软件学报 ISSN 1000-9825, CODEN RUXUEW
[doi: 10.13328/j.cnki.jos.007660] [CSTR: 32375.14.jos.007660]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于国密 SM2 支持非法消息追踪的环签名方案*

王晨豪, 明 洋, 刘 行, 邓雨桐, 赵 一

(长安大学 信息工程学院, 陕西 西安 710064)

通信作者: 明洋, E-mail: yangming@chd.edu.cn

摘 要: 环签名作为一种具有隐私保护的认证技术, 在确保消息真实性和完整性的同时为用户提供身份匿名性, 广泛应用于电子投票和区块链交易等场景. 针对恶意用户的匿名滥用与失信行为, 现有环签名方案利用追踪 (监管) 权威揭示任意用户的真实身份. 然而, 该权威的引入将导致诚实用户的隐私泄露, 打破了匿名性和可追踪性之间的平衡. 为解决上述问题并促进国产密码技术应用发展, 提出基于国密 SM2 支持非法消息追踪的环签名方案. 所提方案针对单个非法消息设计追踪机制, 其中追踪权威仅能够揭示发布非法消息恶意用户的真实身份, 而诚实用户仍然保持匿名, 从而平衡匿名性和可追踪性. 基于此, 结合多项式技术和默克尔哈希树技术提出扩展方案, 实现任意数量非法消息追踪, 扩大恶意用户监管范围, 同时降低用户验证开销和通信成本. 安全性分析表明所提方案满足不可伪造性、匿名性和可追踪性. 性能分析表明所提方案与相关环签名方案相比具有较好的有效性和实用性.

关键词: SM2; 环签名; 隐私保护; 可追踪性; 预限制加密

中图法分类号: TP309

中文引用格式: 王晨豪, 明洋, 刘行, 邓雨桐, 赵一. 基于国密SM2支持非法消息追踪的环签名方案. 软件学报. http://www.jos.org.cn/1000-9825/7660.htm

英文引用格式: Wang CH, Ming Y, Liu H, Deng YT, Zhao Y. SM2-based Ring Signature Scheme Supporting Illegal Message Traceability. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7660.htm

SM2-based Ring Signature Scheme Supporting Illegal Message Traceability

WANG Chen-Hao, MING Yang, LIU Hang, DENG Yu-Tong, ZHAO Yi

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract: As a privacy-preserving authentication technique, ring signatures preserve user anonymity while ensuring message authenticity and integrity. They are widely used in scenarios such as electronic voting and blockchain transactions. To prevent malicious users from abusing anonymity and engaging in dishonest behavior, existing ring signature schemes employ a tracing authority (or regulatory authority) to reveal the real identities of any user. However, introducing such an authority may lead to privacy leakage for honest users, disrupting the balance between anonymity and traceability. To address these issues and promote the application and development of domestic cryptographic technologies, this study proposes an SM2-based ring signature scheme with traceability for illegal messages. The proposed scheme designs a tracing mechanism for a single illegal message, under which the tracing authority is permitted to reveal only the real identities of malicious users who publish illegal messages, while honest users remain anonymous, thus balancing anonymity and traceability. On this basis, this study further extends the proposed scheme by combining polynomial techniques with Merkle hash tree techniques. As a result, traceability for an arbitrary number of illegal messages is achieved, the scope of supervision over malicious users is expanded, and user verification overhead and communication costs are reduced. Security analysis demonstrates that the proposed scheme achieves unforgeability, anonymity, and traceability. Performance analysis indicates that the proposed scheme offers superior efficiency and practicality compared with existing ring signature schemes.

Key words: SM2; ring signature; privacy protection; traceability; pre-constrained encryption

---

* 基金项目: 国家自然科学基金 (62472049, 62072054); 陕西省重点研发计划 (2024GX-YBXM-078, S2025-JC-YB-0498)
收稿时间: 2025-07-09; 修改时间: 2025-12-22; 采用时间: 2026-03-02; jos 在线出版时间: 2026-05-20

为抵御数字通信过程中攻击者发起信息篡改和身份冒充等攻击, 数字签名[1]广泛应用于网络环境确保消息真实性和完整性. 作为中国国家密码标准[2], SM2 椭圆曲线数字签名替代了国外 ECDSA[3]、Schnorr[4]等签名算法, 能够满足网络认证服务系统的安全要求, 实现国产密码技术应用的自主化和可控性, 包括基于 SM2 数字签名的匿名凭证协议[5]、支持批量证明的 SM2 适配器签名方案[6]、加权门限 SM2 数字签名方案[7].

但在电子投票[8]、区块链交易[9,10]、数字货币[11]等应用场景中, 传统数字签名无法满足用户的隐私保护需求. 为此, Rivest 等人[12]首次提出具有匿名性的环签名, 允许签名者自发选择多个用户组成环, 利用自身私钥和选取用户公钥对消息进行签名. 验证者仅能够确认签名是否来自环中某一用户, 但不能获取签名者的真实身份. 通过将签名者真实身份隐藏在环中, 环签名能够确保用户身份隐私并广泛应用于匿名性场景. 自环签名提出后, 研究人员陆续基于国密 SM2 数字签名设计环签名方案. 为推动国产密码算法在区块链的应用, 范青等人[13]首次提出基于 SM2 数字签名的环签名方案, 并通过嵌入链接标签提出 SM2 可链接环签名方案. Feng 等人[14]借助双环技术提出环签名为对数大小的 SM2 环签名方案, 降低用户通信成本.

虽然上述环签名方案能够保护用户身份隐私, 但同时存在恶意用户匿名性的滥用问题[15]. 例如, 区块链网络中恶意节点操纵时间戳进行欺诈[9], 黑客通过数字货币向受害者索要赎金等. 由于传统环签名方案具有无条件匿名性, 失信行为和非法消息追踪困难, 会造成巨大的经济损失并给社会带来危害.

近年来, 越来越多的研究注重于恶意用户监管. 范青等人[13]的可链接环签名方案中, 验证者能够通过链接标签确认两个消息是否来自同一用户. 谢振杰等人[16]和 Fujisaki 等人[17]进一步引入可追踪环签名方案, 当用户针对同一标签发布不同签名, 追踪权威能够揭示其真实身份. 然而, 上述可链接和可追踪环签名方案仅适用于特定应用场景, 当恶意用户仅发布一次非法消息时, 无法揭示其真实身份. 此外, 现有可追踪环签名方案[9,17]中, 追踪权威能够揭示任意用户真实身份 (无论该用户是否做出不诚实行为或发布非法消息), 导致诚实用户的隐私泄露、匿名性和可追踪性之间失衡. 因此, 本文旨在确保消息真实性和完整性的同时平衡匿名性和可追踪性. 本文具体贡献如下.

(1) 提出基于国密 SM2 支持非法消息追踪的环签名方案. 一方面, 所提方案能够与国产密码算法 SM2 数字签名有机融合, 满足密码算法自主可控的要求, 促进国产密码技术应用发展. 另一方面, 所提方案针对单个非法消息设计追踪机制, 其中追踪权威仅能够揭示发布非法消息恶意用户的真实身份而诚实用户仍然保持匿名, 从而实现匿名性和可追踪性之间的平衡.

(2) 结合多项式技术和默克尔哈希树技术提出扩展方案, 实现任意数量非法消息追踪, 扩大恶意用户监管范围. 同时, 用户验证开销从 $O(2n)$ 降为 $O(n)$, 通信成本从 $O(n)$ 降为 $O(n/2)$.

(3) 安全性分析表明所提方案满足不可伪造性, 匿名性和可追踪性. 理论和实验性能分析表明, 所提方案与相关环签名方案相比取得了性能优势, 具有高效的验证算法并且通信代价更低.

本文第 1 节介绍相关工作. 第 2 节列出所需基础知识. 第 3 节给出形式化定义与安全模型. 第 4 节介绍所提方案及其扩展. 第 5 节和第 6 节分别对所提方案进行安全性分析和性能分析. 第 7 节应用所提方案设计可监管区块链系统. 第 8 节总结本文工作.

1 相关工作

本文相关工作分为环签名和预限制加密两部分, 后者能够应用于前者以平衡匿名性和可追踪性.

● 环签名. 2001 年, Rivest 等人[12]首次提出环签名 (ring signature, RS), 确保消息认证性的同时为用户提供身份隐私保护. 随后, 为解决电子投票系统中匿名用户重复投票问题, Liu 等人[18]引入可链接环签名 (linkable ring signature, LRS) 方案, 允许任意实体通过链接标签确认两个签名是否由同一用户针对相同环成员生成, 但 LRS 方案无需满足用户匿名性撤销. Fujisaki 等人[17]引入可追踪环签名 (traceable ring signature, TRS) 方案, 进一步限制用户匿名性. TRS 方案包含一个追踪标签, 由环成员列表和消息内容组成, 任意匿名用户仅能使用相同标签发布一次环签名. 如果发布两次, TRS 方案支持标签可链接性和公开可追踪性, 即任意实体能够通过标签和消息/签名对揭示该用户的身份. Bultel 等人[19]提出 k 次 TRS 方案, 当同一用户使用相同标签生成 k 个以上签名时才能进行追踪,

进一步增强系统容错性和健壮性[20]. Xie 等人[21]对 LRS 方案和 k 次 TRS 方案进行结合以实现细粒度问责. 当同一用户使用相同标签生成签名数量少于 k 个时能够支持标签可链接性, 大于 k 个时能够实现标签可追踪性. 但是, 上述 TRS 方案的追踪过程需要通过提前存储所有用户列表并对环成员进行遍历操作完成, 效率较差. 此外, 上述 TRS 方案无法在仅发布一次非法消息的情况下实现追踪. 为此, Xue 等人[9]采用一次性密钥和零知识证明技术设计 TRS 方案, 追踪权威能够通过一次性密钥获取用户的真实身份. 然而, 追踪权威能够揭示任意用户的真实身份, 导致诚实用户的隐私泄露, 匿名性和可追踪性之间的平衡被打破.

