基于国密算法SM9的可追踪环签名方案

谢振杰[1,2]，尹小康[1]，蔡瑞杰[1]，张耀[1,3]
（1.信息工程大学数学工程与先进计算国家重点实验室，河南 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）

摘　要：为解决数字签名用户的隐私保护问题，并防止恶意用户滥用完全匿名性，提出一种基于国密算法SM9的可追踪环签名方案。国密算法SM9是我国自主研发的标识密码算法，具有较高的安全性和良好的性能，避免了公钥基础设施的建设成本和证书管理开销。通过引入密码累加器，环签名的生成和验证过程的计算量以及签名数据大小均降低至常数级。在随机预言机模型下，基于q-SDH困难问题证明了该方案具有EUF-CMIA安全性，并证明了在出现争议时可追踪实际签名者的条件匿名性。理论分析和测试结果表明，该方案的签名和验证效率分别达到现有同类方案的7.3倍和3.3倍，签名数据大小约为其$\frac{1}{5}$，在计算效率和通信开销方面具有显著优势。

关键词：可追踪环签名；国密算法；SM9算法；密码累加器；基于标识的密码
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025041

Traceable ring signature scheme based on domestic cryptographic algorithm SM9

XIE Zhenjie[1,2], YIN Xiaokang[1], CAI Ruijie[1], ZHANG Yao[1,3]
1. State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China
2. Unit 78156 of the Chinese People's Liberation Army, Chongqing 400039, China
3. Xinjiang Changji Military Subarea of the Chinese People's Liberation Army, Changji 831100, China

Abstract: To address the privacy protection issues of digital signature users and prevent the misuse of complete anonymity by malicious users, a traceable ring signature scheme based on the domestic cryptographic algorithm SM9 was proposed. The SM9 algorithm was an identity-based cryptographic algorithm independently developed by China, which was characterized by high security and excellent performance, eliminating the costs associated with public key infrastructure construction and certificate management. By introducing a cryptographic accumulator, the computational costs of ring signature generation and verification, as well as the size of the signature data, were reduced to a constant level. Under the random oracle model, the scheme was proven to achieve EUF-CMIA security based on the q-SDH hard problem, and it was demonstrated to have conditional anonymity, enabling the tracing of the actual signer in case of disputes. Theoretical analysis and experimental results show that the signature and verification efficiencies of the proposed scheme are 7.3 times and 3.3 times, respectively, higher than those of existing similar schemes, while the signature data size was approximately one-fifth of theirs. This scheme exhibits significant advantages in both computational efficiency and communication overhead.

Keywords: traceable ring signature, domestic cryptographic algorithm, SM9 algorithm, cryptographic accumulator, identity-based cryptography

收稿日期：2024–09–27；**修回日期：**2025–02–07
通信作者：蔡瑞杰，wsxcrj@163.com
基金项目：装备预先研究基金资助项目（No.30603010601）
Foundation Item：Equipment Pre Research Project (No.30603010601)

0 引言

Rivest等[1]在群签名的基础上提出环签名的概念。在传统的环签名方案中，签名者自发选择多个成员组成环，利用这些环成员的公钥以及签名者的公钥、私钥和随机数等生成签名数据，而验证者仅能验证签名是否来源于环中的某一用户，无法确认签名者的具体身份。与群签名相比，环签名无须设置群管理员，可由签名者自发组建用户群组，且签名过程无须其他环成员参与。环签名的命名源于其最初的实现方式，即签名数据按照特定规则排列成环状。然而，随着新的数学工具的应用，近年来许多新提出的签名方案虽然未采用环状结构，但只要保持了自发性和匿名性的特点，仍被纳入环签名的范畴。环签名的核心安全特性包括不可伪造性和匿名性，这使得其在区块链[2]、电子选举[3]和数字货币[4]等需要保护签名者身份的场景中具有重要应用价值。最初，Rivest等[1]提出的环签名方案基于RSA算法，此后，研究者们开发了基于离散对数[5]、双线性对[6]和格理论[7]等多种密码学原语的环签名方案。

传统的环签名方案通常依赖于公钥基础设施（PKI, public key infrastructure），这种体系面临复杂的证书管理问题。对于PKI体制下的环签名，无论是签名还是验证过程，都需要大量证书来获取环用户的公钥，特别是在环用户数量较多时，证书申请容易成为系统性能的瓶颈。为解决这一问题，研究人员开发了基于标识的环签名方案，在一定程度上缓解了PKI体系带来的性能压力。

国密算法SM9是我国自主研发的基于标识的密码体制（IBC, identity-based cryptography），包括数字签名算法、密钥交换协议、密钥封装机制和加密算法[8-9]。在IBC中，用户的身份信息直接作为公钥使用，因此无须依赖第三方颁发的证书来验证公钥的真实性。这种设计避免了PKI体系的构建，显著降低了密码系统的运维成本。此外，SM9算法基于椭圆曲线，与传统公钥密码算法（如RSA算法）相比，在提供同等安全强度的情况下，所需的密钥长度更短，计算效率更高，从而增强了系统的整体安全性。近年来，除环签名外，基于国密算法SM9设计的可搜索加密[10]、分层标识加密[11-12]、广播加密[13-14]和容错加密[15]等标识密码应用方案被陆续提出，体现了SM9算法优异的性能及其在各类密码应用场景下的良好适配能力。

密码累加器（以下简称“累加器”）是一种高效的密码学工具，能够累加集合内所有元素，并快速验证任意元素是否属于该集合。文献[16]对累加器的研究进展进行了综述，将累加器分为静态累加器、动态累加器和通用累加器3类。静态累加器针对静态集合中的元素进行累加，动态累加器允许动态地添加和删除元素，而通用累加器能同时支持成员证明和非成员证明（即元素不属于集合）。累加器的构造方法包括基于RSA、双线性对和Merkle哈希树等技术，其应用范围涵盖群签名、环签名、匿名凭证、广播加密、时间戳和外包数据验证等领域，主要用于优化时空开销。例如，在标识广播加密中，可将所有广播接收者的标识聚合到累加器中，以获得恒定大小的密文，只有累加器中的用户能够解密，从而节省通信开销[13-14]。同理，累加器也可应用于环签名方案设计，以解决传统环签名方案中签名数据随用户数量线性增长的问题。本文所使用的累加器是基于双线性对构造的动态累加器。

匿名性是保护用户隐私的重要特性，但同时也为不法行为提供了隐蔽条件。例如，在电子投票系统中，不诚实的参与方可能试图违反“一人一票”的规则。Liu等[17]提出的可链接环签名（LRS, linkable ring signature）除了具有普通环签名的匿名属性，还能验证2个签名是否源自同一签名者。在采用LRS的电子投票系统中，选民对某候选人多次投赞成票（即对“赞成”消息进行多次环签名）的行为可被检测，但不会暴露该选民的身份。Fujisaki等[18]进一步提出可追踪环签名（TRS, traceable ring signature）的概念，在该方案中环成员针对每个标签（标签由环成员列表和一个涉及社会事件或选举的问题组成）仅可匿名发表一次意见，如果某成员针对同一标签提交了另一份不同意见的签名（例如，先投赞成票，又试图假冒他人投反对票），其身份将立即暴露。除电子投票外，可追踪环签名还在区块链交易和数字货币转账等领域具有广泛的应用前景。沈蒙等[19]对区块链数字货币的匿名性保护和对抗技术进行对比分析，将交易匿名性的内涵归纳为不可标识性、不可链接性和不可追踪性3个方面，强调数字货币的匿名性保护方案应具备可监管属性，以防不法分子危害金融秩序。总之，可追踪环签名旨在防止签名者滥用匿名性，其实现的是条件匿名性，即在正常情况下用户保持匿名，而在

