基于国密算法SM9的环签密方案

谢振杰[1,2]，刘胜利[1]，谢耀滨[1]，李路凯[1]，卫明远[1]
（1.信息工程大学网络空间安全教育部重点实验室，河南 郑州 450001；2.中国人民解放军78156部队，重庆 400039）

摘　要：针对现有标识环签密方案计算开销随环成员规模线性增长的问题，提出一种基于国密算法SM9的高效环签密方案。该方案通过将涉及环成员的线性运算迁移至有限域，实现近似常数级的计算开销；采用新的私钥设计，签密时将签名与密钥要素封装于单个群元素，进一步降低了计算开销和通信开销。在随机预言机模型下，证明了所提方案满足机密性、不可伪造性和完全匿名性。实验表明，当环规模为1 024时，所提方案环签密和解密验证效率分别是现有方案的20.79倍和87.73倍，较最优环签名与加密的组合方案分别提升16.02%和46.86%。

关键词：环签密；国密算法；SM9算法；基于标识的密码；常数级开销；可证安全
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025244

Ring signcryption scheme based on domestic cryptographic algorithm SM9

XIE Zhenjie[1,2], LIU Shengli[1], XIE Yaobin[1], LI Lukai[1], WEI Mingyuan[1]
1. Key Laboratory of Cyberspace Security, Ministry of Education, Information Engineering University, Zhengzhou 450001, China
2. Unit 78156 of the Chinese People's Liberation Army, Chongqing 400039, China

Abstract: To address the linear computational increase with ring size in existing identity-based ring signcryption schemes, an efficient ring signcryption scheme based on the Chinese national cryptographic standard SM9 was proposed. Linear operations involving ring members were shifted to finite fields, achieving approximately constant computational cost. By redesigning the private key structure, signature and key components were encapsulated into a single group element during signcryption, further reducing both computational and communication overhead. Under the random oracle model, the proposed scheme was proven to satisfy confidentiality, unforgeability, and perfect anonymity. Experimental results show that for a ring size of 1 024, the signcryption and unsigncryption efficiencies of the proposed scheme are 20.79 and 87.73 times those of existing solutions, representing improvements of 16.02% and 46.86% over the optimal ring-signature-then-encryption combination, respectively.

Keywords: ring signcryption, domestic cryptographic algorithm, SM9 algorithm, identity-based cryptography, constant overhead, provable security

0　引言

现代密码学是网络安全的基石。物联网、云计算、区块链等前沿技术的广泛应用，离不开加密和数字签名等密码技术的坚实支撑。加密保护数据机密性，数字签名则实现身份认证、确保数据完整性并提供不可否认性。传统的系统常需同时应用签名和加密，但“先签名后加密”的做法会增加计算开销和密文长度，时空效率有待提升。

收稿日期：2025–08–05；修回日期：2025–12–16
通信作者：谢耀滨，yb_xie@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)

为应对这一挑战，Zheng[1]于1997年在美密会上首次提出签密概念。签密融合公钥密码与对称加密，通过单次运算即可同时完成签名和加密功能，且仅指定接收方能正确解密并验证签名有效性。相较于传统方式，签密技术能显著降低计算与通信开销。

然而，在需要群体匿名性的场景（如电子投票、敏感举报、匿名支付）中，不提供匿名保护的标准签密技术无法满足需求。Rivest等[2]提出了保证签名者身份匿名的环签名技术。环签名允许签名者代表一个任意选定的用户集合（称为“环”）生成签名，验证者能确认签名来自该环的某个成员，却无法确定具体身份，为签名者提供了匿名性保护。

因此，结合签密效率优势与环签名匿名特性的环签密技术应运而生。Huang等[3]首次提出环签密的概念，并在基于标识的密码（IBC, identity-based cryptography）体制下构造了一个环签密算法。环签密能在一次操作中为指定接收者生成一个来自特定环成员的机密且可验证的消息。它在保障机密性的同时，完美隐藏了签密者在环中的真实身份，适用于兼具匿名性和机密性要求的应用场景。

另一方面，基于公钥基础设施（PKI, public key infrastructure）的方案存在建设和维护代价较高的弊端，密集的证书请求易形成系统瓶颈。IBC体制则能规避证书依赖，直接使用用户唯一标识（如邮箱、手机号）作为公钥，不仅降低了对第三方证书机构的信任依赖，也为公钥管理提供了更简洁高效的路径。基于椭圆曲线双线性对的国密算法SM9是我国自主设计的IBC标准[4-5]，包含数字签名、密钥交换、密钥封装和加密。相比RSA等传统算法，SM9在相同安全强度下具有密钥短、效率高的优势，能有效提升系统安全与性能。近年来，基于SM9的密码方案研究蓬勃发展，涌现出环签名[6-7]、可搜索加密[8]、属性签名[9]、代理重加密[10]及容错加密[11]等成果，彰显了SM9优异的性能及其在密码应用领域的拓展潜力。

本文基于国密算法SM9设计了一种标识环签密方案，核心创新在于：在确保可证安全的前提下，深度整合环签名与密钥封装的核心步骤，成功将耗时运算的次数降至常数级。该方案采用与SM9数字签名算法一致的系统公共参数设置，通过重新设计用户私钥，将密钥信息与环签名要素融合封装于同一群元素，并将环成员相关的线性运算从原本的耗时运算（椭圆曲线标量乘、群G_T上的幂和双线性对）全部迁移至轻量的有限域内完成，最后在随机预言机模型（ROM, random oracle model）下证明了其机密性、不可伪造性和匿名性。经理论分析与实验评估，本文方案的计算开销和通信开销均明显优于同类方案及当前性能最优的SM9环签名与加密的组合方案。

1　相关工作

自Zheng[1]的开创性工作提出签密概念以来，早期方案多基于PKI体制。随着IBC兴起，首个基于标识的签密方案于2002年由Malone-Lee[12]提出，但其采用“先加密后签名”结构，难以满足语义安全要求。后续研究人员提出了更安全高效的改进方案[13-19]，其更关注特定应用场景（如物联网[20]）和新密码学基础（如格密码[21]、属性基[22]、三因素认证[23]）下的签密方案设计。赖建昌等[24]首次基于国密算法SM9设计签密方案，其计算和通信效率与同期国际标识签密方案相当，并在ROM下证明了机密性和不可伪造性。

自2005年环签密概念[3]提出以来，环签密研究在多类密码体制下展开。黄欣沂等[25]提出的标识环签密方案相比先签名后加密实现了密文长度的缩减。Zhu等[26]观察到，标识环签密方案多依赖双线性对，且运算次数随环成员规模线性增长，导致显著的计算开销，其设计的方案将双线性对次数恒定在4次，不随环成员数量增加而变化，从而在计算效率上较同类方案展现出显著优势。Guo等[27]提出了基于属性的环签密方案。Yu等[28]则基于格上困难问题构造了无证书的环签密方案。包嘉斌[29]针对车联网隐私保护需求，基于SM9提出了2个标识环签密方案，该方案在ROM下证明了其安全性，并在计算效率上优于当时的同类方案。Du等[30]针对车载自组织网络的条件隐私保护问题，提出了一种基于IBC体制的环签密方案，该方案改进了Cai等[31]方案的安全性问题并提高了计算效率。罗铭等[32]为实现车辆到公钥基础设施的跨域通信，基于无证书密码体制与椭圆曲线密码构造了条件隐私保护的环签密方案，实现了较低的签密、验证和追

踪成本。总体而言，现有方案仅对签名和加密步骤进行简单合并，在二者深度整合方面仍有优化空间，且当前基于SM9的环签密（包括签密）的代表性成果有限。此外，环签密的效率瓶颈往往在于环签名，环签名的最新研究成果对于环签密研究也有重要参考价值。

环签密方案的安全性涉及机密性、不可伪造性和匿名性，其严格证明需坚实的理论基础。分叉引理[33]及其在环签名[34]、标识签名[35]和标识环签名[36]领域的扩展，为证明方案的不可伪造性提供了核心工具。国密算法SM9的安全性已得到严格证明：Cheng[37]基于Gap-q-BCAA1假设证明了SM9密钥封装机制在ROM下自适应选择密文攻击下的不可区分性（IND-CCA, indistinguishability against adaptive chosen-ciphertext attack）；赖建昌等[38]基于q-SDH和q-BDHI假设，分别证明了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）和改进的Twin-SM9密钥封装机制的IND-CCA安全性；Selvi等[39]完善了标识环签密的安全模型，系统分析了几个经典方案的安全性。上述成果在理论和实践上为基于SM9的环签密构建了可证安全框架。