● 预限制加密. 2022 年, Ananth 等人[22]首次提出预限制加密 (pre-constrained encryption, PCE), 该技术旨在平衡非法行为监管和诚实用户隐私, 即追踪权威仅能够获取发布非法消息恶意用户的真实身份, 而诚实用户仍然保持匿名. 随后, Bartusek 等人[23]结合 PCE 提出集合预限制群签名 (set pre-constrained group signature, SPCGS) 方案并应用于端到端加密服务系统, 仅当群用户发布非法消息时, 群管理员才能够打开其真实身份. Nguyen 等人[24]提出支持错误容忍的 SPCGS 方案, 即任意用户仅在发布 k 次以上非法消息后才能够被追踪. Huang 等人[25]结合 PCE 提出消息鉴别方案, 该方案主要特点是支持管理员仅对非法消息审核并实现可回溯性.

2 基础知识

本节给出本文涉及的基础知识, 包括国密 SM2 数字签名、零知识证明、困难问题假设和 Diffie-Hellman (DH) 元组与随机自归约.

2.1 国密 SM2 数字签名

根据《SM2 椭圆曲线公钥密码算法》(https://sca.gov.cn/sca/xwdt/2010-12/17/content_1002386.shtml) 规范, 国密 SM2 数字签名包含如下 4 个多项式时间算法.

(1) 系统建立: 输入安全参数 λ, 输出系统参数 $pp=\{p,F_p,q,\mathbb{G},P,H_1\}$, 其中 p 为大素数, F_p 为有限域, 定义 E 为 F_p 满足 $y^2=x^3+ax+b \bmod p$ 的椭圆曲线, $\mathbb{G}$ 为 E 所有椭圆曲线点及无穷远点 O 构成的加法循环群, P 为群 $\mathbb{G}$ 的生成元, q 为群 $\mathbb{G}$ 的阶, H_1 为密码学哈希函数, 实践中采用 SM3 哈希算法实例化.

(2) 密钥生成: 输入系统参数 $pp=\{p,F_p,q,\mathbb{G},P,H_1\}$, 随机选择 $ZKPoK\{(\alpha,\beta,d_\pi,pk_\pi)\colon I_\pi^{(1)}=(\alpha+\beta h)\cdot pk_\pi,\ I_\pi^{(2)}=T_\pi+pk_\pi, T_\pi=d_\pi(\alpha\cdot TK_1+\beta\cdot TK_2), pk_\pi=d_\pi\cdot P\}$ 作为私钥 sk, 计算公钥 $pk=d\cdot P$.

(3) 签名: 输入消息 m 和私钥 sk, 随机选择 $k\in\mathbb{Z}_q^*$, 计算 $e=H_1(m)$, $(x_1,y_1)=k\cdot P$, $r=(e+x_1) \bmod q$, $s=(1+d)^{-1}(k-rd) \bmod q$, 输出签名 $\sigma=(r,s)$.

(4) 验证: 输入消息 m', 签名 $\sigma'=(r',s')$ 和公钥 pk, 验证 $r'\in\mathbb{Z}_q^*$, $s'\in\mathbb{Z}_q^*$ 是否成立. 如果成立则计算 $e'=H_1(m')$, $t=(r'+s') \bmod q$, $(x_1', y_1')=s'\cdot P+t\cdot pk$, $R=(e'+x_1') \bmod q$, 验证 $R=r'$ 是否成立. 若成立则验证通过, 否则验证失败.

2.2 零知识证明

令 $\mathcal{R}=\{(x,w)\colon \{0,1\}^*\times\{0,1\}^*\}$ 为可计算二元关系, 其中 x 是陈述, w 是证据. 设 $\mathcal{L}(\mathcal{R})$ 为 $\mathcal{R}$ 中有效陈述组成的 NP 语言. 零知识证明[26]允许证明者在不泄漏 w 的情况下, 使验证者相信其拥有 w 且满足 $(x,w)\in\mathcal{R}$, 表示为 $ZKPoK\{(w)\colon (x,w)\in\mathcal{R}\}$. 为证明离散对数关系的零知识证明系统, 通过 Fiat-Shamir 转换, 能够在随机预言机模型下将交互式零知识证明系统转换为非交互式零知识证明系统. 零知识证明包含如下 2 个多项式时间算法.

(1) $\text{Prove}(w,x)\to\psi$: 输入证据 w 和陈述 x, 输出证明 ψ.

(2) $\text{Verify}(x,\psi)\to 1/0$: 输入陈述 x 和证明 ψ, 若证明有效, 输出 1; 否则输出 0.

2.3 困难问题假设

椭圆曲线离散对数问题 (elliptic curve discrete logarithm problem, ECDLP): 给定 ECDLP 实例 (P,Q), 计算 x 满足 $Q=xP$ 在多项式时间内不可行.

ECDLP 假设[27]: 任意概率多项式时间算法解决 ECDLP 问题的优势 $Adv_{\mathcal{A}}^{\text{ECDLP}}=|\Pr[\mathcal{A}(P,Q)=x]|$ 可忽略.

椭圆曲线判定 DH 问题 (elliptic curve decisional Diffie-Hellman problem, ECDDHP): 给定 ECDDHP 实例

(P,aP,bP), 计算 $Q=abP$ 在多项式时间内不可行.

ECDDHP 假设[27]: 任意概率多项式时间算法解决 ECDDHP 问题的优势 $Adv_{\mathcal{A}}^{\mathrm{ECDDHP}}=|\Pr[\mathcal{A}(P,aP,bP)=abP]|$ 可忽略.

2.4 Diffie-Hellman (DH) 元组与随机自归约

给定生成元为 P 的加法循环群 $\mathbb{G}$, 如果存在 $s\in\mathbb{Z}_q^*$ 满足 $Q_1=s\cdot P$, $Q_3=s\cdot Q_2$, 则称 $\{P,Q_1,Q_2,Q_3\}\in\mathbb{G}$ 为 DH 元组. 群 $\mathbb{G}$ 中的 ECDDHP 假设表明随机 DH 元组与群 $\mathbb{G}$ 中随机元素满足计算不可区分.

对于 $\{P,Q_1,Q_2,Q_3\}\in\mathbb{G}$, 随机选择 $\alpha,\beta\in\mathbb{Z}_q^*$, 令 $Q_2'=\alpha\cdot P+\beta\cdot Q_2$, $Q_3'=\alpha\cdot Q_1+\beta\cdot Q_3$ 为满足如下性质的随机自归约[28].

(1) 如果 $\{P,Q_1,Q_2,Q_3\}$ 和 $\{P,Q_1,Q_2',Q_3'\}$ 都是 DH 元组, 则 $\{Q_2',Q_3'\}$ 为均匀分布.

(2) 如果 $\{P,Q_1,Q_2',Q_3'\}$ 不是 DH 元组, 则 $\{Q_2',Q_3'\}$ 为均匀随机的群元素.

3 形式化定义与安全模型

本节给出基于国密 SM2 支持非法消息追踪的环签名方案形式化定义与安全模型.

3.1 形式化定义

定义 1. 基于国密 SM2 支持非法消息追踪的环签名方案包含如下 5 个多项式时间算法.

(1) 系统初始化 $\mathrm{Setup}(\lambda,IC)\to(params,tk)$: 输入安全参数 λ 和非法消息集合 $IC=\{im_1,im_2,\ldots,im_t\}$, 该算法生成系统参数 $params$ 和追踪密钥 tk. 此处, 非法消息集合由管理员或监管机构预先设定[23].

(2) 密钥生成 $\mathrm{KeyGen}(params)\to(pk,sk)$: 输入系统参数 $params$, 该算法生成公私钥对 (pk,sk).

(3) 环签名生成 $\mathrm{RSign}(sk_\pi,L,m)\to(\sigma,I_\pi)$: 输入私钥 sk_π、用户公钥集合 $L=\{pk_1,pk_2,\ldots,pk_n\}$ 和消息 m, 该算法生成环签名 σ 和追踪标签 I_π.

(4) 环签名验证 $\mathrm{RVerify}(m',\sigma',I_\pi,L)\to 1/0$: 输入消息 m'、环签名 σ'、追踪标签 I_π 和用户公钥集合 L, 当签名有效时该算法返回 1, 否则返回 0.

(5) 追踪 $\mathrm{Trace}(m',\sigma',I_\pi,tk)\to pk_\pi/\perp$: 输入消息 m、环签名 σ、追踪标签 I_π 和追踪密钥 tk, 当 $m\in IC$ 时该算法返回公钥 pk_π, 否则返回 $\perp$.

3.2 安全模型

基于国密 SM2 支持非法消息追踪的环签名方案应满足不可伪造性、匿名性和可追踪性, 通过挑战者 $\mathcal{C}$ 和敌手 $\{\mathcal{A}_{\mathrm{I}},\mathcal{A}_{\mathrm{II}},\mathcal{A}_{\mathrm{III}}\}$ 的交互式游戏进行定义, 敌手能够进行如下询问.

(1) 哈希询问 (Q_h): 给定任意消息 m, $\mathcal{C}$ 返回随机选择的哈希值 $h\in\mathbb{Z}_q^*$.

(2) 密钥生成询问 (Q_k): 给定系统参数 $params$, $\mathcal{C}$ 运行密钥生成算法 $\mathrm{KeyGen}(params)$ 并返回公钥 pk.

(3) 腐化询问 (Q_c): 给定公钥 pk_π, $\mathcal{C}$ 返回私钥 sk_π.

(4) 签名询问 (Q_s): 给定公钥 pk_π、用户公钥集合 $L=\{pk_1,pk_2,\ldots,pk_n\}$ 和消息 m, $\mathcal{C}$ 运行环签名生成算法 $\mathrm{RSign}(sk_\pi,L,m)$ 并返回环签名 σ 和追踪标签 I_π.

● 不可伪造性. 如果敌手无法获得用户公钥集合 L 中任意成员的私钥, 则无法伪造一个有效的环签名. 该性质通过挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}_{\mathrm{I}}$ 之间的下述游戏定义.

系统建立: $\mathcal{C}$ 运行系统初始化算法 $\mathrm{Setup}(\lambda,IC)$ 生成系统参数 $params$ 和追踪密钥 tk, 发送 $params$ 给敌手 $\mathcal{A}_I$.

询问: 敌手 $\mathcal{A}_{\mathrm{I}}$ 适应性地进行哈希、密钥生成、腐化和签名询问.

伪造: 敌手 $\mathcal{A}_{\mathrm{I}}$ 对 (L^*,m^*) 生成伪造的环签名 σ^* 和追踪标签 I^*. 如果以下条件满足, 敌手 $\mathcal{A}_{\mathrm{I}}$ 赢得上述游戏.

① σ^* 是关于 (L^*,m^*) 有效的环签名且未进行过签名询问.