出现纠纷时，可通过去匿名化揭示相关用户的真实身份，在保证投票、交易的安全性以及用户隐私的同时，保留了追踪不法行为的能力。

本文基于国密算法SM9的数字签名算法，提出一种基于标识的可追踪环签名方案。该方案的系统初始化和用户签名私钥生成过程与SM9数字签名算法基本一致，并且完全兼容SM9国家标准定义的公共参数。通过引入累加器，签名和验证过程的计算量及签名数据大小均降至常数级，不随环用户数量线性增长。同时，证明了本文方案在随机预言机模型下的不可伪造性以及条件匿名性，在符合环签名方案通用安全模型要求的同时，实现了在必要情况下对真实签名者身份的可追踪性。通过理论分析和实验测试结果表明，本文方案在环签名生成与验证算法方面，相较于现有方案在计算效率方面具有显著优势，签名数据为常数级使得通信开销显著减少。

1　相关工作

Zhang等[6]提出基于标识的环签名方案，随后这一领域的研究大多以双线性对作为核心数学工具[20-22]。Brakerski等[23]提出一种利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一种环状结构，生成单个环签名消息的计算开销与执行n次传统数字签名相当（n为环用户数量）。这种方法为后续环签名方案的设计提供了基本依据，但也导致计算和通信开销随环用户数量线性增长的问题。鉴于时空效率在环签名方案应用中的重要性，后续研究更加注重提高计算效率和降低通信开销。Dodis等[24]基于累加器提出一种具有常数级签名数据大小的环签名方案，其身份验证耗时与环成员数量无关，从而显著提升时空效率。Nguyen[25]提出一种基于双线性对的动态累加器方案，并在此基础上构建了一种具有常数级签名数据大小的基于标识的环签名方案。这些创新方法不仅优化了环签名方案的签名和验证性能，还解决了签名数据大小随环用户数量线性增长的问题。

彭聪等[26]将基于标识的国密算法SM9用于环签名方案设计，提出一种与SM9数字签名算法兼容的环签名方案，该方案的通信开销优于传统环签名方案，但签名和验证开销较大。随后，包嘉斌[27]提出基于SM9的环签密方案，邓浩明等[28]提出基于SM9的门限环签名方案，饶金涛等[3]设计了基于SM9盲签名与环签名的安全电子选举协议。安浩杨等[29]提出基于SM9的环签名方案，通过累加器将签名大小降至常数级，通过在公共参数中添加长度与最大环用户数量成正比的累加器元组，实现签名和验证开销不随环用户数量变化。然而，该方案的设计思路较复杂，安全性证明存在不足，且计算开销仍有较大优化空间，仅在环用户数量大于20时，签名数据长度才小于文献[26]方案。

在环签名方案的安全性证明方面，Pointcheval等[30]提出并证明了分叉引理，为数字签名方案的不可伪造性证明提供了有效途径。随后，Herranz等[31]在随机预言机模型下，提出用于证明一般环签名方案安全性的分叉引理。周瑾等[32]进一步将分叉引理扩展至基于身份的签名体制。接着，周敏等[33]利用分叉引理，证明了一般基于身份的环签名体制的安全性。赖建昌等[34]基于q-SDH困难问题假设，在随机预言机模型下给出SM9数字签名算法在自适应选择消息和身份攻击下的存在性不可伪造（EUF-CMIA, existential unforgeability under adaptive chosen-message-and-identity attack）安全性证明。这些研究成果为环签名方案的安全性证明和分析提供了重要的理论基础和方法支撑。

在可追踪环签名的研究方面，Fujisaki等[18]提出的方案在安全性上依赖于随机预言机，签名大小与环成员数量呈线性关系。Liu等[35]提出可撤销环签名的概念，该方案通过指定的权威机构揭露实际签名者，以便必要时撤销签名者的匿名性。Fujisaki[36]进一步提出了签名大小降至次线性级别的可追踪环签名方案，其安全性基于标准模型。Zeng等[37]提出一种基于双线性对的非交互式可否认环签名方案，证明者和验证者无须在确认协议和否认协议中频繁交互，并在标准模型下证明了其安全性[38]。Au等[39]构造了一种基于标识的可追踪环签名方案，如果用户在同一事件中生成2个可链接的环签名，则任意参与者均可通过这2个签名计算出其身份。该方案还具有恒定大小的签名，相较于传统方案在效率上有显著提升。Bootle等[40]基于EIGamal密码设计了一种可问责的环签名方案，并为此类方案提出一个正式的安全模型。包子健等[41]基于SM2数字签名算法提出一种可否认环签名方案，采用交互式确认和否认方法。丁勇等[42]设计的可否认环签名方案基于SM9数字签名算法，

满足可追踪性和不可诽谤性，其环签名验证开销与环成员数量无关，而环签名生成开销及签名数据大小随环用户数量线性增长，在计算效率上较现有方案具有一定优势。然而，该方案与文献[41]方案均需要证明者配合验证者进行确认或否认，在离线状态或证明者不诚实的情况下，两者均无法实现对签名者的追踪。

2 基于标识的环签名概述

本节阐述了符号含义、基于标识的环签名方案所依托的数学困难问题，并概述该类方案的通用系统模型和安全模型。

2.1 符号含义

本文的符号含义与SM9国家标准[8-9]基本一致。G_1, G_2是椭圆曲线加法循环群，P_1, P_2分别是G_1, G_2的生成元，且满足$P_1=\psi(P_2)$（ψ为G_2到G_1的同态映射），G_T是乘法循环群（其元素均为有限域12次扩域上的元素），G_1, G_2, G_T的阶均为素数N。$[k]U$表示G_1或G_2中元素U的k倍（即椭圆曲线上点的标量乘），e表示从$G_1\times G_2$映射到G_T的双线性对，$x\parallel y$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, $N-1$]范围内整数的哈希函数。为简化符号表示，并与本文方案的公开参数P_1, P_2相区分，在困难问题的实例中，使用P, Q分别表示群G_1, G_2的生成元。

2.2 困难问题

在非对称双线性群上定义的q-SDH问题（q-Strong Diffie-Hellman Problem）如下[34]。

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

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。

2.3 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）4个算法构成[26]。该方案涉及密钥生成中心（KGC, key generation center）、签名者和验证者3种角色。其中，KGC采用Setup算法完成系统初始化，并采用KeyGen算法为用户生成签名私钥；签名者采用RingSign算法生成环签名；验证者采用RingVerify算法验证环签名的有效性。

1) 系统建立Setup(λ)→(**params**, **msk**)：KGC运行概率多项式时间（PPT, probabilistic polynomial time）算法，输入安全参数λ，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KeyGen(ID, **msk**)→ds：KGC运行确定性算法，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RingSign(M, U_n, ds)→$\boldsymbol{\sigma}$：签名者（标识为ID_π，$1\leqslant\pi\leqslant n$，n为环用户数量）运行PPT算法，输入待签名消息M、环用户集合$U_n=\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$和签名私钥ds，输出环签名消息$\boldsymbol{\sigma}$。$U_n$中的环成员可为任意用户，甚至可包含未向KGC申请私钥的虚拟用户，但签名者必须拥有签名私钥。

4) 环签名验证RingVerify(M, U_n, $\boldsymbol{\sigma}$)→accept/reject：验证者运行确定性算法，输入被签名消息M、环用户集合$U_n=\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$和环签名消息$\boldsymbol{\sigma}$。若验证通过，则输出accept；否则，输出reject。