2 预备知识

本节描述本文的主要符号，以及标识环签密的困难问题、系统模型和安全模型。

2.1 符号含义

表1列出了本文使用的主要符号及含义，未列出的符号在首次出现时说明。

在困难问题实例及安全性证明中，群G_1, G_2的生成元需与方案公开参数P_1, P_2有所区分，故分别用P, Q表示，且满足$P=\psi(Q)$。

2.2 困难问题

所提方案的安全性与以下困难问题相关[37-38]。

定义1 q-SDH问题（q-strong Diffie-Hellman problem）。令秘密整数$a\in Z_N^*$，给定$q+2$个元素$(P, Q, [a]Q, [a^2]Q, \cdots, [a^q]Q)\in G_1\times G_2^{q+1}$，计算任意一组$\left(c,\left[\frac{1}{c+a}\right]P\right)$，其中$c\in Z_N$。

定义2 DBIDH问题（decision bilinear inversion Diffie-Hellman problem）。令秘密整数$a,b,r\in Z_N^*$，区分$(P_1, P_2, [a]P_i, [b]P_j, e(P_1,P_2)^{\frac{b}{a}})$和$(P_1, P_2, [a]P_i, [b]P_j, e(P_1,P_2)^r)$，其中$i,j\in\{1,2\}$。

定义3 q-BDHI问题（q-bilinear Diffie-Hellman inversion problem）。令秘密整数$a\in Z_N^*$，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$e(P,Q)^{\frac{1}{a}}$。

定义4 Gap-q-BDHI问题。令秘密整数$a\in Z_N^*$，给定$q+2$个元素$(P, Q, [a]Q, [a^2]Q, \cdots, [a^q]Q)\in G_1\times G_2^{q+1}$和DBIDH确定算法，计算$e(P,Q)^{\frac{1}{a}}$。

表1 主要符号及含义

符号	含义	符号	含义
G_1, G_2	椭圆曲线加法循环群	λ	安全参数
G_T	乘法循环群	**params**	系统公开参数
N	大素数，群G_1, G_2, G_T的阶	**msk**	主私钥
P_1, P_2	群G_1, G_2的生成元	ID	用户身份标识
Z_N^*	$[1, N-1]$范围内整数构成的群	**sk**	用户私钥
Z_N	$[0, N-1]$范围内整数构成的群	M	原始消息
ψ	同态映射：$G_2\to G_1$	U	环成员集合$\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$
e	双线性对：$G_1\times G_2\to G_T$	**SC**	环签密消息
H_1, H_2	哈希函数：$\{0,1\}^*\to Z_N^*$	klen	密钥的比特位数
$[k]P$	椭圆曲线点P的k倍（标量乘）	KDF	密钥派生函数：$\{0,1\}^*\to\{0,1\}^{\mathrm{klen}}$
$x\Vert y$	x与y的字节串拼接	$\mathrm{Enc}_K(M)$	以密钥K对消息M执行对称加密
$x\in_R X$	从X（集合、群等）中随机选择元素x	$\mathrm{Dec}_K(C)$	以密钥K对密文C执行对称解密

如果上述各问题在多项式时间内的求解概率可忽略，则其困难假设成立。上述问题的困难性可规约到G_1, G_2, G_T上离散对数问题的困难性，它们是基于双线性对的IBC体制安全性的基石。

2.3　系统模型

标识环签密方案一般包含4项算法[3]，模型描述如表2所示。其中，KGC表示密钥生成中心，PPT表示概率多项式时间；签密者标识为$\mathrm{ID}_\pi \in U$（私钥为$\mathbf{sk}_\pi$），接收者标识为ID_R（私钥为$\mathbf{sk}_\mathrm{R}$）；Unsigncrypt算法验证通过时输出原始消息，解密失败或验证不通过时输出⊥。

正确的标识环签密方案应满足：合法的环签密消息–定通过验证（即对于$\mathrm{ID}_\pi \in U$，式(1)成立），非法消息的通过概率可忽略。

$$\Pr\left[\mathrm{Unsigncrypt}(\mathbf{params},\mathbf{SC},U,sk_\mathrm{R}) \to M \;\middle|\; \begin{array}{c}\mathrm{Setup}(\lambda) \to (\mathbf{params},\mathbf{msk})\\ \mathrm{KeyGen}(\mathbf{params},\mathrm{ID}_\pi,\mathbf{msk}) \to \mathbf{sk}_\pi\\ \mathrm{KeyGen}(\mathbf{params},\mathrm{ID}_\mathrm{R},\mathbf{msk}) \to \mathbf{sk}_\mathrm{R}\\ \mathrm{RingSigncrypt}(\mathbf{params},M,U,\mathrm{ID}_\mathrm{R},\mathbf{sk}_\pi) \to \mathbf{SC}\end{array}\right] = 1$$

2.4　安全模型

标识环签密必须同时具备公钥加密和环签名的安全特性[39]：机密性，由IND-CCA定义；不可伪造性，由EUF-CMIA定义；匿名性。具体介绍如下。

定义5　IND-CCA。该性质由挑战者D与PPT敌手A的交互游戏定义。

1)初始化。D生成(**params**, **msk**)并公开**params**。

2)询问1。A按需向D查询给定输入的私钥、环签密或解密验证结果。

3)挑战。A向D提供2个等长的消息(M_0^*, M_1^*)、挑战用户集合U^*和接收者标识ID_R^*，要求A从未询问过ID_R^*的私钥。D选择$b \in_\mathrm{R} \{0,1\}$和签密者$\mathrm{ID}^* \in_\mathrm{R} U^*$，生成$(M_b^*, U^*, \mathrm{ID}_\mathrm{R}^*)$的环签密消息$\mathbf{SC}^*$并发送至$A$。

4)询问2。同询问1，但要求A不能询问ID_R^*的私钥，也不能对$\mathbf{SC}^*$发起解密验证询问。

5)猜测。A输出$b' \in \{0,1\}$，若$b' = b$，则A获胜。

令negl(λ)为可忽略函数（输出随λ扩大而迅速趋于零），若A获胜的优势为$\mathrm{Adv}_A^{\mathrm{IND\text{-}CCA}} = \Pr[b' = b] - \frac{1}{2} \leqslant \mathrm{negl}(\lambda)$，则该标识环签密方案满足IND-CCA安全性。

定义6　EUF-CMIA。与定义5的交互游戏类似且步骤1)和步骤2)相同，区别如下。

3)伪造。A输出挑战用户集合U^*、接收者标识ID_R^*和环签密消息$\mathbf{SC}^*$（U^*中标识对应的私钥及$(M^*, U^*, \mathrm{ID}_\mathrm{R}^*)$的环签密均未被询问）。若$\mathbf{SC}^*$解密得出$M^*$并通过验证，则$A$获胜。

令接收者私钥为$\mathbf{sk}_\mathrm{R}^*$，若A获胜的优势为$\mathrm{Adv}_A^{\mathrm{EUF}} = \Pr[\mathrm{Unsigncrypt}(\mathbf{params}, \mathbf{SC}^*, U^*, \mathbf{sk}_\mathrm{R}^*) \to M^*] \leqslant \mathrm{negl}(\lambda)$，则该标识环签密方案满足EUF-CMIA安全性。

定义7　匿名性。与定义5的交互游戏类似且步骤1)、步骤2)和步骤5)相同，区别如下。

3)挑战。A向D提供消息M^*、挑战用户集合U^*、接收者标识ID_R^*和2个标识$\mathrm{ID}_1^*, \mathrm{ID}_2^* \in U^*$。$D$选择$b \in_\mathrm{R} \{0,1\}$，用$\mathrm{ID}_b^*$的私钥生成$(M^*, U^*, \mathrm{ID}_\mathrm{R}^*)$的环签密消息$\mathbf{SC}^*$并发送至$A$。

4)询问2。同询问1。

若A获胜的优势为$\mathrm{Adv}_A^{\mathrm{ANON}} = \Pr[b' = b] - \frac{1}{2} \leqslant \mathrm{negl}(\lambda)$，则该标识环签密方案满足匿名性。

3　方案构造

本节描述基于SM9的环签密方案的各项算法。

表2　标识环签密系统模型

算法名称	中文含义	执行者	算法性质	输入	输出
Setup	系统建立	KGC	PPT算法	λ	**params**, **msk**
KeyGen	用户私钥生成	KGC	确定性算法	**params**, ID, **msk**	**sk**
RingSigncrypt	环签密	签密者	PPT算法	**params**, M, U, ID_R, $\mathbf{sk}_\pi$	**SC**
Unsigncrypt	解密验证	接收者	确定性算法	**params**, **SC**, U, $\mathbf{sk}_\mathrm{R}$	M/⊥