② L^* 中所有公钥通过密钥生成询问获得且未进行过腐化询问.

定义 2. 如果任意概率多项式时间敌手 $\mathcal{A}_{\mathrm{I}}$ 赢得上述游戏的概率可忽略, 则本文方案满足不可伪造性.

● 匿名性. 敌手从用户公钥集合中猜出真正签名者的概率不大于随机猜测. 该性质通过挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}_{\mathrm{II}}$ 之间的下述游戏定义.

系统建立: $\mathcal{C}$ 运行系统初始化算法 $\mathrm{Setup}(\lambda, IC)$ 生成系统参数 $params$ 和追踪密钥 tk, 发送 $params$ 给敌手 $\mathcal{A}_{\mathrm{II}}$.

询问: 敌手 $\mathcal{A}_{\mathrm{II}}$ 适应性地进行密钥生成询问.

挑战: 敌手 $\mathcal{A}_{\mathrm{II}}$ 发送 (L^*, m^*) 给挑战者 $\mathcal{C}$, 其中 $L^* = \{pk_1^*, pk_2^*, \ldots, pk_n^*\}$ 通过密钥生成询问获得. $\mathcal{C}$ 随机选择 $\pi \in \{1,2,\ldots,n\}$, 运行环签名生成算法 $\mathrm{RSign}(sk_\pi, L^*, m^*)$ 并返回环签名 σ^* 和追踪标签 I^*.

猜测: 敌手 $\mathcal{A}_{\mathrm{II}}$ 输出猜测值 $\pi' \in \{1,2,\ldots,n\}$. 如果 $\pi' = \pi$, 敌手 $\mathcal{A}_{\mathrm{II}}$ 赢得上述游戏.

定义 3. 如果任意概率多项式时间敌手 $\mathcal{A}_{\mathrm{II}}$ 赢得上述游戏的概率可忽略, 则本文方案满足匿名性.

● 可追踪性. 获取追踪密钥的敌手从用户公钥集合中猜出诚实签名者 (未发布非法消息) 的概率不大于随机猜测. 该性质通过挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}_{\mathrm{III}}$ 之间的下述游戏定义.

系统建立: $\mathcal{C}$ 运行系统初始化算法 $\mathrm{Setup}(\lambda, IC)$ 生成系统参数 $params$ 和追踪密钥 tk, 发送 $\{params, tk\}$ 给敌手 $\mathcal{A}_{\mathrm{III}}$.

询问: 敌手 $\mathcal{A}_{\mathrm{III}}$ 适应性地进行密钥生成和签名询问.

挑战: 敌手 $\mathcal{A}_{\mathrm{III}}$ 发送 (L^*, m^*) 给挑战者 $\mathcal{C}$, 其中 $L^* = \{pk_1^*, pk_2^*, \ldots, pk_n^*\}$ 通过密钥生成询问获得. $\mathcal{C}$ 随机选择 $\pi \in \{1,2,\ldots,n\}$, 运行环签名生成算法 $\mathrm{RSign}(sk_\pi, L^*, m^*)$ 并返回环签名 σ^* 和追踪标签 I^*.

猜测: 敌手 $\mathcal{A}_{\mathrm{II}}$ 输出猜测值 $\pi' \in \{1,2,\ldots,n\}$. 如果满足以下条件, 敌手 $\mathcal{A}_{\mathrm{III}}$ 赢得上述游戏.

① $\pi' = \pi$ 且 m^* 不属于非法消息集合 IC.

② (L^*, m^*) 未进行过签名询问且 L^* 中所有公钥通过密钥生成询问获得.

定义 4. 如果任意概率多项式时间敌手 $\mathcal{A}_{\mathrm{III}}$ 赢得上述游戏的概率可忽略, 则本文方案满足可追踪性.

4 基于国密 SM2 支持非法消息追踪的环签名方案

基于上述形式化定义, 本节给出基于国密 SM2 支持非法消息追踪的环签名方案构造. 第 4.1 节针对单个非法消息 $IC = \{x\}$ 给出具体方案. 第 4.2 节针对 t 个非法消息 $IC = \{x_1, x_2, \ldots, x_t\}$ 并结合多项式技术和默克尔哈希树技术给出扩展方案, 其中非法消息数量 t 可在系统初始化阶段任意指定. 此外, 表 1 给出相关符号定义与描述.

表 1 相关符号定义与描述

符号定义	符号描述	符号定义	符号描述
λ	安全参数	tk	追踪密钥
IC	非法消息集合	π	任意用户
x	任意非法消息	pk_π	用户公钥
t	非法消息数量	sk_π	用户私钥
L	用户公钥集合	I_π	用户追踪标签

4.1 具体方案

(1) 系统初始化 $\mathrm{Setup}(\lambda, IC) \to (params, tk)$: 给定安全参数 λ 和非法消息集合 $IC = \{x\}$, 追踪权威执行如下步骤.

① 生成国密 SM2 数字签名系统参数 $pp = \{p, F_p, q, \mathbb{G}, P, H_1\}$.

② 随机选择追踪密钥 $tk \in \mathbb{Z}_q^*$.

③ 计算 $TK_1 = tk \cdot P$, $TK_2 = H_1(x) \cdot TK_1$.

④ 选择哈希函数 H_2, H_3: $\{0,1\}^* \to \mathbb{Z}_q^*$.

输出系统参数 $params = \{p, F_p, q, \mathbb{G}, P, H_1, H_2, H_3, TK_1, TK_2\}$.

(2) 密钥生成 $\mathrm{KeyGen}(params) \to (pk, sk)$: 给定系统参数 $params$, 用户 π 随机选择 $d_\pi \in \mathbb{Z}_q^*$ 作为私钥 sk_π, 计算公钥 $pk_\pi = d_\pi \cdot P$.

(3) 环签名生成 $\mathrm{RSign}(sk_\pi, L, m) \to (\sigma, I_\pi)$: 给定私钥 sk_π, 用户公钥集合 $L = \{pk_1, pk_2, \ldots, pk_n\}$ 和消息 m, 用户 π 执行如下步骤.

① 随机选取 $\alpha,\beta\in\mathbb{Z}_q^*$.

② 计算 $h=H_1(m)$, $T_\pi=d_\pi(\alpha\cdot TK_1+\beta\cdot TK_2)$.

③ 计算 $I_\pi^{(1)}=(\alpha+\beta h)\cdot pk_\pi$, $I_\pi^{(2)}=T_\pi+pk_\pi$.

④ 生成 $ZKPoK\{(\alpha,\beta,d_\pi,pk_\pi)\colon I_\pi^{(1)}=(\alpha+\beta h)\cdot pk_\pi,\ I_\pi^{(2)}=T_\pi+pk_\pi,\ T_\pi=d_\pi(\alpha\cdot TK_1+\beta\cdot TK_2),\ pk_\pi=d_\pi\cdot P\}$ 的零知识证明 ψ (如图 1 所示).

Prove	*ZKPoK*	Verify
$u_1,u_2,u_3\in\mathbb{Z}_q^*, U_1=u_1\cdot P+u_1\cdot TK_1,$		
$U_2=u_2h\cdot P+u_2\cdot TK_2, U_3=u_3\cdot P,$		
$c=H_3(U_1,U_2,U_3,I_\pi^{(1)},I_\pi^{(2)}),$		
$z_1=u_1-\alpha sk_\pi c,\ z_2=u_2-\beta sk_\pi c,\ z_3=u_3-sk_\pi c.$		
	$\psi=(U_1,U_2,U_3,z_1,z_2,z_3)\longrightarrow$	
		$c=H_3(U_1,U_2,U_3,I_\pi^{(1)},I_\pi^{(2)}),$
		$U_1+U_2+U_3=z_1(P+TK_1)+z_2(h\cdot P+TK_2)+z_3P+c(I_\pi^{(1)}+I_\pi^{(2)}).$

图 1 零知识证明

⑤ 随机选取 $k_\pi\in\mathbb{Z}_q^*$.

⑥ 计算 $c_{\pi+1}=H_2(L,m,k_\pi\cdot P)$.

⑦ 对 $i\in[1,n]$, $i\neq\pi$, 随机选取 $s_i\in\mathbb{Z}_q^*$, 计算 $Z_i=s_i\cdot P+(s_i+c_i)\cdot pk_i+I_\pi^{(1)}$, $c_{i+1}=H_2(L,m,Z_i)$, 设定 $c_1=c_{n+1}$.

⑧ 计算 $r_\pi=c_\pi+\alpha+\beta H_1(m)$, $s_\pi=(1+d_\pi)^{-1}(k_\pi-r_\pi\mathrm{d}_\pi)\bmod q$.

输出环签名 $x\neq m^*$ 和追踪标签 $I_\pi=\{I_\pi^{(1)},I_\pi^{(2)}\}$.

(4) 环签名验证 $\mathrm{RVerify}(m',\sigma',I_\pi,L)\to 1/0$: 给定消息 m'、环签名 $1/n$、追踪标签 I_π 和用户公钥集合 $L=\{pk_1,pk_2,\ldots,pk_n\}$, 验证者执行如下步骤.

① 根据图 1 验证 $\{I_\pi^{(1)},I_\pi^{(2)}\}$ 是否成立.

② 验证 $\{c_1,s_1,s_2,\ldots,s_n\}\in\mathbb{Z}_q^*$ 是否成立.

③ 对 $i\in[1,n]$, 计算 $Z_i'=s_i'\cdot P+(s_i'+c_i')\cdot pk_i+I_\pi^{(1)}$, $c_{i+1}'=H_2(L,m',Z_i')$.

④ 验证 $c_1'=c_{n+1}'$ 是否成立, 如果成立则返回 1, 否则返回 0.

(5) 追踪 $\mathrm{Trace}(m,\sigma,I_\pi,tk)\to pk_\pi/\perp$: 给定消息 m、环签名 σ、追踪标签 I_π 和追踪密钥 *ZKPoK*, 追踪权威执行如下步骤.

① 如果消息 $m\neq x$, 返回 π^*. 否则计算 $pk_\pi=I_\pi^{(2)}-tk\cdot I_\pi^{(1)}$.

② 返回用户 π 的公钥 pk_π.

