基于 Dilithium 的可追踪环签名方案*

刘　健[1,2]，王伊婷[1]，严　妍[3]，霍珊珊[1]，李艳俊[1]

（1. 中国电子科技集团公司第十五研究所　信息产业信息安全测评中心，北京　100083；
2. 清华大学　网络科学与网络空间研究院，北京　100084；
3. 中国网络安全审查认证和市场监管大数据中心，北京　100045）

摘　要：传统基于数论难题的环签名方案面临严峻安全威胁，且完全匿名的特性易被滥用于非法活动。可追踪环签名作为环签名的变体，在满足匿名性的同时，又可追踪恶意签名避免匿名滥用，实现对签名者的可控监管。后量子数字签名方案 Dilithium 具有开销小、运算快且可抵御量子攻击等优点。提出一种基于 Dilithium 的可追踪环签名方案，首次将 NIST 标准化签名算法 Dilithium 与可控匿名性相结合，实现抗量子攻击的隐私保护与滥用追溯双重目标。在随机预言机模型下，证明本方案具有不可伪造性、匿名性、可链接性以及可追踪性。同时，基于 Dilithium 可追踪环签名算法设计了一种跨链交易方案，满足数据交易的隐私保护。与其他方案对比，该方案计算开销显著降低，而通信开销还需进一步优化。

关键词：Dilithium 算法；可追踪环签名；哈希锁定；随机预言机模型

中图分类号：TP309. 7　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 06. 003

引用格式：刘健，王伊婷，严妍，等. 基于 Dilithium 的可追踪环签名方案［J］. 网络安全与数据治理，2025，44(6)：20 - 27.

A traceable ring signature scheme based on Dilithium algorithm

Liu Jian[1,2], Wang Yiting[1], Yan Yan[3], Huo Shanshan[1], Li Yanjun[1]

(1. Information Industry Information Security Evaluation Center, The 15th Research Institute of China Electronics Technology Group Corporation, Beijing 100083, China; 2. Insitute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China; 3. China Cybersecurity Review, Certification and Market Regulation Big Data Center, Beijing 100045, China)

Abstract: Traditional ring signature schemes based on number theory problems face severe security threats, and their completely anonymous characteristics are easily abused for illegal activities. As a variant of ring signature, the trackable ring signature can be traced while satisfying anonymity, while also tracking malicious signatures to avoid anonymity abuse, achieving controllable supervision of the signer. The post-quantum digital signature solution Dilithium has the advantages of small overhead, fast computing and resistance to quantum attacks. A traceable ring signature scheme based on Dilithium is proposed, combining the NIST standardized signature algorithm Dilithium with controllable anonymity for the first time to achieve the dual goals of privacy protection and abuse traceability against quantum attacks. Under the random oracle model, it is proved that this scheme is non-forgery, anonymous, linkability and traceability. At the same time, this paper designs a cross-chain transaction solution based on Dilithium traceable ring signature algorithm to meet the privacy protection of data transactions. Compared with other schemes, this scheme has significantly reduced computational overhead, while communication overhead still needs further optimization.

Key words: Dilithium algorithm; traceable ring signature; hash lock; random oracle model

* 基金项目：云南省区块链应用技术重点实验室开放课题（202305AG340008）

0 引言

随着数据安全向后量子时代迈进，传统的数字签名技术因易暴露身份信息逐渐显现其局限性。环签名[1]作为一种特殊的数字签名技术，可以让用户在不暴露自己身份的情况下进行签名，从而保护用户的隐私。因此，将环签名技术应用于区块链可以有效保护用户的隐私，提高交易的匿名性和安全性。但完全匿名的机制也会造成匿名性滥用的风险，于是，在2006年，Fujisaki等人[2]提出了一种基于离散对数的可追踪环签名，作为环签名的变种，可追踪环签名（Traceable Ring Signature，TRS）在满足匿名性的同时，又可追踪恶意签名，从而避免匿名滥用。2011年，Fujisaki[3]提出了一种基于双线性对的TRS方案，该方案减少了签名大小的长度，提升了效率。2022年，Zhang等[4]提出了一种基于SM2算法的TRS方案，满足了自主安全性。2025年，谢振杰等[5]提出了一种基于SM9算法的TRS方案，该方案兼容国密算法SM9定义的公共参数，效率显著提高。

随着量子计算的快速发展，传统的数字签名技术正面临着严峻的挑战，如基于公钥加密的数论难题会受到Shor算法[6]的威胁。因此，上述基于传统数论难题的方案不再安全。2019年，Branco等[7]提出了第一个抗量子攻击的TRS方案。2021年，Scafuro等[8]提出了一种基于编码理论的TRS方案，该方案减小了签名大小，被广泛认为是抗量子攻击的。2023年，叶青等[9]提出了第一个格上基于身份的TRS方案，该方案在避免了传统数字证书复杂性的同时也能抵御量子攻击，在性能上具有一定优势。同年，Ye等[10]提出了一种基于格的高效可追踪环签名方案，该方案基于TripleRing结构，在签名大小和时间方面有显著优势。

2024年，NIST宣布了三个后量子密码相关标准，分别为CRYSTALS-Kyber[11]、CRYSTALS-Dilithium[12]和SPHINCS+[13]。其中，CRYSTALS-Dilithium作为NIST主要标准的数字签名算法，具有开销小、运算快的优势，能够保证安全性的同时减少密钥和签名大小[14]。2023年，Wen等[15]提出了一种基于Dilithium的可撤销环签名方案，该方案主要应用在车联网场景中。2024年，杨亚涛等[16]提出了一种基于Dilithium的盲签名方案，该方案仅需3轮交互。同年，常鑫[17]提出了一种基于Dilithium的新型基于身份的可撤销环签名方案，该方案在时间开销和存储开销上具有一定优势。