3.1 Setup

KGC选定一个1 B大小的私钥生成函数识别符hid，生成主私钥$\mathrm{ks}\in{}_{\mathrm{R}}Z_N^*$，计算主公钥$P_{\text{pub-s}}=[\mathrm{ks}]P_2\in G_2$，公开$P_{\text{pub-s}}$和hid。为简化表述，后文以$H_1(\mathrm{ID})$指代$H_1(\mathrm{ID}\|\mathrm{hid},N)$。

3.2 KeyGen

设用户标识为ID，KGC计算$v=H_1(\mathrm{ID})\in Z_N^*$、签名私钥$\mathrm{ds}=\left[\frac{\mathrm{ks}}{v+\mathrm{ks}}\right]P_1\in G_1$和解密私钥$\mathrm{de}=\left[\frac{\mathrm{ks}^2}{v+\mathrm{ks}}\right]P_2\in G_2$，以秘密渠道向用户发送私钥元组$\mathbf{sk}=(\mathrm{ds},\mathrm{de})$。若$v+\mathrm{ks}=0$，则主密钥$(\mathrm{ks},P_{\text{pub-s}})$和全部用户的私钥均需更换。

3.3 RingSigncrypt

令签密者标识为$\mathrm{ID}_\pi\in U$（U中包含n个成员，$\pi\in\{1,2,\cdots,n\}$），接收者标识为ID_{R}。签密者（签名私钥为ds_π）预先计算$g_0=e(P_1,P_{\text{pub-s}})\in G_T$, $g_1=e(\mathrm{ds}_\pi,P_2)\in G_T$, $g_2=e(\mathrm{ds}_\pi,P_{\text{pub-s}})\in G_T$，环签密计算步骤如下。

1)$r,r_0\in{}_{\mathrm{R}}Z_N^*$，$\omega=g_0{}^{r\,r_0}\in G_T$。

2)$v_i=H_1(\mathrm{ID}_i)\in Z_N^*$，$i=1,2,\cdots,n$。

3)r_1，r_2，$\cdots$，$r_{\pi-1}$，$r_{\pi+1}$，$\cdots$，r_n，$\rho\in{}_{\mathrm{R}}Z_N^*$，$\beta=\left(g_1{}^{r\sum\limits_{i=1,i\neq\pi}^{n}r_iv_i}\cdot g_2{}^{r\sum\limits_{i=1,i\neq\pi}^{n}r_i}\cdot g_0{}^{r\rho}\right)^{-1}\in G_T$。

4)$h=H_2(U\|M\|\omega\|\beta)\in Z_N^*$。

5)$r_\pi=\frac{r\,r_0-h}{r}+\rho\in Z_N^*$，若$r_\pi=0$，则返回步骤1)。

6)$v_{\mathrm{R}}=H_1(\mathrm{ID}_{\mathrm{R}})\in Z_N^*$，$S=\left[r\left(1-\frac{v_{\mathrm{R}}}{v_\pi}\right)\right]\mathrm{ds}_\pi+\left[r\frac{v_{\mathrm{R}}}{v_\pi}\right]P_1\in G_1$。

7)$K=\mathrm{KDF}(r_1\|r_2\|\cdots\|r_n\|\omega\|\mathrm{ID}_{\mathrm{R}})$。

8)$C=\mathrm{Enc}_K(M)$。

9)输出环签密消息$\mathbf{SC}=(C,h,S,\beta,r_1,r_2,\cdots,r_n)$。

3.4 Unsigncrypt

接收者（标识为ID_{R}，解密私钥为de_{R}）预先计算$g_0=e(P_1,P_{\text{pub-s}})\in G_T$，收到$U'=\{\mathrm{ID}_1',\mathrm{ID}_2',\cdots,\mathrm{ID}_n'\}$的环签密消息$\mathbf{SC}'=(C',h',S',\beta',r_1',r_2',\cdots,r_n')$后，计算步骤如下。

1)检查$h',r_1',r_2',\cdots,r_n'\in Z_N^*$、$S'\in G_1$和$\beta'\in G_T$，若任何一项不符合，则中止并输出⊥。

2)$v_i=H_1(\mathrm{ID}'_i)\in Z_N^*$，$i=1,2,\cdots,n$。

3)$T=\left[\sum\limits_{i=1}^{n}r_i'-\frac{\sum\limits_{i=1}^{n}r_i'v_i}{v_{\mathrm{R}}}\right]\mathrm{de}_{\mathrm{R}}+\left[\frac{\sum\limits_{i=1}^{n}r_i'v_i}{v_{\mathrm{R}}}\right]P_{\text{pub-s}}\in G_2$。

4)$\omega'=e(S',T)\cdot g_0^{h'}\cdot\beta'\in G_T$。

5)$K'=\mathrm{KDF}(r_1'\|r_2'\|\cdots\|r_n'\|\omega'\|\mathrm{ID}_{\mathrm{R}})$。

6)$M'=\mathrm{Dec}_K(C')$。

7)$h''=H_2(U'\|M'\|\omega'\|\beta')\in Z_N^*$。

8)检验$h''=h'$是否成立，若成立，则验证通过并输出M'，否则输出⊥。

4 方案性质推导与证明

本节通过理论推导和安全规约，证明方案的正确性、机密性、不可伪造性和匿名性。

4.1 正确性

若各方正确运行算法，且$U=U'$, $\mathbf{SC}=\mathbf{SC}'$，则ω'推导过程为

$$\omega'=e(S',T)\cdot g_0{}^{h'}\cdot\beta'=e\left(\left[r\left(1-\frac{v_{\mathrm{R}}}{v_\pi}\right)\right]\mathrm{ds}_\pi+\left[r\frac{v_{\mathrm{R}}}{v_\pi}\right]P_1,\left[\sum_{i=1}^{n}r_i-\frac{\sum\limits_{i=1}^{n}r_iv_i}{v_{\mathrm{R}}}\right]\mathrm{de}_{\mathrm{R}}+\left[\frac{\sum\limits_{i=1}^{n}r_iv_i}{v_{\mathrm{R}}}\right]P_{\text{pub-s}}\right)\cdot g_0{}^{h}\cdot\beta=$$

$$e\left(\left[r\frac{(v_\pi-v_{\mathrm{R}})\mathrm{ks}}{v_\pi(v_\pi+\mathrm{ks})}+r\frac{v_{\mathrm{R}}(v_\pi+\mathrm{ks})}{v_\pi(v_\pi+\mathrm{ks})}\right]P_1,\left[\frac{(v_{\mathrm{R}}\sum\limits_{i=1}^{n}r_i-\sum\limits_{i=1}^{n}r_iv_i)\mathrm{ks}^2}{v_{\mathrm{R}}(v_{\mathrm{R}}+\mathrm{ks})}+\frac{\sum\limits_{i=1}^{n}r_iv_i\,(v_{\mathrm{R}}+\mathrm{ks})\mathrm{ks}}{v_{\mathrm{R}}(v_{\mathrm{R}}+\mathrm{ks})}\right]P_2\right)\cdot g_0{}^{h}\cdot\beta=$$

$$e\left(\left[r\frac{v_{\mathrm{R}}+\mathrm{ks}}{v_\pi+\mathrm{ks}}\right]P_1,\left[\frac{(\mathrm{ks}\sum\limits_{i=1}^{n}r_i+\sum\limits_{i=1}^{n}r_iv_i)\mathrm{ks}}{v_{\mathrm{R}}+\mathrm{ks}}\right]P_2\right)\cdot g_0{}^{h}\cdot\left(g_1{}^{r\sum\limits_{i=1,i\neq\pi}^{n}r_iv_i}\cdot g_2{}^{r\sum\limits_{i=1,i\neq\pi}^{n}r_i}\cdot g_0{}^{r\rho}\right)^{-1}=$$

$$e(\mathrm{ds}_\pi,[r(\mathrm{ks}\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}r_iv_i)]P_2)\cdot e(\mathrm{ds}_\pi,[r\sum_{i=1,i\neq\pi}^{n}r_iv_i]P_2)^{-1}\cdot e(\mathrm{ds}_\pi,[r\sum_{i=1,i\neq\pi}^{n}r_i\cdot\mathrm{ks}]P_2)^{-1}\cdot g_0^{h-r\rho}=$$

$$e(\mathrm{ds}_\pi,[rr_\pi(v_\pi+\mathrm{ks})]P_2)\cdot g_0^{h-r\rho}=e\left([\mathrm{ks}]P_1,\left[r\left(\frac{rr_0-h}{r}+\rho\right)\right]P_2\right)\cdot g_0^{h-r\rho}=g_0^{rr_0-h+r\rho+h-r\rho}=g_0^{rr_0}=\omega$$

故$K=K'$，$M=M'$，$h''=h=h'$。本文方案的正确性得证。

4.2　机密性

通过安全规约证明本文方案符合IND-CCA安全性。为避免考虑对称密码算法的安全性，令加解密采用模2加法，即$C=M\oplus K$，此假设不影响证明的有效性，也简化了证明流程。此外，约定签密者和接收者的标识不相同。