本文方案的正确性要求如下。对于合法的签名，验证通过的概率为1；对于非法签名，验证通过的概率是可忽略的[26]。令RandSign代表随机生成签名的算法，negl(λ)表示可忽略函数（随着输入λ增加，函数值快速趋近于零），即式(1)和式(2)成立。

$$\Pr\left[\begin{array}{l}\mathrm{RingVerify}(M, U_n, \boldsymbol{\sigma})= \\ \quad \mathrm{accept}\left|\begin{array}{c}\mathrm{Setup}(\lambda)\rightarrow(\mathbf{params}, \mathbf{msk}) \\ \mathrm{KeyGen}(\mathrm{ID}, \mathbf{msk})\rightarrow \mathrm{ds} \\ \mathrm{RingSign}(M, U_n, \mathrm{ds})\rightarrow \boldsymbol{\sigma}\end{array}\right.\end{array}\right]=1 \tag{1}$$

$$\Pr\left[\begin{array}{l}\mathrm{RingVerify}(M, U_n, \boldsymbol{\sigma})= \\ \quad \mathrm{accept}\left|\begin{array}{c}\mathrm{Setup}(\lambda)\rightarrow(\mathbf{params}, \mathbf{msk}) \\ \mathrm{RandSign}(M, U_n)\rightarrow \boldsymbol{\sigma}\end{array}\right.\end{array}\right]\leqslant \mathrm{negl}(\lambda) \tag{2}$$

需要注意的是，下文中的正确性证明仅针对式(1)，而式(2)的相关证明将在安全性证明中进行详细阐述。

2.4　安全模型

基于标识的环签名方案，需要满足以下2个安全特性[43]，即EUF-CMIA安全性和匿名性。

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**params**和签名主私钥**msk**，将**params**发送给敌手A。

2) 询问。A以自适应方式向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$U_n=\{\mathrm{ID}_1, \mathrm{ID}_2,\cdots, \mathrm{ID}_n\}$，C从$U_n$中随机选择标识$\mathrm{ID}_\pi$（$1\leqslant\pi\leqslant n$），调用KeyGen生成签名私钥$\mathrm{ds}_\pi$，再调用RingSign生成$U_n$对$M$的环签名消息$\boldsymbol{\sigma}$并返回。

3) 伪造。A伪造挑战用户集合$U^*=\{\mathrm{ID}_1^*, \mathrm{ID}_2^*, \cdots, \mathrm{ID}_l^*\}$对消息$M^*$的环签名消息$\boldsymbol{\sigma}^*$，要求A从未询问过$U^*$中任意用户的签名私钥，也从未询问过$U^*$对$M^*$的签名。如果A伪造的签名$\boldsymbol{\sigma}^*$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$\mathrm{Adv_A^{EUF}}=\Pr[\mathrm{RingVerify}(M^*, U^*, \boldsymbol{\sigma}^*)=\mathrm{accept}]$。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**params**和签名主私钥**msk**，将**params**发送给敌手A。

2) 询问。A以自适应方式向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$U_n=\{\mathrm{ID}_1, \mathrm{ID}_2,\cdots, \mathrm{ID}_n\}$，C从$U_n$中随机选择标识$\mathrm{ID}_\pi$（$1\leqslant\pi\leqslant n$），调用KeyGen生成签名私钥$\mathrm{ds}_\pi$，再调用RingSign生成$U_n$对$M$的环签名消息$\boldsymbol{\sigma}$并返回。

3) 挑战。A向C提供挑战用户集合$U^*=\{\mathrm{ID}_1^*, \mathrm{ID}_2^*,\cdots, \mathrm{ID}_l^*\}$、消息$M^*$和2个标识$\mathrm{ID}_{\pi_1}, \mathrm{ID}_{\pi_2}\in U^*$，C随机选择$b\in\{0, 1\}$，调用KeyGen生成$\mathrm{ID}_{\pi_b}$对应的签名私钥$\mathrm{ds}_{\pi_b}$，再调用RingSign生成$U^*$对$M^*$的环签名消息$\boldsymbol{\sigma}^*$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$\mathrm{Adv_A^{ANON}}=\left|\Pr[b'=b]-\frac{1}{2}\right|$。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。

在上述匿名性定义的基础上，进一步定义条件匿名性。假设初始化过程额外生成追踪密钥**tk**（**tk**不属于系统公开参数**params**和签名主私钥**msk**），任意PPT敌手A在不掌握**tk**时，赢得该游戏的优势是可以忽略的，而掌握**tk**后能以不可忽略的优势赢得该游戏，则称该环签名方案满足条件匿名性。

3　基于SM9的可追踪环签名方案构造

本节详细阐述本文所设计的可追踪环签名方案的各项算法，其运行流程如图1所示。

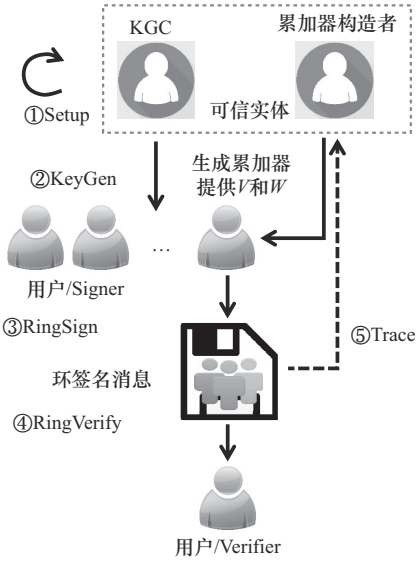

图1　方案运行流程

3.1　系统建立Setup

KGC生成随机数$\mathrm{ks}\in[1, N-1]$作为签名主私钥，计算G_2中的元素$P_{\text{pub-s}}=[\mathrm{ks}]P_2$作为签名主公钥，则签名主密钥对为$(\mathrm{ks}, P_{\text{pub-s}})$。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。

生成随机数 $s\in[1, N-1]$，计算 G_2 中的元素 $S_{\text{pub}}=[s]P_2$，计算 G_1 中的元素集合 $L=\{P_1, [s]P_1, [s^2]P_1,\cdots, [s^q]P_1\}$，其中 q 是累加器可以累加的最大数量，公开 S_{pub} 和 L。累加器相关参数（S_{pub}, L）可由 KGC 生成，也可由其他可信的第三方生成。此类累加器的详细描述和安全性证明可参考文献[25]，文献[29]描述了如何动态添加和删除累加器元素，本文不再赘述。

3.2 用户签名私钥生成 KeyGen

设用户的标识为 ID，为生成其签名私钥 ds，KGC 在有限域 F_N 上计算 $t_1=H_1(\text{ID}\parallel\text{hid}, N)+\text{ks}$，若 $t_1=0$，则重新生成系统签名主密钥，并更新已有用户的签名私钥；否则，计算 $t_2=\text{ks}\cdot t_1^{-1}$，再计算 $\text{ds}=[t_2]P_1$。最后，将签名私钥 ds 通过安全途径传递给用户。

3.3 环签名生成 RingSign

设环用户集合 $U_n=\{\text{ID}_1, \text{ID}_2,\cdots, \text{ID}_n\}$（$n\leqslant q$），待签名的消息为比特串 M，签名者的标识为 ID_π（$1\leqslant\pi\leqslant n$），生成环签名消息 $\boldsymbol{\sigma}$ 的运算步骤如下。

步骤 1 计算整数 $v_i=H_1(\text{ID}_i\parallel\text{hid}, N)$（$1\leqslant i\leqslant n$），计算 G_1 中的元素 $V=[\prod_{i=1}^{n}(v_i+s)]P_1$ 和 $W_\pi=[\prod_{i=1,i\neq\pi}^{n}(v_i+s)]P_1$。