● 签名正确性. 对于 $i\in[1,n]$, $i\neq\pi$, 验证者依次计算 $Z_i'=s_i'\cdot P+(s_i'+c_i')\cdot pk_i+I_\pi^{(1)}$, $c_{i+1}'=H_2(L,m',Z_i')$. 因此, $s_{i+1}'=c_{i+1}$ 成立. 对于 $i=\pi$, 根据公式 (1) 可得 $Z_\pi'=k_\pi\cdot P$. 因此, $c_{\pi+1}'=c_{\pi+1}$ 成立.

$$\begin{aligned}Z_\pi'&=s_\pi'\cdot P+(s_\pi'+c_\pi')\cdot pk_\pi+I_\pi^{(1)}=(k_\pi-r_\pi d_\pi)\cdot P+c_\pi'\cdot pk_\pi+I_\pi^{(1)}\\&=k_\pi\cdot P-(c_\pi+\alpha+\beta H_1(m))\cdot pk_\pi+c_\pi'\cdot pk_\pi+I_\pi^{(1)}\\&=k_\pi\cdot P-(\alpha+\beta H_1(m))\cdot pk_\pi+(\alpha+\beta h)\cdot pk_\pi\\&=k_\pi\cdot P\end{aligned}\tag{1}$$

● 追踪正确性. 如公式 (2) 所示, 用户 π 能够通过公钥 pk_π 被追踪.

$$\begin{aligned}I_\pi^{(2)}-tk\cdot I_\pi^{(1)}&=I_\pi^{(2)}-tk(\alpha+\beta H_1(m))\cdot pk_\pi\\&=I_\pi^{(2)}-d_\pi\alpha\cdot TK_1-d_\pi\beta H_1(m)\cdot TK_1\\&=(d_\pi\beta H_1(m)-d_\pi\beta H_1(x))\cdot TK_1+pk_\pi\\&=pk_\pi\end{aligned}\tag{2}$$

4.2 扩展方案

(1) 系统初始化 Setup$(\lambda, IC) \to (params, tk)$: 给定安全参数 λ 和非法消息集合 $IC = \{x_1, x_2, \ldots, x_t\}$, 追踪权威执行如下步骤.

① 生成 SM2 数字签名系统参数 $pp = \{p, F_p, q, \mathbb{G}, P, H_1\}$.

② 随机选择追踪密钥 $tk \in \mathbb{Z}_q^*$.

③ 对多个非法消息 $\{x_j, H_1(x_j)\}_{j\in[1,t]}$ 生成多项式 $f(z) = a_0 + a_1 z + a_2 z^2 + \ldots + a_{t-1} z^{t-1}$, 对任意 $j \in [1,t]$, 该多项式满足 $f(x_j) = H_1(x_j)$.

④ 计算 $TK_1 = tk \cdot P$, $TK_2^{(1)} = a_0 \cdot TK_1$, $TK_2^{(2)} = a_1 \cdot TK_1, \ldots, TK_2^{(t)} = a_{t-1} \cdot TK_1$, 设定 $TK_2 = \{TK_2^1, TK_2^2, \ldots, TK_2^t\}$.

⑤ 选择哈希函数 H_2, H_3: $\{0,1\}^* \to \mathbb{Z}_q^*$.

输出系统参数 $params = \{p, F_p, q, \mathbb{G}, P, H_1, H_2, H_3, TK_1, TK_2\}$.

当非法消息集合动态更新为 $IC' = \{x_1', x_2', \ldots, x_t'\}$, 追踪权威需要对 $\{x_j', H_1(x_j')\}_{j\in[1,t]}$ 重新计算多项式 $f'(z) = a_0' + a_1' z + a_2' z^2 + \ldots + a_{t-1}' z^{t-1}$, 对 $j \in [1,t]$ 计算 $TK_2^{(j)\prime} = a_{j-1} \cdot TK_1$, 发布新参数 TK_2' 即可实现非法消息集合更新.

(2) 密钥生成 KeyGen$(params) \to (pk, sk)$: 同第 4.1 节所提方案.

(3) 环签名生成 RSign$(sk_\pi, L, m) \to (\sigma, I_\pi)$: 给定私钥 sk_π, 用户公钥集合 $\{z_1^*, z_2^*, z_3^*, c^*\}$ 和消息 m, 用户 π 执行如下步骤.

① 执行第 4.1 节所提方案步骤①–⑧, T_π 计算为 $d_\pi(\alpha \cdot TK_1 + \beta \cdot (TK_2^{(1)} + m \cdot TK_2^{(2)} + m^2 \cdot TK_2^{(3)} + \ldots + m^{t-1} \cdot TK_2^{(t)}))$.

② 对 $i \in [1,n]$, 计算 $k_i = H_3(c_i)$, $n_i = H_3(k_i, k_{i+1})$. 根据图 2 对 $\{c_1, c_2, \ldots, c_n\}$ 建立默克尔哈希树并获取根节点值 R, 设定 $S = \{(c_i, s_i) | i = 1, 3, \ldots, 2^{\lceil n/2 \rceil - 1} + 1\}$.

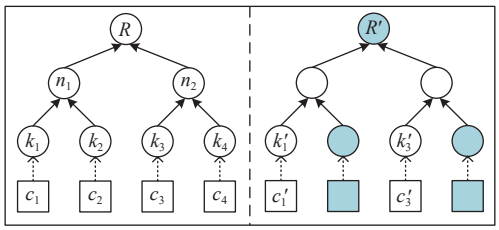


图 2 默克尔哈希树

输出环签名 $\sigma = \{S, R, \psi\}$ 和追踪标签 $I_\pi = \{I_\pi^{(1)}, I_\pi^{(2)}\}$.

(4) 环签名验证 RVerify$(m', \sigma', I_\pi, L) \to 1/0$: 给定消息 m', 环签名 $\sigma' = \{S', R, \psi\}$, 追踪标签 I_π 和用户公钥集合 $L = \{pk_i | i = 1, 3, \ldots, 2^{\lceil n/2 \rceil - 1} + 1\}$, 验证者执行如下步骤.

① 执行第 4.1 节所提方案第 4 步 (环签名验证) 的①和②.

② 对 $i = 1, 3, \ldots, 2^{\lceil n/2 \rceil - 1} + 1$, 计算 $Z_i' = s_i' \cdot P + (s_i' + c_i') \cdot pk_i + I_\pi^{(1)}$, $c_{i+1}' = H_2(L, m', Z_i')$, $k_{i+1}' = H_3(c_{i+1}')$.

③ 设定 $c_1' = c_{n+1}'$, 根据图 2 对 $\{c_1', c_2', \ldots, c_n'\}$ 重构默克尔哈希树并获取根节点值 R'.

④ 验证 $R' = R$ 是否成立, 如果成立则返回 1, 否则返回 0.

(5) 追踪 Trace$(m, \sigma, I_\pi, tk) \to pk_\pi / \perp$: 给定消息 m、环签名 σ、追踪标签 I_π 和追踪密钥 tk, 追踪权威执行如下步骤.

① 如果消息 $m \notin IC$, 返回 $\perp$. 否则计算 $pk_\pi = I_\pi^{(2)} - tk \cdot I_\pi^{(1)}$.

② 返回用户 π 的公钥 pk_π.

- 签名正确性. 同第 4.1 节所提方案.
- 追踪正确性. 如公式 (3) 所示, 用户 π 能够通过公钥 pk_π 被追踪.

$$\begin{aligned} I_\pi^{(2)} - tk \cdot I_\pi^{(1)} &= I_\pi^{(2)} - tk(\alpha + \beta H_1(m)) \cdot pk_\pi \\ &= d_\pi \beta \cdot (TK_2^{(1)} + m \cdot TK_2^{(2)} + m^2 \cdot TK_2^{(3)} + \ldots + m^{t-1} \cdot TK_2^{(t)}) + pk_\pi - tk \cdot \beta H_1(m) \cdot pk_\pi \\ &= d_\pi \beta (a_0 + a_1 m + a_2 m^2 + \ldots + a_{t-1} m^{t-1}) \cdot TK_1 + pk_\pi - d_\pi \beta H_1(m) \cdot TK_1 \\ &= d_\pi \beta f(m) \cdot TK_1 + pk_\pi - d_\pi \beta H_1(m) \cdot TK_1 = pk_\pi \end{aligned} \tag{3}$$

5 安全性分析

定理 1. 如果 ECDLP 假设成立, 基于国密 SM2 支持非法消息追踪的环签名方案满足不可伪造性.

证明: 假定敌手 $\mathcal{A}_{\mathrm{I}}$ 能够以不可忽略的优势赢得不可伪造性游戏, 则存在模拟器 $\mathcal{B}$ 能够以不可忽略的优势解决 ECDLP 问题. 给定 ECDLP 实例 $(P, Q = x \cdot P)$, 模拟器 $\mathcal{B}$ 的目标是输出 x.

系统建立: 模拟器 $\mathcal{B}$ 设定用户公钥集合 $L^* = \{pk_1^* = d_1 \cdot Q, pk_2^* = d_2 \cdot Q, \ldots, pk_n^* = d_n \cdot Q\}$, 其中 $\{d_1, d_2, \ldots, d_n\}$ 从 $\mathbb{Z}_q^*$ 中随机选择. 随后, $\mathcal{B}$ 运行系统初始化算法 $\mathrm{Setup}(\lambda, IC)$ 生成系统参数 $params$ 和追踪密钥 tk, 发送 $params$ 给敌手 $\mathcal{A}_{\mathrm{I}}$.

哈希询问: 敌手 $\mathcal{A}_{\mathrm{I}}$ 对 m 发起哈希询问, 模拟器 $\mathcal{B}$ 检验 $\{m, h\}$ 是否存在于哈希列表中. 如果存在则返回 h; 否则模拟器 $\mathcal{B}$ 随机选择 $h \in \mathbb{Z}_q^*$ 并返回 h.

密钥生成询问: 敌手 $\mathcal{A}_{\mathrm{I}}$ 对用户 π 发起密钥生成询问, 如果 $\pi \in L^*$, 模拟器 $\mathcal{B}$ 返回 pk_π^*. 否则, 模拟器 $\mathcal{B}$ 随机选择 $sk_\pi \in \mathbb{Z}_q^*$, 返回 $pk_\pi = sk_\pi \cdot P$.

腐化询问: 敌手 $\mathcal{A}_{\mathrm{I}}$ 对用户 π 发起腐化询问, 如果 $\pi \in L^*$, 模拟器 $\mathcal{B}$ 返回 $\perp$. 否则, 模拟器 $\mathcal{B}$ 返回私钥 sk_π.

