的计算效率为文献[19]方案的 2.21~2.34 倍,其优势与环用户数量的相关性不明显;而对于环签名验证,随着环用户数量由 4 增加至 1024,本文方案相较于文献[19]方案的相对速率由 0.62 增加至 2.11,这是因为应用文献[30]方法优化  $G_T$  上固定基的幂运算,需要对步骤 2)的  $g_3, g_4$  计算额外数据( $g_3, g_4$  由环签名数据计算而来,无法在预计算阶段获取),所以当环用户数量越大时,优化所带来的性能优势越明显。

且具有更小的签名数据从而降低了通信开销。本文方案较现有方案更加高效、实用,对于提高环签名计算的性能具有理论价值和实践意义。但本文方案的签名和验证开销以及签名数据长度仍与环用户数量成正比,下一步将继续基于 SM9 数字签名算法,设计一个常数级环签名方案,实现计算和通信开销不随环用户数量线性增长。

本文方案实现与测试的全部 Python 代码,已在“码云”平台开源<sup>[32]</sup>。

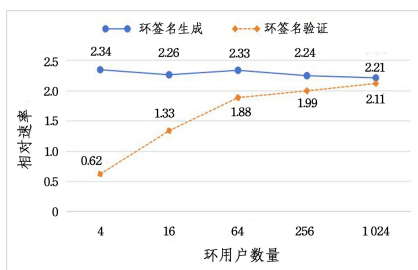


图 1 本文方案相较于文献[19]方案的相对速率

Fig. 1 Relative velocity of the proposed scheme compared to the scheme in reference [19]

综上,本文方案相较于文献[19]方案在环签名生成与验证算法上具有明显的性能优势,当环用户数量大于 1000 时,前者计算效率为后者的 2 倍以上,前者传递环签名数据的通信开销约为后者的 50%。

**结束语** 本文基于国密算法 SM9 的数字签名算法,设计了一种高效的环签名方案。通过理论推导,证明了本文方案的正确性,以形式化的安全分析证明了本文方案具有 EUF-CMIA 安全性和完全匿名性,在随机预言机模型下满足一般环签名方案的系统模型和安全模型,是一个可证明安全的基于标识的环签名方案。通过理论分析和编程实现,重点对比了本文方案和文献[19]方案,二者都是基于 SM9 的环签名方案,但本文方案的签名算法避免了耗时的双线性对运算,验证算法将双线性对运算次数降为常数级,计算性能有明显优势,

### 参考文献

- [1] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C] // Proceedings of Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Berlin: Springer, 2001: 552-565.
- [2] LI X F, MEI Y R, GONG J, et al. A blockchain privacy protection scheme based on ring signature[J]. IEEE Access, 2020, 8: 76765-76772.
- [3] SUN S F, AU M H, LIU J K, et al. RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero[C] // Proceedings of Computer Security—ESORICS 2017. Cham: Springer, 2017: 456-474.
- [4] ABE M, MIYAKO O, KOUTAROU S. 1-out-of-n signatures from a variety of keys[C] // Proceedings of Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Berlin: Springer, 2002: 415-432.
- [5] ZHANG F G, KWANGJO K. ID-based blind signature and ring signature from pairings[C] // Proceedings of Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Berlin: Springer, 2002: 533-547.
- [6] JIA X Y, HE D B, XU Z Y, et al. An efficient identity-based ring signature scheme over a lattice[J]. Journal of Cryptologic Re-