步骤 2 计算 G_T 中的元素 $g_1=e(P_1, P_{\text{pub-s}})\cdot e(V, P_2)$ 和 $g_2=e(W_\pi+\text{ds}_\pi, P_2)$。

步骤 3 生成随机数 $r_1, r_2\in[1, N-1]$，计算 G_T 中的元素 $\omega=g_1^{r_1}\cdot g_2^{r_2}$。

步骤 4 计算整数 $h=H_2(U_n\parallel M\parallel\omega, N)$。

步骤 5 计算 G_1 中的元素 $R=[r_1-h]W_\pi$ 和 $S=[r_1-h]\text{ds}_\pi$，计算 G_2 中的元素 $T=[r_2(r_1-h)^{-1}+v_\pi]P_2$。

步骤 6 输出环签名消息 $\boldsymbol{\sigma}=(h, R, S, T)$。

值得注意的是，在系统参数和环用户固定的情况下，步骤 1 和步骤 2 可预先计算完成。此外，在步骤 1 中，签名者在已知 L 而不知 s 的情况下即可计算 V 和 W_π。但有限域 F_N 上模乘运算的计算复杂度为 $O(2^n)$，当 $n=26$ 时，计算 V 的实际耗时已超过 1 min。若 n 继续增大，则耗时将难以接受，因此步骤 1 可由累加器的构造者辅助完成（该构造者同 KGC 一样是可信的）。签名者收到 V 和 W_π 后，可通过验证等式 $e(W_\pi, [v_\pi]P_2+S_{\text{pub}})=e(V, P_2)$ 以快速确认 V 和 W_π 的有效性。

3.4 环签名验证 RingVerify

验证者收到消息 M' 的环签名消息 $\boldsymbol{\sigma}'=(h', R', S', T')$ 后，运算步骤如下。

步骤 1 检验 $h'\in[1, N-1]$, $R', S'\in G_1$, $T'\in G_2$ 是否完全成立，若不完全成立，则验证不通过。

步骤 2 计算整数 $v_i=H_1(\text{ID}_i\parallel\text{hid}, N)$（$1\leqslant i\leqslant n$），计算 G_1 中的元素 $V=[\prod_{i=1}^{n}(v_i+s)]P_1$。

步骤 3 计算群 G_T 中的元素 $g_1=e(P_1, P_{\text{pub-s}})\cdot e(V, P_2)$。

步骤 4 计算 G_T 中的元素 $\omega'=e(R', S_{\text{pub}}+T')\cdot e(S', P_{\text{pub-s}}+T')\cdot g_1^{h'}$。

步骤 5 计算整数 $h_2=H_2(U_n\parallel M'\parallel\omega', N)$。

步骤 6 检验 $h_2=h'$ 是否成立，若成立，则验证通过；否则，验证不通过。

同理，步骤 2 和步骤 3 可预先计算完成，步骤 2 的 V 可由累加器的构造者计算并分发。

3.5 签名者追踪 Trace

在标识环签名通用系统模型的基础上，定义签名者追踪算法（由仲裁者运行的确定性算法），可用于否认签名值来自某用户，也可通过遍历环用户集合找到实际签名者。当出现不诚实的签名或用户之间产生纠纷时，由掌握累加器秘密参数 s 的累加器构造者作为仲裁者。假设 $\boldsymbol{\sigma}=(h, R, S, T)$ 是环用户集合 $U_n=\{\text{ID}_1, \text{ID}_2,\cdots, \text{ID}_n\}$ 对消息 M 的合法签名，为判断 $\boldsymbol{\sigma}$ 是否由特定签名者 ID_π（$1\leqslant\pi\leqslant n$）生成，仲裁者执行以下运算步骤。

步骤 1 计算整数 $v_i=H_1(\text{ID}_i\parallel\text{hid}, N)$（$1\leqslant i\leqslant n$）。

步骤 2 计算群 G_T 中的元素 $T_1=e(S, [v_\pi]P_2+P_{\text{pub-s}})$，$T_2=e\left(\left[\frac{1}{\prod_{i=1,i\neq\pi}^{n}(v_i+s)}\right]R, P_{\text{pub-s}}\right)$。

步骤 3 检验 $T_1=T_2$ 是否成立，当且仅当 $T_1=T_2$ 时，签名者为 ID_π。

4 方案性质推导与证明

本节通过理论推导验证本文方案的正确性，并通过形式化的安全分析证明了本文方案具有不可伪造性和条件匿名性。

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 $\boldsymbol{\sigma}'$ 在传输过程中未被篡改，即 $M=M'$, $h=h'$, $R=R'$, $S=S'$, $T=T'$，则方案的正确性来自以下推导。

由于 $V=[v_\pi+s]W_\pi$，即 $e(W_\pi, [v_\pi]P_2+S_{\text{pub}})=e(V, P_2)$，又有 $e(\text{ds}_\pi, [v_\pi]P_2+P_{\text{pub-s}})=e(P_1, P_{\text{pub-s}})$，则有

$$\omega'=e(R',S_{\text{pub}}+T')\cdot e(S',P_{\text{pub-s}}+T')\cdot g_1^{h'}=$$
$$e([r_1-h]W_\pi,S_{\text{pub}}+[r_2(r_1-h)^{-1}+v_\pi]P_2)\cdot$$
$$e([r_1-h]\text{ds}_\pi,P_{\text{pub-s}}[r_2(r_1-h)^{-1}+v_\pi]P_2)\cdot g_1^{h}=$$
$$e([r_1-h]W_\pi,[v_\pi]P_2+S_{\text{pub}})\cdot$$
$$e([r_1-h]\text{ds}_\pi,[v_\pi]P_2+P_{\text{pub-s}})\cdot$$
$$e([r_1-h](W_\pi+\text{ds}_\pi),[r_2(r_1-h)^{-1}]P_2)\cdot g_1^{h}=$$
$$e([r_1-h]V,P_2)\cdot e([r_1-h]P_1,P_{\text{pub-s}})\cdot$$
$$e(W_\pi+\text{ds}_\pi,[r_2]P_2)\cdot g_1^{h}=$$
$$g_1^{r_1-h}\cdot g_2^{r_2}\cdot g_1^{h}=g_1^{r_1}\cdot g_2^{r_2}=\omega$$

故 $h_2=h'$。

因此，本文环签名方案是正确的。

4.2　不可伪造性

本节运用形式化的安全规约方法证明本文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, 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 ε 伪造本文方案签名，则可构建模拟器S解决 q-SDH 问题。S以一个 q-SDH 问题实例（$P, Q, [a]Q, [a^2]Q,\cdots, [a^q]Q$）$\in G_1\times G_2^{q+1}$ 作为输入，控制随机预言机并运行A的任意攻击算法，进行以下操作。

1) 初始化。令 ψ 为 G_2 到 G_1 的同态映射，满足 $[a^i]P=\psi([a^i]Q)$，$0\leqslant i\leqslant q$。模拟器S随机选择 $q+1$ 个互不相同的数 $w^*, w_1, w_2,\cdots, w_q\in[1, N-1]$，令 $f(x)=\prod_{i=1}^{q}(w_i+x)$，$f(x)$ 是 $Z_N[x]$ 中次数为 q 的多项式。设 $P_1=[f(a)]P$，$P_2=Q$，$P_{\text{pub-s}}=[a]Q$；S随机选择 $s\in[1, N-1]$，生成累加器相关参数 $S_{\text{pub}}=[s]P_2$, $L=\{P_1, [s]P_1, [s^2]P_1,\cdots, [s^q]P_1\}$。除了签名主私钥 $\text{ks}=a$ 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S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。在开始询问前，S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S发起以下哈希询问。