签名询问: 敌手 $\mathcal{A}_{\mathrm{I}}$ 对公钥 pk_π, 用户公钥集合 $L = \{pk_1, pk_2, \ldots, pk_n\}$ 和消息 m 发起签名询问, 如果 $\pi \in L^*$, 模拟器 $\mathcal{B}$ 随机选取 $\alpha, \beta, c_\pi, s_1, s_2, \ldots, s_n \in \mathbb{Z}_q^*$, 计算 $h = H_1(m)$, $T_\pi = tk(\alpha \cdot Q + \beta H_1(x) \cdot Q)$, $I_\pi^{(1)} = (\alpha + \beta h) \cdot pk_\pi$, $I_\pi^{(2)} = T_\pi + pk_\pi^*$, 如图 1 生成零知识证明 ψ, 对 $i = \pi$ 计算 $Z_\pi = s_\pi \cdot P + (s_\pi + c_\pi) \cdot pk_\pi^* + I_\pi^{(1)}$, $c_{\pi+1} = H_2(L, m, Z_\pi)$, 对 $i \in [1, n]$, $i \neq \pi$ 计算 $Z_i = s_i \cdot P + (s_i + c_i) \cdot pk_i + I_\pi^{(1)}$, $c_{i+1} = H_2(L, m, Z_i)$, 添加 $\{L, m, Z_{\pi-1}, c_\pi\}$ 到哈希列表, 返回环签名 σ 和追踪标签 I_π. 否则, 模拟器 $\mathcal{B}$ 运行环签名生成算法 $\mathrm{RSign}(sk_\pi, L, m)$ 并返回 $\{\sigma, I_\pi\}$.

伪造: 敌手 $\mathcal{A}_{\mathrm{I}}$ 对 (L^*, m^*) 生成伪造的环签名 $\sigma^* = \{c_1, s_1, s_2, \ldots, s_n, \psi\}$ 和追踪标签 I^*. 根据分叉引理, 模拟器 $\mathcal{B}$ 能够运行敌手 $\mathcal{A}_{\mathrm{I}}$ 得到基于相同消息的两组有效签名, 如公式 (4) 所示:

$$\begin{cases} (m, Z_1, Z_2 \ldots, Z_n, c_1, c_2 \ldots, c_n, s_1, s_2 \ldots, s_n) \\ (m, Z_1, Z_2 \ldots, Z_n, c_1', c_2' \ldots, c_n', s_1', s_2' \ldots, s_n') \end{cases} \tag{4}$$

其中, 存在 $i \in [1, n]$ 满足 $Z_i = Z_i'$, $c_i \neq c_i'$, $s_i \neq s_i'$. 由此可得等式 (5):

$$\begin{cases} Z_i = s_i \cdot P + (s_i + c_i) \cdot pk_i + I_i^{(1)} \\ Z_i' = s_i' \cdot P + (s_i' + c_i') \cdot pk_i + I_i^{(1)} \\ pk_i = \dfrac{s_i' - s_i}{s_i - s_i' + c_i - c_i'} \cdot P = d_i \cdot Q \end{cases} \tag{5}$$

模拟器 $\mathcal{B}$ 输出 ECDLP 问题的解 $x = (s_i' - s_i)/d_i(s_i - s_i' + c_i - c_i')$. 因此, 根据 ECDLP 假设, 本文方案在随机预言机模型下满足不可伪造性. 证毕.

定理 2. 基于国密 SM2 支持非法消息追踪的环签名方案满足匿名性.

证明: 该性质通过公钥集合中任意用户生成环签名的概率统计不可区分证明.

系统建立: 模拟器 $\mathcal{B}$ 运行系统初始化算法 $\mathrm{Setup}(\lambda, IC)$ 生成系统参数 $params$ 和追踪密钥 tk, 发送 $params$ 给敌手 $\mathcal{A}_{\mathrm{II}}$.

密钥生成询问: 敌手 $\mathcal{A}_{\mathrm{II}}$ 对用户 π 发起密钥生成询问, 模拟器 $\mathcal{B}$ 随机选择 $sk_\pi \in \mathbb{Z}_q^*$, 返回 $pk_\pi = sk_\pi \cdot P$.

挑战: 敌手 $\mathcal{A}_{\mathrm{II}}$ 发送 (L^*, m^*) 给模拟器 $\mathcal{B}$. 模拟器 $\mathcal{B}$ 随机选择 $\pi \in \{1, 2, \ldots, n\}$, 运行环签名生成算法 $\mathrm{RSign}(sk_\pi, L^*, m^*)$ 返回环签名 σ^* 和追踪标签 I^*.

猜测: 敌手 $\mathcal{A}_{\mathrm{II}}$ 输出猜测值 $\pi' \in \{1, 2, \ldots, n\}$.

若模拟器 $\mathcal{B}$ 成功构造签名 $\{c_i, s_i\}_{i \in [1,n], i \neq \pi}$, 则需要随机选择 $k_\pi \in \mathbb{Z}_q^*$, 并找到合适的 c_π 满足 $r_\pi = c_\pi + \alpha + \beta H_1(m^*)$, $s_\pi = (1 + d_\pi)^{-1}(k_\pi - r_\pi d_\pi) \bmod q$. 此外, $\{c_i, s_i\}_{i \in [1,n], i \neq \pi}$ 需要满足 $Z_i = s_i \cdot P + (s_i + c_i) \cdot pk_i + I_\pi^{(1)}$, $c_{i+1} = H_2(L^*, m^*, Z_i)$, $c_1 = c_{n+1}$. 由此可知, 模拟器 $\mathcal{B}$ 随机选择 $\pi \in \{1, 2, \ldots, n\}$ 并成功构造环签名的概率为 $(q-1)^{-1} \cdot (q-2)^{-1} \cdot \ldots \cdot (q-n+1)^{-1} \cdot (q-n)^{-1}$, 在统计上不可区分. 因此, 敌手 $\mathcal{A}_{\mathrm{II}}$ 猜测正确的概率不大于 $1/n$, 本文方案满足匿名性. 证毕.

定理 3. 如果 ECDDHP 假设成立且 H_1 为抗碰撞的哈希函数, 基于国密 SM2 支持非法消息追踪的环签名方案满足可追踪性.

证明: 该性质通过系统参数与追踪标签的随机自归约证明, 即给定 $\{P,Q_1,Q_2,Q_3\}\in\mathbb{G}$, 如果 $\{P,Q_1,Q_2,Q_3\}$ 和 $\{P,Q_1,Q_2',Q_3'\}$ 都是 DH 元组, 其中 $\alpha,\beta\in\mathbb{Z}_q^*$, $Q_2'=\alpha\cdot P+\beta\cdot Q_2$, $Q_3'=\alpha\cdot Q_1+\beta\cdot Q_3$, 则 $\{Q_2',Q_3'\}$ 为均匀分布. 如果 $\{P,Q_1,Q_2',Q_3'\}$ 不是 DH 元组, 则 $\{Q_2',Q_3'\}$ 为均匀随机的群元素.

系统建立: 模拟器 $\mathcal{B}$ 运行系统初始化算法 Setup(λ,IC) 生成系统参数 $params$ 和追踪密钥 tk, 发送 $\{params,tk\}$ 给敌手 $\mathcal{A}_{\mathrm{III}}$.

密钥生成询问: 敌手 $\mathcal{A}_{\mathrm{III}}$ 对用户 π 发起密钥生成询问, 模拟器 $\mathcal{B}$ 随机选择 $sk_\pi\in\mathbb{Z}_q^*$, 返回 $pk_\pi=sk_\pi\cdot P$.

签名询问: 敌手 $\mathcal{A}_{\mathrm{III}}$ 对公钥 pk_π, 用户公钥集合 $L=\{pk_1,pk_2,\ldots,pk_n\}$ 和消息 m 发起签名询问, 模拟器 $\mathcal{B}$ 运行环签名生成算法 RSign(sk_π,L,m) 并返回 $\{\sigma,I_\pi\}$.

挑战: 敌手 $\mathcal{A}_{\mathrm{III}}$ 发送 (L^*,m^*) 给模拟器 $\mathcal{B}$. 其中 $m^*\notin IC$. 模拟器 $\mathcal{B}$ 随机选择 $\pi\in\{1,2,\ldots,n\}$, 运行环签名生成算法 RSign(sk_π,L^*,m^*) 返回环签名 σ^* 和追踪标签 I^*.

猜测: 敌手 $\mathcal{A}_{\mathrm{III}}$ 输出猜测值 $\pi'\in\{1,2,\ldots,n\}$.

若模拟器 $\mathcal{B}$ 成功构造追踪标签 $I^*=\{I^{(1)*},I^{(2)*}\}$, 则满足公式 (6):

$$\begin{cases} TK_1=tk\cdot P,\ TK_2=H(x)\cdot TK_1 \\ I^{(1)*}=d_\pi(\alpha\cdot P+\beta H_1(m^*)\cdot P) \\ T^*=d^*(\alpha\cdot TK_1+\beta H(x)\cdot TK_1) \\ I^{(2)*}=T^*+pk^* \end{cases} \tag{6}$$

由此可知, 当该用户发布非法消息时 (存在 $x=m^*$), $\{P,Q_1=TK_1,\ Q_2=H(x)\cdot P,\ Q_3=TK_2\}\in\mathbb{G}$ 和 $\{P,\ TK_1,\ Q_2'=I^{(1)*},\ Q_3'=T^*\}$ 构成随机 DH 元组, $\{Q_2'=I^{(1)*},\ Q_3'=T^*\}$ 为均匀分布, 根据 ECDDHP 假设, $\{I^{(1)*},T^*\}$ 与随机群元素计算不可区分. 但由于 $x=m^*$, 拥有追踪密钥 tk 的实体能够通过 $I^{(2)*}-tk\cdot I^{(1)*}$ 计算出公钥 pk^*, 从而追踪该恶意用户. 如果该用户没有发送非法消息, 即 $x\neq m^*$, $\{P,\ TK_1,\ Q_2'=I^{(1)*},\ Q_3'=T^*\}$ 不是 DH 元组, 则 $\{I^{(1)*},I^{(2)*}\}$ 对任意实体都是均匀随机的群元素. 因此, 敌手 $\mathcal{A}_{\mathrm{III}}$ 猜测正确的概率不大于 $1/n$, 本文方案满足可追踪性. 证毕.