定理1　若H_1, H_2, KDF是随机预言机（RO, random oracle），且Gap-q-BDHI问题是困难的，则本文方案在IND-CCA模型下是安全的。

证明　假设IND-CCA模型中的PPT敌手A获胜的优势ε不可忽略，则可构建模拟器B求解Gap-q-BDHI问题。B掌握可解决DBIDH问题的预言机O_{DBIDH}，接收q-BDHI问题实例$(P, Q, [a]Q, [a^2]Q, \cdots, [a^q]Q)$后，与$A$的交互如下。

初始化。B生成$q-1$个两两互异的整数$w^*,w_1,w_2,\cdots,w_{q-2}\in_{\mathrm{R}}Z_N^*$，令多项式$f(x)=\prod_{i=1}^{q-2}(w_i+x-w^*)$，由问题实例和$f(x)$计算$P_1=[f(a)]P$，$P_2=[f(a)]Q$，$P_{\text{pub-s}}=[(a-w^*)f(a)]Q$（$\mathrm{ks}=a-w^*$隐式存在；计算$P_1$时，有$[a^i]P=\psi([a^i]Q)$，$i=0,1,\cdots,q$），生成$i^*\in_{\mathrm{R}}\{1,2,\cdots,q-2\}$，建立3个记录哈希询问的列表$L_1, L_2, L_3$。

哈希询问。H_1、H_2、KDF是B掌握的RO，令非重复询问数分别为q_{H_1}、q_{H_2}、q_{KDF}，且$q_{H_1}=q-2$。A（或B自身）随时可发起询问，若L_1, L_2, L_3存在询问记录，则直接答复；否则，B处理如下。

1) H_1询问。设第i次询问的输入为ID_i，答复$H_1(\mathrm{ID}_i)=\begin{cases}w^*, i=i^*\\ w_i, i\neq i^*\end{cases}$，将$(i,\mathrm{ID}_i,H_1(\mathrm{ID}_i))$记录至$L_1$。

2) H_2询问。设第j次询问的输入为U_j、M_j以及$\omega_j,\beta_j\in G_T$，生成$h_j\in_{\mathrm{R}}Z_N^*$，答复$H_2(U_j\|M_j\|\omega_j\|\beta_j)=h_j$，将$(j,U_j,M_j,\omega_j,\beta_j,h_j)$记录至$L_2$。

3) KDF询问。设第k次询问的输入为整数序列$\boldsymbol{Z}_k=(r_{1,k}, r_{2,k}, \cdots, r_{n,k})$、$\omega_k\in G_T$和$\mathrm{ID}_{\mathrm{R},k}$，生成$K_k\in_{\mathrm{R}}\{0,1\}^{\mathrm{klen}}$，答复$\mathrm{KDF}(\boldsymbol{Z}_k\|\omega_k\|\mathrm{ID}_{\mathrm{R},k})=K_k$，将$(k, \boldsymbol{Z}_k, \omega_k, \mathrm{ID}_{\mathrm{R},k}, K_k)$记录至$L_3$。

询问1。该阶段A可按需向B进行以下询问。

1) 私钥询问。设输入为ID_i，B查找L_1记录$(i,\mathrm{ID}_i,H_1(\mathrm{ID}_i))$（若无，先进行$H_1$询问）。若$i=i^*$，则中止；否则，$B$令多项式$f_i(x)=(x-w^*)\prod_{j=1,j\neq i}^{q-2}(w_j+x-w^*)$，由问题实例和$f_i(x)$计算

$$\mathrm{ds}_i=[f_i(a)]P=\left[\frac{(a-w^*)f(a)}{w_i+a-w^*}\right]P=\left[\frac{\mathrm{ks}}{H_1(\mathrm{ID}_i)+\mathrm{ks}}\right]P_1$$

$$\mathrm{de}_i=[(a-w^*)f_i(a)]Q=\left[\frac{(a-w^*)^2f(a)}{w_i+a-w^*}\right]Q=\left[\frac{\mathrm{ks}^2}{H_1(\mathrm{ID}_i)+\mathrm{ks}}\right]P_2$$

然后返回私钥$\mathbf{sk}_i=(\mathrm{ds}_i, \mathrm{de}_i)$。

2) 环签密询问。设输入为$M, U, \mathrm{ID}_{\mathrm{R}}$，$B$选择$\mathrm{ID}_\pi\in_{\mathrm{R}}U$（$\pi\neq i^*$），利用其签名私钥$\mathrm{ds}_\pi$计算环签密消息$\mathbf{SC}$并返回。

3) 解密验证询问。设输入为$U=\{\mathrm{ID}_{l_1},\mathrm{ID}_{l_2},\cdots,\mathrm{ID}_{l_n}\}$, ID_{R}, $\mathbf{SC}=(C, h, S, \beta, r_1, r_2, \cdots, r_n)$，若$\mathrm{ID}_{\mathrm{R}}\neq\mathrm{ID}_{i^*}$，$B$可利用解密私钥$\mathrm{de}_{\mathrm{R}}$执行解密验证；否则，$B$执行以下步骤。

①遍历列表L_1，若U中任意元素或ID_{R}未在L_1中出现过，则返回$\perp$并结束，否则执行步骤②。

②遍历列表L_2，令满足$U_j=U, \beta_j=\beta, h_j=h$的记录$(j,U_j,M_j,\omega_j,\beta_j,h_j)$构成集合$V$，执行步骤③。

③若$V=\varnothing$，则返回$\perp$并结束，否则随机移除V中一条记录$(j, U, M_j, \omega_j, \beta, h)$并对其执行步骤④。

④计算$K_j=C\oplus M_j$，遍历列表L_3查找$(r_1, r_2, \cdots, r_n, \omega_j, \mathrm{ID}_{\mathrm{R}}, K_j)$，若找到该记录，则执行步骤⑤，否则返回步骤③。

⑤向O_{DBIDH}询问$(P_1, [((a-w^*)\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}r_iw_{l_i})(a-w^*)f(a)]Q, [a\cdot f(a)]P, S, \omega_j\cdot g_0^{-h}\cdot\beta^{-1})$，若$O_{\mathrm{DBIDH}}$返回1，则向$A$返回$M_j$作为解

密结果并结束，否则返回步骤③。

预言机O_{DBIDH}可解决定义2描述的$i=j=1$时的DBIDH问题，即询问形如$(P_1, P_2, [a]P_1, [b]P_1, y)\in G_1\times G_2\times G_1^2\times G_T$的5元组，若$y=e(P_1,P_2)^{\frac{b}{a}}$，则返回1，否则返回0。

若A伪造了能通过解密验证的**SC**，必定成功求解了U中某标识ID_{l_π}对应的签名私钥ds_{l_π}（$\pi\in\{1,2,\cdots,n\}$），并正确发起H_1, H_2, KDF询问。因为$H_1(\mathrm{ID_R})=w^*$，$H_1(\mathrm{ID_R})+\mathrm{ks}=w^*+a-w^*=a$，又因为$H_1(\mathrm{ID}_{l_i})=w_{l_i}$（$i=1,2,\cdots,n$），$\omega_j=g_0^{rr_0}$，则$O_{\mathrm{DBIDH}}$询问中元素的推导过程为

$$[a\cdot f(a)]P=[a]P_1$$

$$S=\left[r\left(1-\frac{H_1(\mathrm{ID_R})}{H_1(\mathrm{ID}_{l_\pi})}\right)\right]\mathrm{ds}_{l_\pi}+\left[r\frac{H_1(\mathrm{ID_R})}{H_1(\mathrm{ID}_{l_\pi})}\right]P_1=$$

$$\left[r\frac{H_1(\mathrm{ID_R})+\mathrm{ks}}{H_1(\mathrm{ID}_{l_\pi})+\mathrm{ks}}\right]P_1=\left[\frac{r\cdot a}{w_{l_\pi}+a-w^*}\right]P_1$$

$$e\left(\left[\frac{r\cdot a}{\left(w_{l_\pi}+a-w^*\right)a}\right]P_1,\right.$$

$$\left.\left[\left((a-w^*)\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}r_iw_{l_i}\right)(a-w^*)f(a)\right]Q\right)=$$

$$e\left(\left[\frac{r}{H_1(\mathrm{ID}_{l_\pi})+\mathrm{ks}}\right]P_1,\right.$$

$$\left.\left[\left(\mathrm{ks}\sum_{i=1}^{n}r_i+\sum_{i=1}^{n}r_iH_1(\mathrm{ID}_{l_i})\right)\mathrm{ks}\right]P_2\right)=$$

$$e(\mathrm{ds}_{l_\pi},[r(\mathrm{ks}\sum_{i=1,i\neq\pi}^{n}r_i+\sum_{i=1,i\neq\pi}^{n}r_iH_1(\mathrm{ID}_{l_i}))]P_2+$$
$$[rr_\pi(H_1(\mathrm{ID}_{l_\pi})+\mathrm{ks})]P_2)=$$

$$g_1^{r\sum_{i=1,i\neq\pi}^{n}r_iH_1(\mathrm{ID}_{l_i})}\cdot g_2^{r\sum_{i=1,i\neq\pi}^{n}r_i}\cdot g_0^{rr_0-h+r\rho}=$$
$$\omega_j\cdot g_0^{-h}\cdot\beta^{-1}$$