①H_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S根据 L_1 的记录进行应答。否则，当 $i=i^*$ 时，设 $H_1(\text{ID}_i)=w^*$；当 $i\neq i^*$ 时，设 $H_1(\text{ID}_i)=w_i$。S将 $H_1(\text{ID}_i)$ 作为该询问的应答，并在 L_1 中记录 $(i, \text{ID}_i, H_1(\text{ID}_i))$。

②H_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S根据 L_2 的记录进行应答。否则，S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以自适应方式向S发起私钥询问、累加器询问和签名询问。

①私钥询问。A询问身份标识 ID_i 的签名私钥，令 $(i, \text{ID}_i, H_1(\text{ID}_i))$ 为 L_1 中对应的记录。若 $i=i^*$，则中止；否则，$H_1(\text{ID}_i)=w_i$。令 $f_i(x)=x\prod_{j=1,j\neq i}^{q}(w_j+x)$，则 $f_i(x)$ 是 $Z_N[x]$ 中的 q 次多项式，利用问题实例和所选参数计算签名私钥 $\text{ds}_i=[f_i(a)]P$。因为 $\text{ds}_i=[f_i(a)]P=\left[\frac{a\cdot f(a)}{w_i+a}\right]P=\left[\frac{a}{w_i+a}\right]P_1$，所以 ds_i 是一个有效的签名私钥。

②累加器询问。A询问环用户集合 U_j 的累加器值，S调用RingSign步骤1计算 G_1 中的元素 V 并返回；当A指定 ID_π（$\text{ID}_\pi\in U_j$）时，S返回 (V, W_π)。

③签名询问。A询问环用户集合 U_j 对消息 M 的签名 $\boldsymbol{\sigma}$。S从 U_j 中随机选择标识 ID_π（$\pi\neq i^*$），生成其签名私钥 ds_π，再调用RingSign生成 U_j 对 M 的环签名消息 $\boldsymbol{\sigma}$ 并返回。

4) 伪造。A伪造挑战用户集合 $U^*=\{\text{ID}_1^*, \text{ID}_2^*,\cdots, \text{ID}_n^*\}$ 对消息 M^* 的环签名消息 $\boldsymbol{\sigma}^*$，要求A从未询问过 U^* 中任意用户的签名私钥，也从未询问过 U^* 对 M^* 的签名。若 $\text{ID}_{i^*}\notin U^*$，则中止；否则，根据分叉引理，在不掌握 U^* 中任意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 $\boldsymbol{\sigma}^*$，则S可构造一个图灵机A′通过多次运行A的攻击算法，以相同的输入 (M^*, U^*) 得到2个有效的环签名消息 $\sigma_1^*=(h_1^*, R_1^*, S_1^*, T_1^*)$ 和 $\sigma_2^*=(h_2^*, R_2^*, S_2^*, T_2^*)$，满足 $h_1^*\neq h_2^*, S_1^*\neq S_2^*$。令 $\frac{x\cdot f(x)}{w^*+x}=F(x)+\frac{d}{w^*+x}$。其中，$F(x)$ 是 $Z_N[x]$ 中的 q 次多项式，d 为非零整数，$F(x)$ 的各项系数和 d 均可通过所选参数计算。S计算 $W^*=\left[\frac{1}{d}\right]\left(\left[\frac{1}{h_2^*-h_1^*}\right](S_1^*-S_2^*)-[F(a)]P\right)$，输出 (w^*, W^*) 作为 q-SDH 问题实例的解。这是由于当签名者恰好为 ID_{i^*}（即A伪造签名私钥的标识在 L_1

中的序号为i^*）时，有$S_1^*=[r_1^*-h_1^*]\mathrm{ds}_{i^*}=\left[\frac{a(r_1^*-h_1^*)}{w^*+a}\right]P_1=\left[\frac{a(r_1^*-h_1^*)f(a)}{w^*+a}\right]P$，$S_2^*=[r_1^*-h_2^*]\mathrm{ds}_{i^*}=\left[\frac{a(r_1^*-h_2^*)}{w^*+a}\right]P_1=\left[\frac{a(r_1^*-h_2^*)f(a)}{w^*+a}\right]P$，则有

$$W^*=\left[\frac{1}{d}\right]\left(\left[\frac{1}{h_2^*-h_1^*}\right](S_1^*-S_2^*)-[F(a)]P\right)=$$
$$\left[\frac{1}{d}\left(\frac{(r_1^*-h_1^*)-(r_1^*-h_2^*)}{h_2^*-h_1^*}\cdot\frac{a\cdot f(a)}{w^*+a}-F(a)\right)\right]P=$$
$$\left[\frac{1}{d}\left(\frac{a\cdot f(a)}{w^*+a}-F(a)\right)\right]P=$$
$$\left[\frac{1}{d}\left(F(a)+\frac{d}{w^*+a}-F(a)\right)\right]P=$$
$$\left[\frac{1}{w^*+a}\right]P$$

因此，(w^*, W^*)可作为q-SDH问题实例的一个解。如果签名者不是ID_{i^*}，则(w^*, W^*)不是q-SDH问题实例的有效解。

以下对S破解q-SDH问题的优势进行分析。首先，只有满足$\mathrm{ID}_{i^*}\in U^*$，S才能成功模拟（指模拟不中止），此概率为$\frac{n}{q_{H_1}}$；其次，在成功模拟的前提下，只有当签名者为ID_{i^*}时，A的攻击是有用的（有用攻击指可以归约到解决底层困难问题的攻击），此概率为$\frac{1}{n}$；则对于任意一次模拟，A发起有用攻击的概率为$\frac{1}{q_{H_1}}$，而q_{H_1}是多项式级别且有上界，故此概率是不可忽略的。因此，若A能以不可忽略的优势ε伪造本文方案签名，则S能以$\frac{\varepsilon}{q_{H_1}}$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，因此本文环签名方案在EUF-CMIA安全模型下是安全的。证毕。

4.3 条件匿名性

对条件匿名性的证明分为2个方面，一方面，证明本文方案可有效追踪合法签名的实际签名者；另一方面，证明签名对于仲裁者以外的实体满足匿名性。在匿名性方面，考虑KGC可能作为好奇的恶意敌手，需要确保即使敌手获知系统主私钥，也无法确定环签名消息的真实签名者。

定理2　如果随机数源满足均匀分布，则本文所提环签名方案具有条件匿名性。

证明　令$\boldsymbol{\sigma}=(h, R, S, T)$是环用户集合$U_n$对消息$M$的合法签名，$v_i=H_1(\mathrm{ID}_i)$（$1\leqslant i\leqslant n$）。根据签名者追踪算法，仲裁者可判断签名是否由特定签名者ID_π（$\mathrm{ID}_\pi\in U_n$）产生，这是由于当签名者为ID_π时，有

$$T_1=e(S, [v_\pi]P_2+P_{\text{pub-s}})=$$
$$e([r_1-h]\mathrm{ds}_\pi, [v_\pi]P_2+P_{\text{pub-s}})=$$
$$e([r_1-h]P_1, P_{\text{pub-s}})$$

$$T_2=e\left(\left[\frac{1}{\prod_{i=1,i\neq\pi}^{n}(v_i+s)}\right]R, P_{\text{pub-s}}\right)=$$
$$e\left(\left[\frac{r_1-h}{\prod_{i=1,i\neq\pi}^{n}(v_i+s)}\right]W_\pi, P_{\text{pub-s}}\right)=$$
$$e([r_1-h]P_1, P_{\text{pub-s}})$$