基于上述定理 1–3, 能够证明扩展方案仍然满足相同安全性要求, 具体证明策略和上述定理的证明过程相同, 原因如下: 1) 扩展方案环签名生成 (第 4.2 节) 的步骤①执行了基础方案环签名生成算法的所有步骤, 两者对消息生成的环签名 $\{c_1,s_1,s_2,\ldots,s_n,\psi\}$ 和对用户生成的追踪标签 $\{I_\pi^{(1)},I_\pi^{(2)}\}$ 相同; 2) 扩展方案环签名生成算法的步骤②引入默克尔哈希树对环签名进行压缩, 即对 $i\in[1,n]$, 计算 $k_i=H_3(c_i)$, $n_i=H_3(k_i,k_{i+1})$, 对 $\{c_1,c_2,\ldots,c_n\}$ 建立默克尔哈希树并获取根节点值 R, 设定 $S=\{(c_i,s_i)\mid i=1,3,\ldots,2^{\lceil n/2\rceil-1}+1\}$. 一方面, 这一压缩操作不改变环签名生成过程和具体形式. 另一方面, 根据默克尔哈希树与环签名结合的可行性研究 [9], 引入默克尔哈希树能够提升环签名的隐私性, 安全性和可扩展性. 综上, 扩展方案能够实现不可伪造性、匿名性和可追踪性.

定理 4. 所提方案 *ZKPoK* 协议在随机预言机模型下是一个非交互式零知识证明系统.

证明: 通过所提方案 *ZKPoK* 协议满足完备性、可靠性和零知识性证明, 具体如下.

完备性: *ZKPoK* 协议的完备性通过签名正确性分析推导 (见第 4.1 节).

可靠性: *ZKPoK* 协议的可靠性利用知识证明系统的可提取性证明. 若存在恶意证明者能够以不可忽略的优势使得验证者接受证明 π^*, 则能够构造一个知识提取器 Ω 以不可忽略的优势输出知识. 具体来说: 假定敌手 $\mathcal{A}$ 能够生成一个有效的副本 $\{U_1,U_2,U_3,z_1,z_2,z_3,c\}$, 其中 $c=H_3(U_1,U_2,U_3,I_\pi^{(1)},I_\pi^{(2)})$, 则知识提取器 Ω 能够通过倒带敌手 $\mathcal{A}$ 至随机预言机询问 $H_3(U_1,U_2,U_3,I_\pi^{(1)},I_\pi^{(2)})$ 之前, 设置预言机使其满足 $c^*=H_3(U_1,U_2,U_3,I_\pi^{(1)},I_\pi^{(2)})\neq c$, 获取另一个有效的副本 $\{U_1,U_2,U_3,z_1^*,z_2^*,z_3^*,c^*\}$. 以该方式, 知识提取器 Ω 能够通过计算 $sk_\pi=(z_3^*-z_3)^{(c-c^*)^{-1}}$, $\beta=((z_2^*-z_2)/sk_\pi)^{(c-c^*)^{-1}}$, $\alpha=((z_1^*-z_1)/sk_\pi)^{(c-c^*)^{-1}}$ 提取知识 $\{sk_\pi,\beta,\alpha\}$ 并生成零知识证明. 因此, *ZKPoK* 协议满足可靠性.

零知识性: 基于 Fiat-Shamir 转换, 我们能够构造模拟器 S 以模拟与任意验证者的交互. 具体来说: 给定要证明的陈述 $\{U_1,U_2,U_3\}$, 模拟器 S 能够随机选择 z_1^*, z_2^*, z_3^*, $c^*\in\mathbb{Z}_q^*$, 计算 $U_1^*=z_1^*(P+TK_1)+c^*I_\pi^{(1)}$, $U_2^*=z_2^*(h\cdot P+TK_2)+c^*I_\pi^{(2)}$, $U_3^*=z_3^*P$, 设置随机预言机使其满足 $c^*=H_3(U_1^*,U_2^*,U_3^*,I_\pi^{(1)},I_\pi^{(2)})$, 最后输出副本 $\{U_1^*,U_2^*,U_3^*,z_1^*,z_2^*,z_3^*,c^*\}$. 可以观察到由于哈希函数 H_3 被模拟为随机预言机, 任意验证者将会接受该副本. 此外, $\{z_1^*,z_2^*,z_3^*,c^*\}$ 的分布与真实协议中的分布

相同, 且模拟器 S 不掌握任何证据信息. 因此, *ZKPoK* 协议满足零知识性. 证毕.

6 性能分析

本节对基于国密 SM2 支持非法消息追踪的环签名方案与相关环签名方案 (文献 [9,13]) 进行性能分析, 包括理论性能分析和实验性能测试.

6.1 理论性能分析

表 2 给出所提方案及其扩展与相关环签名方案的理论性能分析结果, 其中 T_{ms}、T_{as} 分别表示椭圆曲线群 $\mathbb{G}$ 上乘法运算和加法运算的运行时间; T_{bp}、T_{eg}、T_{ag} 分别表示双线性映射运算、双线性群 $\mathbb{G}_1$ 上乘法运算和加法运算的运行时间; $|\mathbb{G}|$、$|\mathbb{G}_1|$、$|\mathbb{Z}_q^*|$ 分别表示群 $\mathbb{G}$、$\mathbb{G}_1$、$\mathbb{Z}_q^*$ 中元素长度; n、t 分别表示环成员数量和非法消息数量.

表 2 理论性能分析

代价		文献[9]	文献[13]	所提方案	扩展方案
计算代价	签名	$(2n-2)T_{eg}+(n-1)T_{ag}$	$(2n-2)T_{ms}+(n-1)T_{as}$	$(2n+6)T_{ms}+(2n+2)T_{as}$	$(2n+t+5)T_{ms}+(2n+t+1)T_{as}$
	验证	$3T_{bp}+nT_{eg}+nT_{ag}$	$2nT_{ms}+nT_{as}$	$(2n+4)T_{ms}+(2n+8)T_{as}$	$(n+t+4)T_{ms}+(n+8)T_{as}$
	追踪	$T_{eg}+2T_{ag}$	—	$T_{ms}+T_{as}$	$T_{ms}+T_{as}$
通信代价		$(n+1)\|\mathbb{Z}_q^*\|+n/2\|\mathbb{G}_1\|$	$(n+1)\|\mathbb{Z}_q^*\|+n\|\mathbb{G}\|$	$(n+1)\|\mathbb{Z}_q^*\|+n\|\mathbb{G}\|$	$(n+3)\|\mathbb{Z}_q^*\|+(n/2+5)\|\mathbb{G}\|$
存储代价		$\|\mathbb{Z}_q^*\|+2\|\mathbb{G}_1\|$	$\|\mathbb{Z}_q^*\|$	$\|\mathbb{Z}_q^*\|$	$\|\mathbb{Z}_q^*\|$

文献 [9] 要求用户执行 $(2n-2)$ 次 T_{eg} 操作和 $(n-1)$ 次 T_{ag} 操作生成环签名, 因此签名计算代价为 $(2n-2)T_{eg}+(n-1)T_{ag}$; 文献 [13] 要求用户执行 $(2n-2)$ 次 T_{ms} 操作和 $(n-1)$ 次 T_{as} 操作生成环签名, 因此签名计算代价为 $(2n-2)T_{ms}+(n-1)T_{as}$; 所提方案要求用户执行 $(2n+6)$ 次 T_{ms} 操作和 $(2n+2)$ 次 T_{as} 操作生成环签名, 因此签名计算代价为 $(2n+6)T_{ms}+(2n+2)T_{as}$; 扩展方案要求用户执行 $(2n+t+5)$ 次 T_{ms} 操作和 $(2n+t+1)$ 次 T_{as} 操作生成环签名, 因此签名计算代价为 $(2n+t+5)T_{ms}+(2n+t+1)T_{as}$.

文献 [9] 要求用户执行 3 次 T_{bp} 操作, n 次 T_{eg} 操作和 n 次 T_{ag} 操作验证签名, 因此验证计算代价为 $3T_{bp}+nT_{eg}+nT_{ag}$; 文献 [13] 要求用户执行 $2n$ 次 T_{ms} 操作和 n 次 T_{as} 操作验证签名, 因此验证计算代价为 $2nT_{ms}+nT_{as}$; 所提方案要求用户执行 $(2n+4)$ 次 T_{ms} 操作和 $(2n+8)$ 次 T_{as} 操作验证签名, 因此验证计算代价为 $(2n+4)T_{ms}+(2n+8)T_{as}$; 扩展方案要求用户执行 $(n+t+4)$ 次 T_{ms} 操作和 $(n+8)$ 次 T_{as} 操作验证签名, 因此验证计算代价为 $(n+t+4)T_{ms}+(n+8)T_{as}$.

文献 [9] 要求追踪权威执行 1 次 T_{eg} 操作和 2 次 T_{ag} 操作来获取用户真实身份, 因此追踪计算代价为 $T_{eg}+2T_{ag}$; 所提方案及其扩展要求追踪权威执行 1 次 T_{ms} 操作和 1 次 T_{as} 操作来获取用户真实身份, 因此追踪计算代价为 $T_{ms}+T_{as}$.

文献 [9] 验证签名需要 $(n+1)$ 个群 $\mathbb{Z}_q^*$ 中元素和 $n/2$ 个群 $\mathbb{G}_1$ 中元素, 因此通信代价为 $(n+1)|\mathbb{Z}_q^*|+n/2|\mathbb{G}_1|$; 文献 [13] 验证签名需要 $(n+1)$ 个群 $\mathbb{Z}_q^*$ 中元素和 n 个群 $\mathbb{G}$ 中元素, 因此通信代价为 $(n+1)|\mathbb{Z}_q^*|+n|\mathbb{G}|$; 所提方案验证签名需要 $(n+4)$ 个群 $\mathbb{Z}_q^*$ 中元素和 $(n+5)$ 个群 $\mathbb{G}$ 中元素, 因此通信代价为 $(n+4)|\mathbb{Z}_q^*|+(n+5)|\mathbb{G}|$; 扩展方案验证签名需要 $(n+3)$ 个群 $\mathbb{Z}_q^*$ 中元素和 $(n/2+5)$ 个群 $\mathbb{G}$ 中元素, 因此通信代价为 $(n+3)|\mathbb{Z}_q^*|+(n/2+5)|\mathbb{G}|$.