当且仅当**SC**可正确解密时，O_{DBIDH}返回1。因此，即使B不掌握接收者ID_{i^*}的私钥，也可利用L_1, L_2, L_3的记录和O_{DBIDH}来模拟解密验证。

挑战。A输出挑战用户集合$U^*=\{\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_n^*\}$（$n<q-2$）、接收者标识$\mathrm{ID}_{\mathrm{R}}^*$和2个等长的消息$(M_0^*, M_1^*)$，且$A$从未询问过$\mathrm{ID}_{\mathrm{R}}^*$的私钥。若$\mathrm{ID}_{\mathrm{R}}^*\neq\mathrm{ID}_{i^*}$，则中止；否则，有$H_1(\mathrm{ID}_{\mathrm{R}}^*)=w^*$。记$H_1(\mathrm{ID}_{i^*})=w_{i^*}^*\in\{w_1, w_2, \cdots, w_{q-2}\}$，$i=1,2,\cdots,n$。$B$选择$\mathrm{ID}_\pi^*\in{}_{\mathrm{R}}U^*, \pi\in\{1,2,\cdots,n\}$，生成与$M_0^*/M_1^*$等长的随机比特串$R$，$r',h^*,r_1^*,r_2^*,\cdots,r_n^*\in{}_{\mathrm{R}}Z_N^*$，$\beta^*\in{}_{\mathrm{R}}G_T$，计算$S^*=\left[\frac{r'\cdot f(a)}{w_\pi^*+a-w^*}\right]P$，将模拟的环签密消息$\mathbf{SC}^*=(R,h^*,S^*,\beta^*,r_1^*,r_2^*,\cdots,r_n^*)$返回给$A$。

S^*可视为以随机数$r^*=\frac{r'}{a}$模拟生成，这是因为

$$S^*=\left[r^*\left(1-\frac{H_1(\mathrm{ID}_{\mathrm{R}}^*)}{H_1(\mathrm{ID}_\pi^*)}\right)\right]\mathrm{ds}_\pi^*+\left[r^*\frac{H_1(\mathrm{ID}_{\mathrm{R}}^*)}{H_1(\mathrm{ID}_\pi^*)}\right]P_1=$$

$$\left[r^*\frac{H_1(\mathrm{ID}_{\mathrm{R}}^*)+\mathrm{ks}}{H_1(\mathrm{ID}_\pi^*)+\mathrm{ks}}\right]P_1=$$

$$\left[\frac{r^*\cdot a}{w_\pi^*+a-w^*}\right]P_1=\left[\frac{r'\cdot f(a)}{w_\pi^*+a-w^*}\right]P$$

所以，A在解密出原始消息（Unsigncrypt步骤6)）前，无法区分$\mathbf{SC}^*$是否为模拟的。

询问2。同询问1，但要求A不能询问$\mathrm{ID}_{\mathrm{R}}^*$的私钥，也不能对$\mathbf{SC}^*$发起解密验证询问。

猜测。A输出猜测结果$b'\in\{0,1\}$。

B忽略A的猜测。若A成功求解$\mathrm{ID}_{\mathrm{R}}^*$对应的解密私钥$\mathrm{de}_{\mathrm{R}}^*$，那么在解密过程中，有

$$T^*=\left[\sum_{i=1}^{n}r_i^*-\frac{\sum_{i=1}^{n}r_i^*H_1(\mathrm{ID}_i^*)}{H_1(\mathrm{ID}_{\mathrm{R}}^*)}\right]\mathrm{de}_{\mathrm{R}}^*+$$

$$\left[\frac{\sum_{i=1}^{n}r_i^*H_1(\mathrm{ID}_i^*)}{H_1(\mathrm{ID}_{\mathrm{R}}^*)}\right]P_{\mathrm{pub\text{-}s}}=$$

$$\left[\frac{(\mathrm{ks}\sum_{i=1}^{n}r_i^*+\sum_{i=1}^{n}r_i^*H_1(\mathrm{ID}_i^*))\mathrm{ks}}{H_1(\mathrm{ID}_{\mathrm{R}}^*)+\mathrm{ks}}\right]P_2=$$

$$\left[\frac{((a-w^*)\sum_{i=1}^{n}r_i^*+\sum_{i=1}^{n}r_i^*w_i^*)(a-w^*)f(a)}{a}\right]Q$$

令

$$\frac{r'((x-w^*)\sum_{i=1}^{n}r_i^*+\sum_{i=1}^{n}r_i^*w_i^*)(x-w^*)f^2(x)}{x(w_\pi^*+x-w^*)}=$$

$$F_1(x)x^{q-2}+F_2(x)+\frac{d}{x}$$

其中，$w_\pi^*+x-w^*$是$f(x)$的因子；多项式$F_1(x)$和$F_2(x)$的次数均为$q-2$，系数及非零整数d均由所选参数计算。则有

$$\omega^*=e(S^*,T^*)\cdot g_0^{h^*}\cdot\beta^*=$$

$$e\left(P,\left[\frac{r'((a-w^*)\sum_{i=1}^{n}r_i^*+\sum_{i=1}^{n}r_i^*w_i^*)(a-w^*)f^2(a)}{a(w_\pi^*+a-w^*)}\right]Q\right)\cdot$$

$$g_0^{h^*}\cdot\beta^*=e$$

$$\left(P,\left[F_1(a)a^{q-2}+F_2(a)+\frac{d}{a}\right]Q\right)\cdot g_0^{h^*}\cdot\beta^*$$

L_3中必有记录包含ω^*，B计算

$$\left(\frac{\omega^*}{e([a^{q-2}]P,[\mathrm{F}_1(a)]Q)\cdot e(P,[\mathrm{F}_2(a)]Q)\cdot g_0^{h^*}\cdot\beta^*}\right)^{\frac{1}{d}}=$$

$$\left(\frac{e\left(P,\left[F_1(a)a^{q-2}+F_2(a)+\frac{d}{a}\right]Q\right)\cdot g_0^{h^*}\cdot\beta^*}{e(P,[F_1(a)a^{q-2}+F_2(a)]Q)\cdot g_0^{h^*}\cdot\beta^*}\right)^{\frac{1}{d}}=$$

$$e\left(P,\left[\frac{d}{a}\right]Q\right)^{\frac{1}{d}}=e(P,Q)^{\frac{1}{a}}$$

并将其作为Gap-q-BDHI问题实例的解。

以下是对B成功模拟的概率和破解Gap-q-BDHI问题优势的分析。首先，只有当A挑战的接收者标识恰好为ID_{i^*}时，B才能成功模拟，此概率为$\frac{1}{q_{H_1}}$。其次，在成功模拟的基础上，根据假设，A能以不可忽略的优势ε区分所选消息的密文，则A将以ε概率向KDF发起包含ω^*的挑战询问。令(k, $r_1^*,r_2^*,\cdots,r_n^*$, ω_k, ID_R^*, K_k)为L_3中可能包含ω^*的记录，逐一向O_{DBIDH}询问(P_1, $[((a-w^*)\sum_{i=1}^{n}r_i^*+\sum_{i=1}^{n}r_i^*w_i^*)(a-w^*)f(a)]Q$, $[a\cdot f(a)]P$, S^*, $\omega_k\cdot(g_0^{h^*}\cdot\beta^*)^{-1}$)，当$O_{\mathrm{DBIDH}}$返回1时有$\omega_k=\omega^*$（推导过程同解密验证询问），即只要$L_3$中包含挑战询问，$B$可在$O_{\mathrm{DBIDH}}$的帮助下找到$\omega^*$。因此，若假设成立，则$B$解决Gap-$q$-BDHI问题的优势为$\frac{\varepsilon}{q_{H_1}}$。由于$q_{H_1}$是有界常数，此优势仍不可忽略，与Gap-$q$-BDHI假设相矛盾，故本文方案在IND-CCA模型下是安全的。证毕。