综上所述，$T_1=T_2$。当实际签名者为ID_j（$1\leqslant j\leqslant n$且$j\neq\pi$）时，有

$$T_1=e\left([r_1-h]\mathrm{ds}_j, [v_\pi]P_2+P_{\text{pub-s}}\right)=$$
$$e\left(\left[\frac{(r_1-h)(v_\pi+\mathrm{ks})}{v_j+\mathrm{ks}}\right]P_1, P_{\text{pub-s}}\right)$$

$$T_2=e\left(\left[\frac{r_1-h}{\prod_{i=1,i\neq\pi}^{n}(v_i+s)}\right]W_j, P_{\text{pub-s}}\right)=$$
$$e\left(\left[\frac{(r_1-h)\prod_{i=1,i\neq j}^{n}(v_i+s)}{\prod_{i=1,i\neq\pi}^{n}(v_i+s)}\right]P_1, P_{\text{pub-s}}\right)=$$
$$e\left(\left[\frac{(r_1-h)(v_\pi+s)}{v_j+s}\right]P_1, P_{\text{pub-s}}\right)$$

因为$\mathrm{ks}\neq s$，所以$T_1\neq T_2$，即签名者追踪算法的正确性得证。

接下来考虑在不掌握累加器秘密参数s的情况下本文方案的匿名性。假设$\boldsymbol{\sigma}$由签名者ID_{π_1}（$1\leqslant\pi_1\leqslant n$）生成，根据本文环签名方案，$S=[r_1-h]\mathrm{ds}_{\pi_1}=\left[\frac{(r_1-h)\mathrm{ks}}{v_{\pi_1}+\mathrm{ks}}\right]P_1$。而$\boldsymbol{\sigma}$同样可视为由签名

者 ID_{π_2}（$1\leqslant\pi_2\leqslant n$ 且 $\pi_2\neq\pi_1$）生成，这是由于 $S=\left[\frac{(r_1-h)\mathrm{ks}}{v_{\pi_1}+\mathrm{ks}}\right]P_1=\left[\frac{(r_1-h)(v_{\pi_2}+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}\cdot\frac{\mathrm{ks}}{v_{\pi_2}+\mathrm{ks}}\right]P_1$，令 $r_1'=\frac{(r_1-h)(v_{\pi_2}+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}+h$，则 $S=\left[\frac{(r_1'-h)\mathrm{ks}}{v_{\pi_2}+\mathrm{ks}}\right]P_1$，此时 T 可视为 $T=\left[\frac{r_2'}{r_1'-h}+v_{\pi_2}\right]P_2=\left[\frac{r_2}{r_1-h}+v_{\pi_1}\right]P_2$，则 $r_2'=\left(\frac{r_2}{r_1-h}+v_{\pi_1}-v_{\pi_2}\right)(r_1'-h)$。当本文方案采用的随机数源满足均匀分布时，签名者 ID_{π_1} 在签名过程中生成的2个随机数(r_1, r_2)是随机且独立的。假设 $\boldsymbol{\sigma}$ 的签名者是 ID_{π_2}，其在签名过程中产生的2个随机数(r_1' r_2')同样是随机且独立的。又因为在不掌握 s 的情况下，R 无法为区分 $\boldsymbol{\sigma}$ 的签名者提供有用信息，所以敌手认为 $\boldsymbol{\sigma}$ 由 ID_{π_1} 或 ID_{π_2} 生成的概率是相等的。进一步地，$\boldsymbol{\sigma}$ 的实际签名者在集合 U_n 内具有不可区分性，即本文所提环签名方案满足匿名性。证毕。

综上所述，本文环签名方案实现了有条件的匿名性，即必要时对签名者真实身份的可追踪性，并以累加器秘密参数 s 而非KGC掌握的系统主私钥作为追踪实际签名者的关键陷门信息。本文方案能够确保KGC和所有用户均无法从环签名消息中获取签名者的真实身份，如果发生争议，则有能力在仲裁者的协助下揭示不诚实的签名者。

5　性能分析与实验

本节对本文方案的计算开销和通信开销进行理论分析与实验测试，通过与同类方案进行对比来验证本文方案的性能优势。

5.1　性能分析

对本文方案的计算开销和通信开销进行定量分析，并与文献[21]、文献[22]、文献[26]、文献[29]、文献[39]和文献[42]提出的环签名方案进行对比。文献[26]、文献[29]、文献[42]和本文方案均基于SM9算法构造，文献[29]、文献[39]和本文都运用了累加器技术，将计算开销和通信开销降至常数级，文献[42]方案的验证开销为常数级且同样具有可追踪性因此，下文将重点与文献[29]方案和文献[42]方案进行对比分析。

在计算开销方面，主要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所示。其中，SM_1 和 SM_2 分别表示 G_1 和 G_2 上的标量乘运算，BP表示双线性对运算，E表示 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，n 表示环用户数量。经实测，其他运算（如有限域 F_N 上的模逆运算、G_1 和 G_2 上的加法运算、G_T 上的乘法运算以及哈希运算 H_1 和 H_2 等）的耗时与上述运算至少相差2个数量级，为突出重点已将其忽略。本文对各方案进行统一的等效替换优化，因此表1中部分数据与文献[29]和文献[42]存在差异。例如，计算 $e([r]P_1, P_2)$ 的方式调整为 G_T 上固定元素 $e(P_1, P_2)$ 的 r 次幂，计算开销从“SM_1+BP”降至“E”。

需要说明的是，对于文献[29]、文献[39]和本文方案，表1中理论分析数据及后文的实验测试数据均未包含生成 V 和 W_π 的计算开销。这是因为无论是在环签名生成还是验证环节，用户自行生成 V 和 W_π 的耗时随环用户数量 n 呈指数级增长。经实测，当 $n>20$ 时，生成 V 和 W_π 的耗时占比已远超其

表1　　**环签名方案的计算开销**

方案	私钥生成	环签名生成	环签名验证
文献[21]	HTP	SM_1+(n−1)SM_2+(n+1)BP	$n\mathrm{SM}_2$+2BP
文献[22]	HTP	nHTP+2$n\mathrm{SM}_2$	$n\mathrm{SM}_2$+2BP
文献[26]	SM_1	(n+1)SM_1+(n−1)SM_2+(n−1)E+nBP	$n\mathrm{SM}_2$+nE+nBP
文献[29]	SM_1	12SM_1+6E+2BP	8SM_1+10E+4BP
文献[39]	6SM_1+SM_2+2BP	12SM_1+14E+2BP	9SM_1+15E+4BP
文献[42]	SM_1	$n\mathrm{SM}_1$+5E	SM_2+E+BP
本文方案	SM_1	2SM_1+SM_2+2E	E+2BP

他运算。因此，本文假定V和W_π由累加器的构造者预先生成并分发。事实上，文献[29]在方案实现与测试时也采用了类似的处理方法。此外，文献[39]方案的用户私钥由KGC和用户共同计算，表1中的私钥生成数据为KGC和用户开销的总和（表2同理）。

在环签名生成过程中，本文方案相较于文献[29]方案避免了耗时较大的双线性对运算，开销均为常数级，而文献[42]方案的G_1上标量乘次数与环用户数相等。在环签名验证过程中，本文方案相较于文献[29]方案减少了大部分双线性对运算和G_T上的幂运算，且无须G_1上的标量乘运算，比文献[42]方案多一次双线性对运算。因此，本文方案的计算性能优于文献[29]方案，环签名生成效率优于文献[42]方案。

在通信开销方面，主要考虑系统公钥、用户私钥和环签名数据的比特位数，对比分析结果如表2所示。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，q表示累加器可以累加的最大数量。具体而言，对于SM9国家标准规范使用的256 bit的BN曲线[8]，$|G_1|=512$ bit，$|G_2|=1\ 024$ bit，$|G_T|=3\ 072$ bit，$|F_N|=256$ bit。SM9国家标准已规定的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