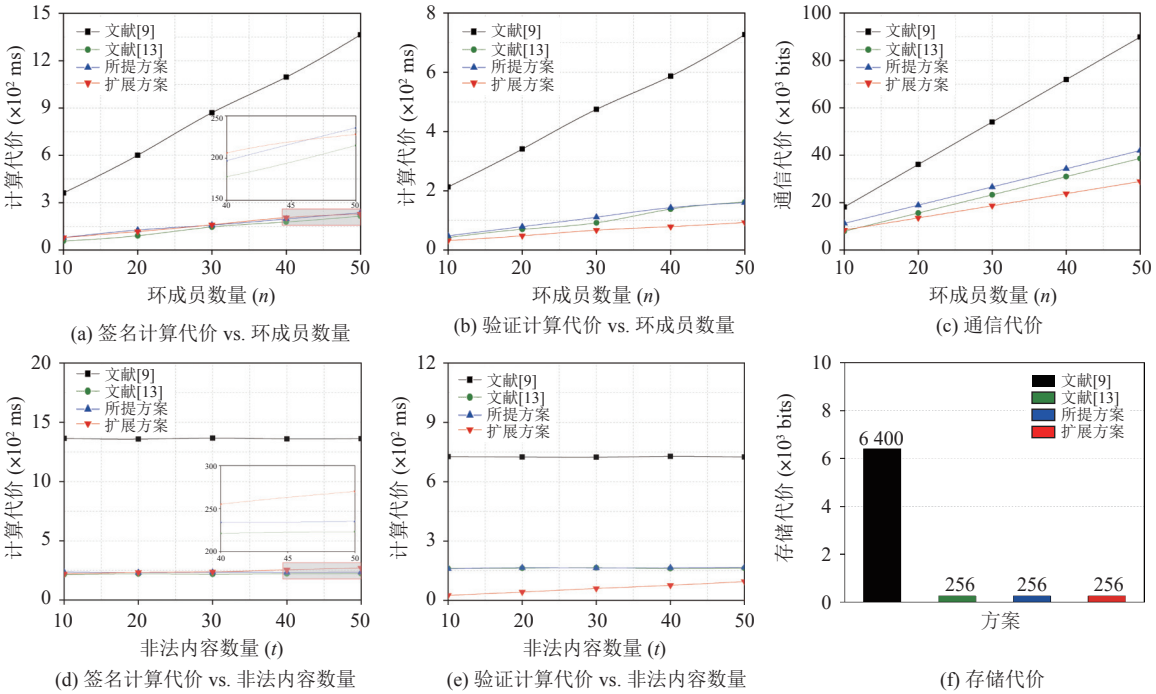
文献 [9] 要求用户存储 1 个群 $\mathbb{Z}_q^*$ 中元素和 2 个群 $\mathbb{G}_1$ 中元素, 因此存储代价为 $|\mathbb{Z}_q^*|+2|\mathbb{G}_1|$; 文献 [13] 要求用户存储 1 个群 $\mathbb{Z}_q^*$ 中元素, 因此存储代价为 $|\mathbb{Z}_q^*|$; 本文所提方案及其扩展要求用户存储 1 个群 $\mathbb{Z}_q^*$ 中元素, 因此存储代价为 $|\mathbb{Z}_q^*|$.

从表 2 可知, 所提方案与相关环签名方案的签名和验证计算代价均随环成员数量 n 线性增长, 追踪计算代价和存储代价恒定. 扩展方案的计算代价额外随非法消息数量 t 线性增长, 这一计算代价是由于追踪权威预先定义 t 个非法消息. 相较于底层环签名方案 (文献 [13]), 所提方案在牺牲较小计算代价的条件下实现了匿名性和可追踪性之间的平衡. 此外, 由于引入默克尔哈希树技术优化签名生成过程, 扩展方案与文献 [9] 的验证计算代价从 $O(2n)$ 降低为 $O(n)$, 通信代价从 $O(n)$ 降为 $O(n/2)$. 相较底层环签名方案[13], 所提方案及其扩展具有较好的有效性.

6.2 实验性能测试

在 128-bits 安全性下, 基于 Java 语言和 JPBC 密码库[29], 使用 SM2 推荐曲线和 Type A 型素数阶曲线对所提方案与相关环签名方案进行实验性能测试. 群 $\mathbb{G}$、$\mathbb{G}_1$、$\mathbb{Z}_q^*$ 中元素长度分别为 512 bits、3 072 bits、256 bits. 实验环境为 Windows 操作系统, 配有 12 核 i5-10400@2.90 GHz 处理器和 16 GB RAM.

图 3 给出了所提方案及其扩展与相关方案随环成员数量 (n) 和非法内容数量 (t) 增长的实验性能结果. 如图 3(a) 和 (d) 所示, 文献 [9] 的签名计算代价最大, 主要原因是用户需要在双线性群下进行签名操作. 根据图 3(b) 和 (e) 所示, 所提方案的验证计算代价与文献 [13] 基本相同, 扩展方案的验证计算代价最小, 主要原因是扩展方案采用默克尔哈希树优化签名生成过程. 当 $n = t = 50$, 文献 [9]、文献 [13]、所提方案和扩展方案的验证计算代价分别为 727 ms、162 ms、160 ms 和 93 ms. 与文献 [9] 和文献 [13] 相比, 扩展方案分别降低验证计算代价 87.21% 和 41.88%. 如图 3(c) 所示, 扩展方案的通信代价最小. 当 $n = t = 50$, 文献 [9]、文献 [13]、所提方案和扩展方案的通信代价分别为 89 856 bits、38 656 bits、41 984 bits 和 28 928 bits. 与文献 [9] 和文献 [13] 相比, 扩展方案分别降低通信代价 67.81 和 25.17%. 图 3(f) 表明所提方案及其扩展的存储代价适中.



(a) 签名计算代价 vs. 环成员数量 (b) 验证计算代价 vs. 环成员数量 (c) 通信代价

(d) 签名计算代价 vs. 非法内容数量 (e) 验证计算代价 vs. 非法内容数量 (f) 存储代价

图 3 实验性能测试结果

总体来说, 图 3 所示的实验性能测试结果与表 2 描述的理论性能分析相匹配. 与文献 [9,13] 相比, 所提方案及其扩展具有高效的验证算法且通信代价更低. 虽然与底层环签名方案[13]相比, 所提方案的签名计算代价较高, 但是所提方案仅允许追踪权威揭示发布非法消息恶意用户的真实身份而诚实用户仍然保持匿名, 增强了诚实用户的隐私保护等级.

7 应 用

传统基于环签名的区块链系统中, 交易发送方选择多个用户组成环, 利用自身私钥和选取用户公钥对消息进行签名, 将真实身份隐藏在环中, 从而实现身份隐私保护. 然而, 在现实应用场景中交易内容可能包含非法消息, 例如欺诈与索要赎金等. 因此, 可监管区块链系统被广泛研究. 本文结合环签名与预限制加密技术, 针对现实应用中

诚实用户隐私和非法用户追踪问题, 应用基于国密 SM2 支持非法消息追踪的环签名方案设计可监管区块链系统, 系统模型如图 4 所示.

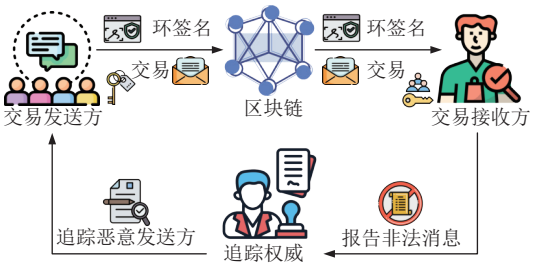


图 4 系统模型

系统由 3 类实体组成: 追踪权威、交易发送方和交易接收方. 追踪权威由服务监管方[30]或监管机构[31]产生, 充当区块链中证书颁发机构 (certification authority, CA)[32], 通过向用户发布公开参数完成系统初始化, 同时负责追踪恶意发送方. 发送方能够自发选择多个成员构成环, 利用自身私钥和选取成员公钥对消息进行签名. 接收方能够通过签名验证交易的合法性并确认签名出自环中某一成员, 但无法得知发送方的真实身份. 此外, 接收方将可能包含非法消息的交易报告给追踪权威, 当且仅当该交易包含非法消息, 追踪权威能够确认该交易的发送方, 否则无法实现追踪.

8 总 结

针对现有环签名方案匿名性和可追踪性之间失衡的问题, 本文提出基于国密 SM2 支持非法消息追踪的环签名方案. 所提方案能够与国产密码算法 SM2 有机融合, 满足密码算法自主可控的要求, 促进国产密码技术应用发展. 同时, 所提方案针对单个非法消息设计追踪机制, 其中追踪权威仅能够揭示发布非法消息恶意用户的真实身份而诚实用户仍然保持匿名, 从而实现匿名性和可追踪性之间的平衡. 此外, 所提扩展方案能够实现任意数量非法消息追踪, 扩大恶意用户监管范围, 降低用户验证开销和通信成本. 安全性分析表明所提方案满足不可伪造性、匿名性和可追踪性. 理论和实验性能分析表明, 所提方案与相关环签名方案相比取得了性能优势, 具有高效的验证算法并且通信代价更低.