- search, 2017, 4(4):392-404.
- [7] Identity-based cryptographic algorithms SM9-Part 1:General: GB/T 38635. 1-2020[S]. Beijing: National Information Security Standardization Technical Committee, 2020-04-28.
- [8] Identity-based cryptographic algorithms SM9-Part 2: Algorithms: GB/T 38635. 2-2020[S]. Beijing: National Information Security Standardization Technical Committee, 2020-04-28.
- [9] PU L, LIN C, WU W, et al. A public-key encryption with keyword search scheme from SM9[J]. Journal of Cyber Security, 2023, 8(1):108-118.
- [10] LAI J C, HUANG X Y, HE D B, et al. An efficient hierarchical identity-based encryption based on SM9[J]. SCIENTIA SINICA Informationis, 2023, 53(5):918-930.
- [11] LIU K, NING J T, WU W, et al. Multi-ciphertext batch auditable decryption outsourcing SM9-HIBE key encapsulation mechanism[J]. Journal on Communications, 2023, 44(12):158-170.
- [12] LI C, LIANG J K, DING Y J, et al. Hierarchical identity-based broadcast inner product functional encryption based on SM9[J]. SCIENTIA SINICA Informationis, 2024, 54(6):1400-1418.
- [13] CUI Y, HUANG X Y, LAI J C, et al. Anonymous broadcast encryption based on SM9[J]. Journal of Cyber Security, 2023, 8(6):15-27.
- [14] LIU X H, HUANG X Y, CHENG Z H, et al. Fault-tolerant identity-based encryption from SM9[J]. Science China(Information Sciences), 2024, 67(2):104-117.
- [15] LIN C Y, WU T C. An identity-based ring signature scheme from bilinear pairings[C]// Proceedings of 18th International Conference on Advanced Information Networking and Applications. IEEE, 2004:182-185.
- [16] HERRANZ J, SAEZ G. New identity-based ring signature schemes[C]// Proceedings of Information and Communications Security—ICICS 2004. Berlin: Springer, 2004:27-39.
- [17] CHOW S S M, YIU S M, HUI L C K. Efficient identity based ring signature[C]// Proceedings of Applied Cryptography and Network Security—ACNS 2005. Berlin: Springer, 2005: 499-512.
- [18] BRAKERSKI Z, KALAI Y T. A framework for efficient signatures, ring signatures and identity based encryption in the standard model[EB/OL]. <https://eprint.iacr.org/2010/086.pdf>.
- [19] 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.
- [20] BAO J B. Identity-based ring signcryption scheme based on SM9 algorithm[D]. Wuhan: Wuhan University, 2022.
- [21] DENG H M, PENG C G, DING H F, et al. A threshold ring signature scheme based on GM SM9 algorithm[J]. Computer Technology and Development, 2022, 32(12):95-102.
- [22] RAO J T, CUI Z. Secure e-voting protocol based on SM9 blind signature and ring signature[J]. Computer Engineering, 2023, 49(6):13-23, 33.
- [23] AN H Y, HE D B, BAO Z J, et al. Ring signature based on the SM9 digital signature and its application in blockchain privacy protection[J]. Journal of Computer Research and Development, 2023, 60(11):2545-2554.
- [24] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3):361-369.
- [25] HERRANZ J, SAEZ G. Forking lemmas for ring signature schemes[C]// Proceedings of Indocrypt'03, LNCS. Berlin: Springer, 2003:266-279.
- [26] ZHOU J, ZHANG Y J, ZHU Y F. Generic ID-based signature schemes and forking lemma[J]. Journal of Information Engineering University, 2007, 8(2):129-133.
- [27] ZHOU M, FU G, ZHOU Q. Proof of generic ID-based ring signature by forking lemma[J]. Communications Technology, 2008, 41(7):183-184, 188.
- [28] LAI J C, HUANG X Y, HE D B, et al. Security analysis of national secret SM9 digital signature and key encapsulation algorithm[J]. SCIENTIA SINICA Informationis, 2021, 51(11):1900-1913.
- [29] BENDER A, KATZ J, MORSELLI R. Ring signatures: Stronger definitions, and constructions without random oracles[J]. Journal of Cryptology, 2009, 22(1):114-138.
- [30] WANG J T, FAN R, HUANG Z. Fast implementation of high power operation in SM9[J]. Computer Engineering, 2023, 49(9):118-124, 136.
- [31] XIE Z J, LIU Y M, CAI R J, et al. Performance optimization method of domestic cryptographic algorithm SM9[J]. Computer Science, 2025, 52(6):390-396.
- [32] BASDDSA. Hggm—Domestic cryptographic algorithm SM2/SM3/SM4/SM9/ZUC—Complete source code for Python implementation[EB/OL]. (2024-07-11) [2024-07-11]. <https://gitee.com/basddsa/hggm>.



**XIE Zhenjie**, born in 1995, Ph.D candidate. His main research interests include cloud security and cryptography applications.



**YANG Qichao**, born in 1992, Ph.D candidate, lecturer. His main research interests include network security, protocol reverse analysis and vulnerability discovery.