4.3　不可伪造性

通过安全规约证明本文方案符合EUF-CMIA安全性。

定理 2　若H_1, H_2, KDF是RO，且q-SDH问题是困难的，则本文方案在EUF-CMIA模型下是安全的。

证明　假设EUF-CMIA模型中的PPT敌手A获胜的优势ε不可忽略，则可构建模拟器B求解q-SDH问题。B接收q-SDH问题实例$(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)$后，与$A$的交互如下。

1)初始化。除$f(x)=\prod_{i=1}^{q-2}(w_i+x)$、$P_{\text{pub-s}}=[af(a)]Q$、$\mathrm{ks}=a$，其余与4.2节相同。

2)哈希询问。与4.2节相同。

3)询问。该阶段A可按需向B进行以下询问。

①私钥询问。除$f_i(x)=x\prod_{j=1,j\neq i}^{q-2}(w_j+x)$，$\mathrm{ds}_i=[f_i(a)]P=\left[\frac{a\cdot f(a)}{w_i+a}\right]P=\left[\frac{\mathrm{ks}}{H_1(\mathrm{ID}_i)+\mathrm{ks}}\right]P_1$，$\mathrm{de}_i=[a\cdot f_i(a)]Q=\left[\frac{a^2\cdot f(a)}{w_i+a}\right]$，其余与4.2节相同。

②环签密询问。与4.2节相同。

③解密验证询问。与4.2节相同。

4)伪造。A输出挑战用户集合$U^*=\{\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_n^*\}$、接收者标识$\mathrm{ID}_\mathrm{R}^*$和环签密消息$\mathbf{SC}^*$（$U^*$中标识对应的私钥及($M^*$, U^*, ID_R^*)的环签密均未被询问）。若$\mathrm{ID}_{i^*}\notin U^*$，则中止；否则，根据分叉引理，若$A$在未持有$U^*$中任一用户私钥时伪造了有效的$\mathbf{SC}^*$，则$B$可构造图灵机$A'$，在$A$的帮助下以同一输入($M^*$, U^*, ID_R^*)获取2个有效的环签密消息$\mathbf{SC}_1^*=(C_1^*,h_1^*,S^*,\beta^*,r_1^*,\cdots,r_{\pi-1}^*,r_{\pi,1}^*,r_{\pi+1}^*,\cdots,r_n^*)$　和$\mathbf{SC}_2^*=(C_2^*,h_2^*,S^*,\beta^*,r_1^*,\cdots,r_{\pi-1}^*,r_{\pi,2}^*,r_{\pi+1}^*,\cdots,r_n^*)$，满足$h_1^*\neq h_2^*,r_{\pi,1}^*\neq r_{\pi,2}^*,\pi\in\{1,2,\cdots,n\}$。若$\mathrm{ID}_\pi^*\neq\mathrm{ID}_{i^*}$，则

中止；否则，令 $H_1(\mathrm{ID}_{\mathrm{R}}^*)=w_{\mathrm{R}}^*$，$\dfrac{(w_{\mathrm{R}}^*+x)f(x)}{w^*+x}=F(x)+\dfrac{d}{w^*+x}$，多项式$F(x)$的系数和非零整数$d$可由$w^*$、$w_{\mathrm{R}}^*$和$f(x)$计算。$B$计算$W^*=\left[\dfrac{1}{d}\right]\left(\left[\dfrac{r_{\pi,1}^*-r_{\pi,2}^*}{h_2^*-h_1^*}\right]S^*-[F(a)]P\right)$，输出$(w^*, W^*)$作为$q$-SDH问题实例的解。

由于 $r_{\pi,1}^*=\dfrac{r^*r_0^*-h_1^*}{r^*}+\rho$，$r_{\pi,2}^*=\dfrac{r^*r_0^*-h_2^*}{r^*}+\rho$，$H_1(\mathrm{ID}_\pi^*)=w^*$，$S^*=\left[r^*\dfrac{H_1(\mathrm{ID}_{\mathrm{R}}^*)+\mathrm{ks}}{H_1(\mathrm{ID}_\pi^*)+\mathrm{ks}}\right]P_1=\left[\dfrac{r^*(w_{\mathrm{R}}^*+a)f(a)}{w^*+a}\right]P$，则有

$$W^*=\left[\frac{1}{d}\right]\left(\left[\frac{r_{\pi,1}^*-r_{\pi,2}^*}{h_2^*-h_1^*}\right]S^*-[F(a)]P\right)=$$

$$\left[\frac{1}{d}\left(\frac{(r^*r_0^*-h_1^*)-(r^*r_0^*-h_2^*)}{r^*(h_2^*-h_1^*)}\cdot\frac{r^*(w_{\mathrm{R}}^*+a)f(a)}{w^*+a}-F(a)\right)\right]P=$$

$$\left[\frac{1}{d}\left(\frac{(w_{\mathrm{R}}^*+a)f(a)}{w^*+a}-F(a)\right)\right]P=$$

$$\left[\frac{1}{d}\left(F(a)+\frac{d}{w^*+a}-F(a)\right)\right]P=\left[\frac{1}{w^*+a}\right]P$$

因此(w^*, W^*)是有效的解。

只有当B成功模拟、A选定的签密者标识恰好为ID_{i^*}（概率为$\dfrac{1}{q_{H_1}}$），且A伪造的环签密有效（优势为ε）时，B才能成功求解q-SDH问题。由于其概率$\dfrac{\varepsilon}{q_{H_1}}$不可忽略，与$q$-SDH假设相矛盾，因此本文方案在EUF-CMIA模型下是安全的。证毕。

4.4　匿名性

本文方案实现了完全匿名性，即使敌手计算能力无限，甚至掌握系统主私钥，也无法识别实际签密者。

定理3　如果环签密所用的随机数源满足均匀分布，则本文方案满足匿名性。

证明　设$\mathbf{SC}=(C, h, S, \beta, r_1, r_2, \cdots, r_n)$由$U$中用户生成，若签密者标识为$\mathrm{ID}_{\pi_1}$（$\pi_1\in\{1,2,\cdots,n\}$），则

$$r_{\pi_1}=\frac{rr_0-h}{r}+\rho$$

$$S=\left[r\left(1-\frac{v_{\mathrm{R}}}{v_{\pi_1}}\right)\right]\mathrm{ds}_{\pi_1}+\left[r\frac{v_{\mathrm{R}}}{v_{\pi_1}}\right]P_1=\left[r\frac{v_{\mathrm{R}}+\mathrm{ks}}{v_{\pi_1}+\mathrm{ks}}\right]P_1$$

$$\beta=\left(g_1^{\,r\sum_{i=1,i\neq\pi_1}^{n}r_iv_i}\cdot g_2^{\,r\sum_{i=1,i\neq\pi_1}^{n}r_i}\cdot g_0^{\,r\rho}\right)^{-1}=$$

$$e(\mathrm{ds}_{\pi_1},[-r\sum_{i=1,i\neq\pi_1}^{n}r_i(v_i+\mathrm{ks})]P_2)\cdot g_0^{-r\rho}=$$

$$e\left([\mathrm{ks}]P_1,\left[\frac{-r\sum_{i=1,i\neq\pi_1}^{n}r_i(v_i+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}-r\rho\right]P_2\right)$$

SC也可视为由签密者ID_{π_2}（$\pi_2\in\{1,2,\cdots,n\}\setminus\{\pi_1\}$）生成，这是因为，令$r'=\dfrac{r(v_{\pi_2}+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}$，$\rho'=r_{\pi_2}+\dfrac{(v_{\pi_1}+\mathrm{ks})(h-rr_0)}{r(v_{\pi_2}+\mathrm{ks})}$，有$r'\rho'=r'r_{\pi_2}+h-rr_0$，则

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

$$\left[r'\frac{v_{\mathrm{R}}+\mathrm{ks}}{v_{\pi_2}+\mathrm{ks}}\right]P_1=\left[r'\left(1-\frac{v_{\mathrm{R}}}{v_{\pi_2}}\right)\right]\mathrm{ds}_{\pi_2}+\left[r'\frac{v_{\mathrm{R}}}{v_{\pi_2}}\right]P_1$$

$$\beta=e\left([\mathrm{ks}]P_1,\left[\frac{-r(v_{\pi_2}+\mathrm{ks})\sum_{i=1,i\neq\pi_2}^{n}r_i(v_i+\mathrm{ks})}{(v_{\pi_1}+\mathrm{ks})(v_{\pi_2}+\mathrm{ks})}+rr_{\pi_1}-\frac{rr_{\pi_2}(v_{\pi_2}+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}-r\rho\right]P_2\right)=$$

$$e\left([\mathrm{ks}]P_1,\left[\frac{-r'\sum_{i=1,i\neq\pi_2}^{n}r_i(v_i+\mathrm{ks})}{(v_{\pi_2}+\mathrm{ks})}+rr_0-h+r\rho-r'r_{\pi_2}-r\rho\right]P_2\right)=$$

$$e(\mathrm{ds}_{\pi_2},[-r'\sum_{i=1,i\neq\pi_2}^{n} r_i(v_i+\mathrm{ks})\,]P_2)\cdot g_0^{-r'\rho'}=\left(e(\mathrm{ds}_{\pi_2},P_2)^{r'\sum_{i=1,i\neq\pi_2}^{n} r_i v_i}\cdot e(\mathrm{ds}_{\pi_2},P_{\mathrm{pub-s}})^{r'\sum_{i=1,i\neq\pi_2}^{n} r_i}\cdot g_0^{r'\rho'}\right)^{-1}$$