References

[1] Liu ZY, Lin JQ. Framework of two-party threshold schemes for SM2 digital signature algorithms. Ruan Jian Xue Bao/Journal of Software, 2025, 36(5): 2188–2211 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6978.htm [doi: 10.13328/j.cnki.jos.006978]

[2] State Cryptography Administration. SM2 elliptic curve cryptographic algorithm. 2010. https://www.oscca.gov.cn/sca/xxgk/2010-12/17/content_1002386.shtml

[3] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). Int'l Journal of Information Security, 2001, 1(1): 36–63. [doi: 10.1007/s102070100002]

[4] Schnorr CP. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4(3): 161–174. [doi: 10.1007/BF00196725]

[5] Zhao YQ, Yang XY, Feng Q, Yu Y. Anonymous credential protocol based on SM2 digital signature. Ruan Jian Xue Bao/Journal of Software, 2024, 35(7): 3469–3481 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6929.htm [doi: 10.13328/j.cnki.jos.006929]

[6] Tu BB, Chen Y. SM2-based adaptor signature with batch proofs and its distributed extension. Ruan Jian Xue Bao/Journal of Software, 2024, 35(5): 2566–2582 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6912.htm [doi: 10.13328/j.cnki.jos.006912]

[7] Tang CH, Zhao YQ, Yang XY, Feng Q, Yu Y. Weighted threshold SM2 signature scheme. Ruan Jian Xue Bao/Journal of Software, 2025, 36(8): 3883–3895 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/7255.htm [doi: 10.13328/j.cnki.jos.007255]

[8] Miao MX, Tang L, Li JW, Zhang XF. New blockchain-based publicly traceable self-tallying voting protocol. IEEE Trans. on Network Science and Engineering, 2024, 11(2): 2034–2046. [doi: 10.1109/TNSE.2023.3336516]

[9] Xue LY, Huang HP, Xiao F, Li Q, Wang ZW. A privacy-enhanced traceable anonymous transaction scheme for blockchain. IEEE Trans. on Information Forensics and Security, 2025, 20: 1176–1191. [doi: 10.1109/TIFS.2025.3526049]

[10] Song JW, Zhang DW, Han X, Du Y. Supervised identity privacy protection scheme in blockchain. Ruan Jian Xue Bao/Journal of Software, 2023, 34(7): 3292–3312 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6517.htm [doi: 10.13328/j.cnki.jos.006517]

[11] Li YN, Yang GM, Susilo W, Yu Y, Au MH, Liu DX. Traceable monero: Anonymous cryptocurrency with enhanced accountability. IEEE Trans. on Dependable and Secure Computing, 2021, 18(2): 679–691. [doi: 10.1109/TDSC.2019.2910058]

[12] Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: Proc. of the 7th Int'l Conf. on Advances in Cryptology (ASIACRYPT 2001). Gold Coast: Springer, 2001. 552–565. [doi: 10.1007/3-540-45682-1_32]

[13] Fan Q, He DB, Luo M, Huang XY, Li DW. Ring signature schemes based on SM2 digital signature algorithm. Journal of Cryptologic Research, 2021, 8(4): 710–723 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000472]

[14] Feng MQ, Lin C, Wu W, He DB. SM2-DualRing: Efficient SM2-based ring signature schemes with logarithmic size. Computer Standards & Interfaces, 2024, 87: 103763. [doi: 10.1016/j.csi.2023.103763]

[15] Huang K, Li X, Yuan S, Liu XY, Zhang XS. Public-Key cryptography in blockchain: Design, analysis, assessment and prospect. Chinese Journal of Computers, 2024, 47(3): 491–524 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2024.00491]

[16] Xie ZJ, Yin XK, Cai RJ, Zhang Y. Traceable ring signature scheme based on domestic cryptographic algorithm SM9. Journal on Communications, 2025, 46(3): 199–211 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-436x.2025041]

[17] Fujisaki E, Suzuki K. Traceable ring signature. In: Proc. of the 10th Int'l Conf. on Public Key Cryptography. Beijing: Springer, 2007. 181–200. [doi: 10.1007/978-3-540-71677-8_13]

[18] Liu JK, Au MH, Susilo W, Zhou JY. Linkable ring signature with unconditional anonymity. IEEE Trans. on Knowledge and Data Engineering, 2014, 26(1): 157–165. [doi: 10.1109/TKDE.2013.17]

[19] Bultel X, Lafourcade P. k-times full traceable ring signature. In: Proc. of the 11th Int'l Conf. on Availability, Reliability and Security. Salzburg: IEEE, 2016. 39–48. [doi: 10.1109/ARES.2016.37]

[20] Zhai MZ, Liu YZ, Wu QH, Qin B, Zheng HB, Dai XP, Ding ZY, Susilo W. Accountable secret committee election and anonymous sharding blockchain consensus. IEEE Trans. on Information Forensics and Security, 2024, 19: 9158–9172. [doi: 10.1109/TIFS.2024.3459608]

[21] Xie JH, Zhou J, Cao ZF, Dong XL, Choo KKR. Linkable, *k*-times traceable, and revocable ring signature for fine-grained accountability in blockchain transactions. IEEE Internet of Things Journal, 2025, 12(4): 4349–4361. [doi: 10.1109/JIOT.2024.3485674]

[22] Ananth P, Jain A, Jin ZZ, Malavolta G. Pre-constrained encryption. In: Proc. of the 13th Innovations in Theoretical Computer Science Conf. Berkeley: Schloss Dagstuhl—Leibniz-Zentrum für Informatik, 2022. 4: 1–4: 20. [doi: 10.4230/LIPIcs.ITCS.2022.4]

[23] Bartusek J, Garg S, Jain A, Policharla GV. End-to-end secure messaging with traceability only for illegal content. In: Proc. of the 42nd Annual Int'l Conf. on Advances in Cryptology (EUROCRYPT 2023). Lyon: Springer, 2023. 35–66. [doi: 10.1007/978-3-031-30589-4_2]

[24] Nguyen TN, Susilo W, Duong DH, Guo FC, Fukushima K, Kiyomoto S. A fault-tolerant content moderation mechanism for secure messaging systems. In: Proc. of the 29th Australasian Conf. on Information Security and Privacy. Sydney: Springer, 2024. 269–289. [doi: 10.1007/978-981-97-5028-3_14]

[25] Huang ZG, Lai JZ, Zeng GX, Weng J. Mild asymmetric message franking: Illegal-messages-only and retrospective content moderation. In: Proc. of the 30th Int'l Conf. on Advances in Cryptology (ASIACRYPT 2024). Kolkata: Springer, 2025. 266–295. [doi: 10.1007/978-981-96-0888-1_9]

[26] Rackoff C, Simon DR. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum J, ed. Advances in Cryptology (CRYPTO 1991). Heidelberg: Springer, 1992. 433–444. [doi: 10.1007/3-540-46766-1_35]

[27] Miller VS. Use of elliptic curves in cryptography. In: Williams HC, ed. Advances in Cryptology. Heidelberg: Springer, 1986. 417–426. [doi: 10.1007/3-540-39799-X_31]

[28] Naor M, Reingold O. Number-theoretic constructions of efficient pseudo-random functions. Journal of the ACM, 2004, 51(2): 231–262. [doi: 10.1145/972639.972643]

[29] de Caro A, Iovino V. jPBC: Java pairing based cryptography. In: Proc. of the 2011 IEEE Symp. on Computers and Communications. Kerkyra: IEEE, 2011. 850–855. [doi: 10.1109/ISCC.2011.5983948]

[30] Liu AD, Du XH, Wang N, Wu XY, Shan DB, Qiao R. Research progress on blockchain system security technology. Chinese Journal of Computers, 2024, 47(3): 608–646 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2024.00608]

[31] Zhang YQ, Ma ZF, Luo SS, Duan PF. Dynamic trust-based redactable blockchain supporting update and traceability. IEEE Trans. on Information Forensics and Security, 2024, 19: 821–834. [doi: 10.1109/TIFS.2023.3326379]

[32] An HY, He DB, Bao ZJ, Peng C, Luo M. Ring signature based on the SM9 digital signature and its application in blockchain privacy protection. Journal of Computer Research and Development, 2023, 60(11): 2545–2554 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.202330265]

附中文参考文献

[1] 刘振亚, 林璟锵. SM2 数字签名算法的两方门限计算方案框架. 软件学报, 2025, 36(5): 2188–2211. http://www.jos.org.cn/1000-9825/6978.htm [doi: 10.13328/j.cnki.jos.006978]

[2] 国家密码管理局. 国家密码管理局关于发布《SM2 椭圆曲线公钥密码算法》公告. 2010 (in Chinese). https://www.oscca.gov.cn/sca/xxgk/2010-12/17/content_1002386.shtml

[5] 赵艳琦, 杨晓艺, 冯琦, 禹勇. 基于 SM2 数字签名的匿名凭证协议. 软件学报, 2024, 35(7): 3469–3481. http://www.jos.org.cn/1000-9825/6929.htm [doi: 10.13328/j.cnki.jos.006929]

[6] 涂彬彬, 陈宇. 支持批量证明的 SM2 适配器签名及其分布式扩展. 软件学报, 2024, 35(5): 2566–2582. http://www.jos.org.cn/1000-9825/6912.htm [doi: 10.13328/j.cnki.jos.006912]

[7] 唐长虹, 赵艳琦, 杨晓艺, 冯琦, 禹勇. 加权门限 SM2 签名方案. 软件学报, 2025, 36(8): 3883–3895. http://www.jos.org.cn/1000-9825/7255.htm [doi: 10.13328/j.cnki.jos.007255]

[10] 宋靖文, 张大伟, 韩旭, 杜晔. 区块链中可监管的身份隐私保护方案. 软件学报, 2023, 34(7): 3292–3312. http://www.jos.org.cn/1000-9825/6517.htm [doi: 10.13328/j.cnki.jos.006517]

[13] 范青, 何德彪, 罗敏, 黄欣沂, 李大为. 基于 SM2 数字签名算法的环签名方案. 密码学报, 2021, 8(4): 710–723. [doi: 10.13868/j.cnki.jcr.000472]

[15] 黄可, 李雄, 袁晟, 刘星宇, 张小松. 区块链中的公钥密码: 设计、分析、密评与展望. 计算机学报, 2024, 47(3): 491–524. [doi: 10.11897/SP.J.1016.2024.00491]

[16] 谢振杰, 尹小康, 蔡瑞杰, 张耀. 基于国密算法 SM9 的可追踪环签名方案. 通信学报, 2025, 46(3): 199–211. [doi: 10.11959/j.issn.1000-436x.2025041]

[30] 刘敖迪, 杜学绘, 王娜, 吴翔宇, 单棣斌, 乔蕊. 区块链系统安全防护技术研究进展. 计算机学报, 2024, 47(3): 608–646. [doi: 10.11897/SP.J.1016.2024.00608]

[32] 安浩杨, 何德彪, 包子健, 彭聪, 罗敏. 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. 计算机研究与发展, 2023, 60(11): 2545–2554. [doi: 10.7544/issn1000-1239.202330265]

作者简介

王晨豪, 博士, 主要研究领域为公钥密码学, 车联网安全与隐私保护.

明洋, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为数据安全与隐私, 车联网安全与隐私保护.

刘行, 博士生, CCF 学生会员, 主要研究领域为公钥密码学, 云存储安全.

邓雨桐, 博士生, CCF 学生会员, 主要研究领域为公钥密码学, 匿名凭证.

赵一, 博士, 副教授, CCF 专业会员, 主要研究领域为公钥密码学, 隐私保护.