方案	系统公钥	用户私钥	环签名数据
文献[21]	$\|G_2\|$	$\|G_1\|$	$n\|G_T\|+\|G_1\|+n\|F_N\|$
文献[22]	$\|G_2\|$	$\|G_1\|$	$(n+1)\|G_2\|$
文献[26]	$\|G_2\|$	$\|G_1\|$	$n\|G_1\|+\|F_N\|$
文献[29]	$2\|G_2\|+(q+4)\|G_1\|$	$\|G_1\|$	$2\|G_T\|+6\|G_1\|+8\|F_N\|$
文献[39]	$(q+2)\|G_2\|$	$2\|G_1\|+\|F_N\|$	$2\|G_T\|+3\|G_1\|+12\|F_N\|$
文献[42]	$\|G_2\|$	$\|G_1\|$	$\|G_T\|+n\|G_1\|+\|F_N\|$
本文方案	$2\|G_2\|+q\|G_1\|$	$\|G_1\|$	$\|G_2\|+2\|G_1\|+\|F_N\|$

由表2可知，文献[29]方案、文献[39]方案和本文方案由于引入了累加器，系统公钥较其他方案有所增大（长度与累加器上限q线性相关），但环签名数据的通信开销降低至常数级。经计算，文献[29]方案的环签名数据大小为1 408 B，而本文方案仅为288 B，约为前者的$\frac{1}{5}$。除文献[39]方案外，其他方案的用户私钥均与标准标识数字签名算法一致。文献[29]方案和本文方案虽然引入了额外的系统公钥，但仍能兼容标准SM9数字签名算法的系统参数和用户私钥，便于在运行SM9算法的既有系统中应用。

5.2 实验测试

本文基于国密算法开源Python库hggm[44]的SM9模块，通过Python编程实现文献[26]方案、文献[29]方案、文献[42]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，以验证本文方案的有效性与性能优势。实验计算机配置如表3所示。

表3 实验计算机配置

项目	配置
设备类型	个人计算机
操作系统	Windows10，64位
CPU	Intel Core i3-10110U（2核心4线程）
内存	8GB LPDDR3 2133 MHz
硬盘	SAMSUNG MZVLB512HBJQ-000L7
Python版本	3.7.1

当环用户数量n分别为4、16、64、256、1 024时，测试各方案的环签名生成与验证耗时（单位为ms），结果如表4所示。除文献[26]方案外，数据对比结果如图2所示。对于可预计算的步骤，均已提前进行预计算，预计算耗时不包括在内。各项算法均执行500次，取平均值为有效数据。

表4 各方案的环签名生成与验证耗时

方案	算法	环用户数量/个				
		4	16	64	256	1 024
文献[26]	环签名生成	118.33	491.86	2 067.99	8 377.71	3 3811.28
文献[29]		89.72	90.39	90.79	90.84	91.87
文献[42]		26.83	35.14	64.27	187.24	676.06
本文方案		12.26	12.28	12.33	12.61	12.74
文献[26]	环签名验证	120.96	485.08	2 025.57	8 175.67	32 848.66
文献[29]		189.25	192.31	191.29	191.21	191.24
文献[42]		32.03	32.65	35.05	38.20	55.51
本文方案		56.30	56.55	58.17	57.52	58.25

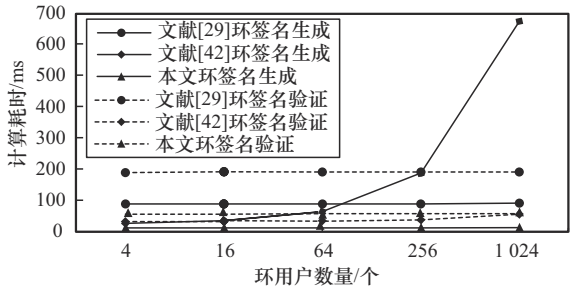

图2　各方案的计算耗时对比

由表4和图2可知，文献[29]方案、文献[42]方案以及本文方案的环签名验证开销为常数级，几乎不随n变化。而文献[26]方案和文献[42]方案的环签名生成开销随n线性增长，当n较大时将产生较大时延。本文方案环签名生成的计算效率为文献[29]方案的7.20~7.36倍、文献[42]方案的2.19~53.07倍，环签名验证效率为文献[29]方案的3.28~3.40倍、文献[42]方案的56.9%~95.3%。

综上所述，相较于现有环签名方案，本文方案在通信开销、环签名生成与验证算法效率等方面均具有明显优势，尤其是在环用户数量较大的情况下。

6　结束语

基于标识的环签名作为一种保护用户隐私的数字签名技术，同时避免了PKI体系下的证书管理问题，随着区块链、电子选举和数字货币等技术的普及，已得到广泛应用并成为近年来的研究热点。本文基于国密算法SM9的数字签名算法，设计了一种高效的可追踪环签名方案。通过理论推导证明本文方案的正确性，并通过形式化的安全分析，证明其在随机预言机模型下具有EUF-CMIA安全性，以及在出现争议时可追踪实际签名者的条件匿名性。通过理论分析和实验测试表明，本文方案和文献[29]方案均为基于SM9算法的常数级环签名方案，签名、验证开销以及签名数据长度与环用户数量无关，而文献[42]方案的验证开销为常数级，签名生成及签名数据长度仍为线性。本文方案的设计思路和计算过程较文献[29]方案进一步简化，安全性分析也更详尽。相较于文献[42]方案，本文方案通过签名数据追踪签名者，无须与用户交互，即使用户不配合或不诚实也能成功追踪。因此，本文方案不仅具有理论意义，在实践中也能显著提升环签名计算的效率，具备广泛的应用前景。考虑本文方案的仲裁者权力过大，下一步将在此基础上设计可否认的环签名方案，在保持计算效率的同时，将确认或否认签名的权限回归到普通用户。

参考文献：

[1] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//2001 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] 饶金涛, 崔喆. 基于SM9盲签名与环签名的安全电子选举协议[J]. 计算机工程, 2023, 49(6): 13-23, 33.
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.

[4] 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]//Computer Security-ESORICS 2017. Berlin: Springer, 2017: 456-474.

[5] ABE M, OHKUBO M, SUZUKI K. 1-out-of-n signatures from a variety of keys[C]//Cryptology-ASIACRYPT 2002. Berlin: Springer, 2002: 415-432.

[6] ZHANG F G, KIM K. ID-based blind signature and ring signature from pairings[C]//Cryptology-ASIACRYPT 2002. Berlin: Springer, 2002: 533-547.

[7] 贾小英, 何德彪, 许芷岩, 等. 格上高效的基于身份的环签名体制[J]. 密码学报, 2017, 4(4): 392-404.
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 Research, 2017, 4 (4): 392-404.

[8] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 SM9标识密码算法 第1部分：总则: GB/T 38635.1—2020[S]. 北京: 中国标准出版社, 2020.
State Administration for Market Regulation, National Standardization Administration. Information security technology-identity-based cryptographic algorithms SM9: Part 1: General: GB/T 38635.1—2020[S]. Beijing: Standards Press of China, 2020.

[9] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 SM9标识密码算法 第2部分：算法: GB/T 38635.2—2020[S]. 北京: 中国标准出版社, 2020.
State Administration for Market Regulation, National Standardization Administration. Information security technology-identity-based cryptographic algorithms SM9: Part 2: Algorithms: GB/T 38635.2—2020[S]. Beijing: Standards Press of China, 2020.