又 $r_{\pi_2}=\dfrac{r'r_0'-h}{r'}+\rho'$，则 $r_0'=\dfrac{r'r_{\pi_2}+h-r'\rho'}{r'}=\dfrac{r_0(v_{\pi_1}+\mathrm{ks})}{v_{\pi_2}+\mathrm{ks}}$，且 $r'r_0'=rr_0$。即 **SC** 同样符合由 ID_{π_2} 作为签密者的计算过程推导。

当环签密过程所采用的随机数源满足均匀分布时，签密者 ID_{π_1} 的随机数 $(r, r_0, r_1, \cdots, r_{\pi_1-1}, r_{\pi_1+1}, \cdots, r_n, \rho)$ 与签密者 ID_{π_2} 的随机数 $(r', r_0', r_1, \cdots, r_{\pi_2-1}, r_{\pi_2+1}, \cdots, r_n, \rho')$ 都是随机且独立的，即使在计算能力无限并且掌握主私钥 ks 的敌手看来，判断签密者是 ID_{π_1} 还是 ID_{π_2} 时仍无任何优势，故无法在集合 U 内辨认实际签名者。因此，本文方案满足完全匿名性。证毕。

5　性能分析与实验

本节对本文方案性能进行理论分析与实验测试，并与同类环签密方案（文献[29]的2个方案）、目前性能最好的SM9环签名[40]和SM9加密[5]的组合方案（下文简称组合方案）、基于国际IBC（采用对称双线性群）的方案[30]以及基于椭圆曲线的方案[32]进行对比。

5.1　性能分析

表3列出了各方案在最优实现方式下，用户私钥生成、环签密和解密验证3个算法中各项耗时运算的次数。其中，SM、SM_1、SM_2 分别表示群 G、G_1、G_2 上的标量乘，E表示群 G_T 上的幂，BP表示双线性对，HTP表示哈希映射到椭圆曲线点的运算，n 表示环成员数量。有限域 F_N 上的运算、群 G_1, G_2 加法、群 G_T 乘法、哈希运算 H_1, H_2 等低耗时运算（合计占比不足2%）以及预计算步骤和对称加解密未计入。

本文方案的环签密与解密验证算法通过相对轻量的有限域运算合并环成员信息，所有耗时运算均为常数次，优于文献[29]的2个线性开销方案。通过签名与加密的融合设计，计算开销较组合方案进一步下降。

在通信开销方面，各方案的系统公钥、用户私钥和环签密消息的长度如表4所示。其中，$|G| = |G_1| = 33$ B、$|G_2| = 65$ B、$|G_T| = 384$ B、$|Z_N| = 32$ B表示对应群元素的字节数[4]，系统公钥不包含 P_1、P_2 等国标规定的公共参数，环签密消息不包含原始消息 M 对应的密文 C、环成员集合和时间戳。

由表4可知，基于SM9方案的系统公钥和用户

表3　　**标识环签密方案的计算开销**

方案	私钥生成	环签密	解密验证
文献[29]方案1	$\mathrm{SM}_1+\mathrm{SM}_2$	$(n+3)\mathrm{SM}_1+4\mathrm{E}$	$n\mathrm{SM}_1+\mathrm{E}+3\mathrm{BP}$
文献[29]方案2	$\mathrm{SM}_1+\mathrm{SM}_2$	$(n+4)\mathrm{SM}_1+\mathrm{E}+\mathrm{BP}$	$n\mathrm{SM}_1+\mathrm{E}+3\mathrm{BP}$
组合方案	$\mathrm{SM}_1+\mathrm{SM}_2$	$3\mathrm{SM}_1+5\mathrm{E}$	$2\mathrm{SM}_2+\mathrm{E}+2\mathrm{BP}$
文献[30]方案	HTP + SM	nHTP + $(n+3)$SM + BP	nHTP + nSM + 3BP
文献[32]方案	2SM	$(2n+4)$SM	$(2n+2)$SM
本文方案	$\mathrm{SM}_1+\mathrm{SM}_2$	$2\mathrm{SM}_1+4\mathrm{E}$	$2\mathrm{SM}_2+\mathrm{E}+\mathrm{BP}$

表4　　**标识环签密方案的通信开销**

方案	系统公钥	用户私钥	环签密消息
文献[29]方案1	$\lvert G_2\rvert+\lvert G_1\rvert$	$\lvert G_2\rvert+\lvert G_1\rvert$	$\lvert G_T\rvert+(n+1)\lvert G_1\rvert+\lvert Z_N\rvert$
文献[29]方案2	$\lvert G_2\rvert+\lvert G_1\rvert$	$\lvert G_2\rvert+\lvert G_1\rvert$	$(n+1)\lvert G_1\rvert+\lvert Z_N\rvert$
组合方案	$\lvert G_2\rvert+\lvert G_1\rvert$	$\lvert G_2\rvert+\lvert G_1\rvert$	$\lvert G_T\rvert+2\lvert G_1\rvert+(n+1)\lvert Z_N\rvert$
文献[30]方案	$\lvert G\rvert$	$\lvert G\rvert$	$(n+2)\lvert G\rvert$
文献[32]方案	$\lvert G\rvert$	$2\lvert Z_N\rvert$	$(n+3)\lvert G\rvert+\lvert Z_N\rvert$
本文方案	$\lvert G_2\rvert+\lvert G_1\rvert$	$\lvert G_2\rvert+\lvert G_1\rvert$	$\lvert G_T\rvert+\lvert G_1\rvert+(n+1)\lvert Z_N\rvert$

私钥长度相同，环签密消息长度都随n线性增长。本文方案环签密消息线性增长的部分略低于文献[29]方案、文献[30]方案和文献[32]方案，较组合方案也有所减少，降低了传递环签密消息的通信开销。

5.2 实验测试

本节基于国密算法Python库hggm[41]实现上述各方案，并进行对比实验。实验计算机配置如表5所示。

表5 实验计算机配置

项目	配置
设备类型	PC
操作系统	Windows10 64位
CPU	Intel Core i3-10110U（2核心4线程）
内存	8 GB LPDDR3 2 133 MHz
硬盘	SAMSUNG MZVLB512HBJQ-000L7
Python版本	3.7.1

表6列出了当环成员数量n为4、16、64、256、1 024时各方案环签密和解密验证的耗时（单位为ms，取500次测试的平均值，不含预计算）。对称加解密采用基于KDF的模2加法，M长度仅为15~17 B，耗时占比不足1%。

表6 各项算法测试结果

方案	算法	环成员数量/个				
		4	16	64	256	1 024
文献[29]方案1	环签密	24.02	33.70	67.00	204.84	757.87
文献[29]方案2		35.39	46.20	83.30	239.11	830.93
组合方案		26.01	27.08	28.02	30.45	42.29
文献[30]方案		44.18	111.03	377.92	1 423.71	5 707.84
文献[32]方案		19.74	87.87	355.37	1 400.53	5 676.28
本文方案		20.45	21.20	21.90	24.67	36.45
文献[29]方案1	解密验证	94.25	145.07	344.22	1 122.24	4 292.10
文献[29]方案2		91.87	144.93	343.30	1 136.41	4 259.42
组合方案		54.13	56.47	57.36	60.19	71.30
文献[30]方案		91.86	152.37	394.07	1 301.59	5 218.85
文献[32]方案		23.46	83.68	326.76	1 234.35	5 137.13
本文方案		32.41	33.81	34.51	38.33	48.55

由表6数据可知，随着n由4增加到1 024，本文方案与组合方案的耗时仅小幅增长，文献[29]方案、文献[30]方案和文献[32]方案的耗时均随n线性增长。当n = 1 024时，本文方案的环签密和解密验证速率分别为文献[29]较快方案（方案1环签密较快，方案2解密验证较快）的20.79倍和87.73倍，较组合方案分别提升16.02%和46.86%。

综上，本文方案环签密与解密验证的计算开销近似常数，较现有同类方案降低了通信开销并提升了算法性能，尤其在较大环规模时有显著优势。

6 结束语

标识环签密技术融合了标识密码、环签名与加密，在需同时保障匿名性与机密性的场景中前景广阔，既避免了PKI体系的建设与管理成本，相比独立应用环签名与公钥加密的方案也更为高效。本文基于国密算法SM9设计了一种环签密方案，在确保可证安全的前提下将环签名与密钥封装的核心步骤深度融合，并将环签密和解密验证的计算开销降至近似常数级。通过形式化的安全规约方法，在ROM下证明了本文方案满足IND-CCA和EUF-CMIA安全性，并实现了完全匿名性。理论分析和实验表明，本文方案在计算效率和通信开销上均优于同类方案以及当前性能最好的SM9环签名与加密的组合方案。接下来将尝试在证明IND-CCA安全性时避免依赖Gap类假设，以进一步提升此类方案的理论安全性。

参考文献：

[1] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption) cost (signature) + cost (encryption)[C]//Advances in Cryptology — CRYPTO 1997. Berlin: Springer, 1997: 165-179.

[2] 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.

[3] HUANG X Y, SUSILO W, MU Y, et al. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world[C]//Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers). Piscataway: IEEE Press, 2005: 649-654.

[4] 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]. Bei-

jing: Standards Press of China, 2020.

[5] 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.

[6] 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.

[7] 谢振杰, 尹小康, 蔡瑞杰, 等. 基于国密算法SM9的可追踪环签名方案[J]. 通信学报, 2025, 46(3): 199-211.
XIE Z J, YIN X K, CAI R J, et al. Traceable ring signature scheme based on domestic cryptographic algorithm SM9[J]. Journal on Communications, 2025, 46(3): 199-211.

[8] 蒲浪, 林超, 伍玮, 等. 基于国密SM9的公钥认证可搜索加密方案[J]. 软件学报, 2025, 36(9): 4271-4284.
PU L, LIN C, WU W, et al. Public-key authenticated encryption scheme with keyword search from Chinese cryptographic SM9[J]. Journal of Software, 2025, 36(9): 4271-4284.

[9] 周权, 陈民辉, 卫凯俊, 等. 基于SM9的支持策略隐藏的可追踪属性签名[J]. 计算机研究与发展, 2025, 62(4): 1065-1074.
ZHOU Q, CHEN M H, WEI K J, et al. Traceable attribute-based signature for SM9-based support policy hidden[J]. Journal of Computer Research and Development, 2025, 62(4): 1065-1074.

[10] 刘行, 明洋, 王晨豪, 等. 基于SM9的可验证公平标识广播代理重加密[J]. 计算机学报, 2025, 48(3): 721-737.
LIU H, MING Y, WANG C H, et al. Verifiable and fair identity-based broadcast proxy re-encryption based on SM9[J]. Chinese Journal of Computers, 2025, 48(3): 721-737.

[11] 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.

[12] MALONE-LEE J. Identity-based signcryption[J]. IACR Cryptology ePrint Archive, 2002(98): 1-8.

[13] LIBERT B, QUISQUATER J J. A new identity based signcryption scheme from pairings[C]//Proceedings 2003 IEEE Information Theory Workshop. Piscataway: IEEE Press, 2003: 155-158.

[14] BARRETO P S L M, LIBERT B, MCCULLAGH N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]//Advances in Cryptology - ASIACRYPT 2005. Berlin: Springer, 2005: 515-532.

[15] YU Y, YANG B, SUN Y, et al. Identity based signcryption scheme without random oracles[J]. Computer Standards & Interfaces, 2009, 31(1): 56-62.

[16] JIN Z P, WEN Q Y, DU H Z. An improved semantically-secure identity-based signcryption scheme in the standard model[J]. Computers & Electrical Engineering, 2010, 36(3): 545-552.

[17] LI X X, QIAN H F, WENG J, et al. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model[J]. Mathematical and Computer Modelling, 2013, 57(3/4): 503-511.

[18] SELVI S S D, VIVEK S S, VINAYAGAMURTHY D, et al. ID based signcryption scheme in standard model[C]//2012 International Conference on Provable Security. Berlin: Springer, 2012: 35-52.

[19] LI F G, TAKAGI T. Secure identity-based signcryption in the standard model[J]. Mathematical and Computer Modelling, 2013, 57(11/12): 2685-2694.

[20] KARATI A, ISLAM S H, BISWAS G P, et al. Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of things environments[J]. IEEE Internet of Things Journal, 2018, 5(4): 2904-2914.

[21] WANG X M, ZHANG Y, GUPTA B B, et al. An identity-based signcryption on lattice without trapdoor[J]. Journal of Universal Computer Science, 2019, 25(3): 282-293.

[22] ELTAYIEB N, ELHABOB R, HASSAN A, et al. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud[J]. Journal of Systems Architecture, 2020, 102: 101653.

[23] MANDAL S, BERA B, SUTRALA A K, et al. Certificateless-signcryption-based three-factor user access control scheme for IoT environment[J]. IEEE Internet of Things Journal, 2020, 7(4): 3184-3197.

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

[25] 黄欣沂, 张福泰, 伍玮. 一种基于身份的环签密方案[J]. 电子学报, 2006, 34(2): 263-266.
HUANG X Y, ZHANG F T, WU W. An identity-based ring signcryption scheme[J]. Acta Electronica Sinica, 2006, 34(2): 263-266.

[26] ZHU Z C, ZHANG Y Q, WANG F J. An efficient and provable secure identity-based ring signcryption scheme[J]. Computer Standards & Interfaces, 2009, 31(6): 1092-1097.

[27] GUO Z Z, LI M C, FAN X X. Attribute-based ring signcryption scheme[J]. Security and Communication Networks, 2013, 6(6): 790-796.

[28] YU H F, WANG W K, ZHANG Q. Certificateless anti-quantum ring signcryption for network coding[J]. Knowledge-Based Systems, 2022, 235: 107655.

[29] 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. Identity-based ring signcryption scheme based on SM9 algorithm[D]. Wuhan: Wuhan University, 2022.

[30] DU H Z, WEN Q Y, ZHANG S S, et al. An improved conditional privacy protection scheme based on ring signcryption for VANETs[J]. IEEE Internet of Things Journal, 2023, 10(20): 17881-17892.

[31] CAI Y, ZHANG H, FANG Y G. A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks[J]. IEEE Internet of Things Journal, 2021, 8(1): 647-656.

[32] 罗铭, 詹骐榜, 邱敏蓉. 面向V2I通信的异构跨域条件隐私保护环签密方案[J]. 信息网络安全, 2024, 24(7): 993-1005.
LUO M, ZHAN Q B, QIU M R. A heterogeneous cross-domain condi-

tional privacy protection ring signcryption scheme for V2I communication[J]. Netinfo Security, 2024, 24(7): 993-1005.

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

[34] HERRANZ J, SÁEZ G. Forking lemmas for ring signature schemes[C]// Progress in Cryptology - INDOCRYPT 2003. Berlin: Springer, 2003: 266-279.

[35] 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.

[36] 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.

[37] CHENG Z H. Security analysis of SM9 key agreement and encryption[C]// 2018 International Conference on Information Security and Cryptology (INSCRYPT). Berlin: Springer, 2019: 3-25.

[38] 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.

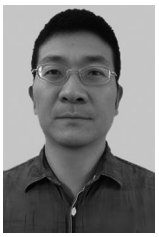
[39] SELVI S S D, VIVEK S S, RANGAN C P. On the security of identity based ring signcryption schemes[C]//2009 International Conference on Information Security. Berlin: Springer, 2009: 310-325.

[40] 谢振杰, 刘胜利, 贾志鹏, 等. 基于SM9的环签名：常数级计算开销的方案构造[J]. 通信学报, 2025, 46(11): 104-113.
XIE Z J, LIU S L, JIA Z P, et al. SM9-based ring signature: a scheme with constant-time computational overhead[J]. Journal on Communications, 2025, 46(11): 104-113.

[41] 谢振杰, 刘奕明, 蔡瑞杰, 等. 国密算法SM9的性能优化方法[J]. 计算机科学, 2025, 52(6): 390-396.
XIE Z J, LIU Y M, CAI R J, et al. Performance optimization method for domestic cryptographic algorithm SM9[J]. Computer Science, 2025, 52(6): 390-396.

[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。



刘胜利（1973– ），男，河南周口人，博士，信息工程大学教授、博士生导师，主要研究方向为网络设备安全、网络攻击检测。

谢耀滨（1981– ），男，福建漳州人，博士，信息工程大学副教授、硕士生导师，主要研究方向为嵌入式系统安全、工业控制系统安全。

李路凯（1999– ），男，河南周口人，信息工程大学助理工程师，主要研究方向为网络设备安全、二进制代码分析。

卫明远（2004– ），男，河南洛阳人，信息工程大学硕士生，主要研究方向为网络空间安全。