[10] 蒲浪, 林超, 伍玮, 等. 基于SM9的公钥可搜索加密方案[J]. 信息安全学报, 2023, 8(1): 108-118.
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.

[11] 赖建昌, 黄欣沂, 何德彪, 等. 基于商用密码SM9的高效分层标识加密[J]. 中国科学: 信息科学, 2023, 53(5): 918-930.
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.

[12] 李聪, 梁俊凯, 丁煜甲, 等. 基于SM9的分层标识广播内积函数加密[J]. 中国科学: 信息科学, 2024, 54(6): 1400-1418.
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] 赖建昌, 黄欣沂, 何德彪. 一种基于商密SM9的高效标识广播加密方案[J]. 计算机学报, 2021, 44(5): 897-907.
LAI J C, HUANG X Y, HE D B. An efficient identity-based broadcast encryption scheme based on SM9[J]. Chinese Journal of Computers, 2021, 44(5): 897-907.

[14] 崔岩, 黄欣沂, 赖建昌, 等. 基于SM9的匿名广播加密方案[J]. 信息安全学报, 2023, 8(6): 15-27.
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.

[15] 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): 122101.

[16] 苗美霞, 武盼汝, 王赟玲. 密码累加器研究进展及应用[J]. 西安电子科技大学学报, 2022, 49(1): 78-91.
MIAO M X, WU P R, WANG Y L. Research progress and applications of cryptographic accumulators[J]. Journal of Xidian University, 2022, 49(1): 78-91.

[17] LIU J K, WEI V K, WONG D S. Linkable spontaneous anonymous group signature for ad hoc groups[C]//Information Security and Privacy. Berlin: Springer, 2004: 325-335.

[18] FUJISAKI E, SUZUKI K. Traceable ring signature[C]//2007 International Workshop on Public Key Cryptography. Berlin: Springer, 2007: 181-200.

[19] 沈蒙, 车征, 祝烈煌, 等. 区块链数字货币交易的匿名性: 保护与对抗[J]. 计算机学报, 2023, 46(1): 125-146.
SHEN M, CHE Z, ZHU L H, et al. Anonymity in blockchain digital currency transactions: protection and confrontation[J]. Chinese Journal of Computers, 2023, 46(1): 125-146.

[20] LIN C Y, WU T C. An identity-based ring signature scheme from bilinear pairings[C]//Proceedings of the 18th International Conference on Advanced Information Networking and Applications (AINA2004). Piscataway: IEEE Press, 2004: 182-185.

[21] HERRANZ J, SÁEZ G. New identity-based ring signature schemes[C]//Information and Communications Security. Berlin: Springer, 2004: 27-39.

[22] CHOW S S M, YIU S M, HUI L C K. Efficient identity based ring signature[C]//Applied Cryptography and Network Security. Berlin: Springer, 2005: 499-512.

[23] BRAKERSKI Z, KALAI Y T. A framework for efficient signatures, ring signatures and identity based encryption in the standard model[J]. IACR Cryptology ePrint Archive, 2010(86): 1-45.

[24] DODIS Y, KIAYIAS A, NICOLOSI A, et al. Anonymous identification in ad hoc groups[C]//2004 International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Berlin: Springer, 2004: 609-626.

[25] NGUYEN L. Accumulators from bilinear pairings and applications[C]//2005 Cryptographers' Track at the RSA Conference (CT-RSA). Berlin: Springer, 2005: 275-292.

[26] 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.

[27] 包嘉斌. 基于SM9标识密码算法的环签密方案设计及其应用研究[D]. 武汉: 武汉大学, 2022.
BAO J B. Design and application of ring signcryption scheme based on SM9 identity cryptography algorithm[D]. Wuhan: Wuhan University, 2022.

[28] 邓浩明, 彭长根, 丁红发, 等. 基于国密SM9算法的门限环签名方案[J]. 计算机技术与发展, 2022, 32(12): 95-102.
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.

[29] 安浩杨, 何德彪, 包子健, 等. 基于SM9数字签名的环签名及其在区块链隐私保护中的应用[J]. 计算机研究与发展, 2023, 60(11): 2545-2554.
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.

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

[31] HERRANZ J, SÁEZ G. Forking lemmas for ring signature schemes[C]//2003 International Conference on Cryptology (INDOCRYPT). Berlin: Springer, 2003: 266-279.

[32] 周瑾, 张亚娟, 祝跃飞. 一般的基于身份签名体制与Forking引理[J]. 信息工程大学学报, 2007, 8(2): 129-133.
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.

[33] 周敏, 傅贵, 周权. 分叉引理对一般基于身份环签名体制的证明[J]. 通信技术, 2008, 41(7): 183-184, 188.
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.

[34] 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.

[35] LIU D Y W, LIU J K, MU Y, et al. Revocable ring signature[J]. Journal of Computer Science and Technology, 2007, 22(6): 785-794.

[36] FUJISAKI E. Sub-linear size traceable ring signatures without random

oracles[C]//2011 Cryptographers' Track at the RSA Conference (CT-RSA). Berlin: Springer, 2011: 393-415.

[37] ZENG S K, JIANG S Q, QIN Z G. An efficient conditionally anonymous ring signature in the random oracle model[J]. Theoretical Computer Science, 2012, 461: 106-114.

[38] ZENG S K, LI Q Y, QIN Z G, et al. Non-interactive deniable ring signature without random oracles[J]. Security and Communication Networks, 2016, 9(12): 1810-1819.

[39] AU M H, LIU J K, SUSILO W, et al. Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction[J]. Theoretical Computer Science, 2013, 469: 1-14.

[40] BOOTLE J, CERULLI A, CHAIDOS P, et al. Short accountable ring signatures based on DDH[C]//2015 European Symposium on Research in Computer Security (ESORICS). Berlin: Springer, 2015: 243-265.

[41] 包子健, 何德彪, 彭聪, 等. 基于SM2数字签名算法的可否认环签名[J]. 密码学报, 2023, 10(2): 264-275.
BAO Z J, HE D B, PENG C, et al. Deniable ring signature scheme based on SM2 digital signature algorithm[J]. Journal of Cryptologic Research, 2023, 10(2): 264-275.

[42] 丁勇, 罗世东, 杨昌松, 等. 基于SM9标识密码算法的可否认环签名方案[J]. 信息网络安全, 2024, 24(6): 893-902.
DING Y, LUO S D, YANG C S, et al. An identity-based deniable ring signature scheme based on SM9 signature algorithm[J]. Netinfo Security, 2024, 24(6): 893-902.

[43] BENDER A, KATZ J, MORSELLI R. Ring signatures: stronger definitions, and constructions without random oracles[J]. Journal of Cryptology, 2009, 22(1): 114-138.

[44] 谢振杰, 付伟, 罗芳. 国密算法Python工具包的性能优化方法[J]. 信息安全研究, 2023, 9(10): 1001-1007.
XIE Z J, FU W, LUO F. Performance optimization method of Python toolkit for domestic cryptographic algorithm[J]. Journal of Information Security Research, 2023, 9(10): 1001-1007.

[作者简介]

谢振杰（1995– ），男，湖南湘潭人，信息工程大学博士生，主要研究方向为云安全、密码学应用。

尹小康（1993– ），男，河南周口人，博士，信息工程大学讲师，主要研究方向为网络安全、二进制代码分析、机器学习。

蔡瑞杰（1990– ），男，河南开封人，信息工程大学博士生、讲师，主要研究方向为网络安全、二进制代码分析、漏洞挖掘。

张耀（1984– ），男，四川自贡人，信息工程大学博士生、工程师，主要研究方向为网络安全、源代码分析、漏洞挖掘。