目前基于Dilithium的数字签名方案还有待被提出，并且现有的可追踪环签名方案大多依赖传统数论假设，能够抵御量子攻击的TRS方案还很少。因此，本文提出一种基于Dilithium的高效可追踪环签名方案，既是后量子时代隐私保护技术的迫切需求，也是将格密码理论应用于复杂密码协议的重要探索。

本文主要贡献为以下三个方面：

（1）提出了一种基于Dilithium的可追踪环签名方案，并在随机预言机模型下证明了该方案满足不可伪造性、匿名性以及可追踪性。

（2）结合哈希锁定技术，设计了一种跨链交易方案，能够在数据交互时抵御量子攻击。

（3）分别从计算开销和通信开销两个方面进行了详细性能分析。通过与现有方案对比表明，本方案计算开销显著降低，通信开销还需进一步优化。

1 预备知识

1.1 符号说明

本文符号说明如表1所示。

表1 符号说明

符号	说明
Z^m	m 维整数向量空间
$Z_q^{n\times m}$	模 q 剩余类环上 $n\times m$ 矩阵空间
$\boldsymbol{A}$、$\boldsymbol{A}^{\mathrm{T}}$	矩阵及其转置
k，l	矩阵 $\boldsymbol{A}$ 的行和列
R_q	模 q 商环 $R_q=Z_q[x]/\langle x^d+1\rangle$
H_1、H_2	两个哈希函数
D	R_q 的子集，且 $D=\{d\in R_q,\ \|d\|_\infty\leqslant 1,\ \|d\|_1\leqslant\kappa\}$
$\|\boldsymbol{x}\|$	向量 $\boldsymbol{x}$ 欧几里得范数
κ	在哈希函数的挑战集 D 中
n	环成员数量
S_β	S_β 包含所有 $f\in R=Z[x]/\langle x^d+1\rangle$，$\|f\|_\infty\leqslant\beta$
γ	r_i 系数范围

1.2 格的相关定义

定义1 设 Z^m 是格 Λ 给定的一系列线性无关向量组的集合 $\{\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n\}\subset Z^m$，其形式定义为[18]：

$$\Lambda:=\left\{\sum_{i=1}^{n}\boldsymbol{b}_i x_i \mid x_i\in Z\,\forall\, i=1,\cdots n\right\}\subseteq Z^m \tag{1}$$

给定矩阵 $\boldsymbol{A}\in Z^{n\times m}$ 和向量 $\boldsymbol{u}\in Z_q^n$，可证明下列集合本质上是格：

$$\Lambda_q(\boldsymbol{A}):=\{\boldsymbol{e}\in Z^m \mid \boldsymbol{e}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s} \bmod q,\ \boldsymbol{s}\in Z^n\} \tag{2}$$

$$\Lambda_q^{\perp}(\boldsymbol{A}):=\{\boldsymbol{e}\in Z^m \mid \boldsymbol{A}\boldsymbol{e}=0 \bmod q\} \tag{3}$$

$$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}):=\{\boldsymbol{e}\in Z^m \mid \boldsymbol{A}\boldsymbol{e}=\boldsymbol{u} \bmod q\} \tag{4}$$

1.3 困难假设

定义2（MLWE问题） 给定随机矩阵 $\boldsymbol{A}\leftarrow R_q^{k\times l}$，以

及 R_q 上的概率分布 x，算法 $\mathcal{A}$ 的决策 MLWE 难题的优势为

$$\left|\Pr\left[\mathcal{A}\left(\boldsymbol{A},\ \boldsymbol{As}+\boldsymbol{e}\right)\rightarrow 1\right]-\Pr\left[\mathcal{A}\left(\boldsymbol{A},\ \boldsymbol{v}\right)\rightarrow 1\right]\right| \tag{5}$$

2　可追踪环签名定义及安全模型

2.1　可追踪环签名定义

可追踪环签名算法共由以下五个概念多项式时间算法组成：

（1）Setup(1^λ)：输入安全参数 λ，输出公共参数 params；

（2）KeyGen(params)：输入公共参数 params，输出公私钥对（pk，sk）；

（3）Sign(params，sk_π，U，L，M)：输入公共参数 params，用户 π 的私钥 sk_π，环公钥列表 $U=\{\mathrm{pk}_1,\ \cdots,\ \mathrm{pk}_n\}$，追踪标签 L 和待签消息 $M\in\{0,\ 1\}^*$，输出一个包含追踪标签和消息的签名 σ；

（4）Verify(params，L，M，σ)：输入公共参数 params，标签 L 和有关消息 M 的签名 σ，输出“valid”或“invalid”；

（5）Trace(params，L，M，σ，M'，σ')：输入公共参数 params，标签 L 和（M，σ），（M'，σ'），输出“accept”“link”或公钥 pk。

2.2　安全模型

随机预言机是一种理想化的哈希函数模型，常用于密码学方案的安全性证明。它假设了一个理论上的黑箱，对于任意输入都能返回均匀随机的输出，并且相同输入始终产生相同输出。本方案基于随机预言机模型对其安全性进行证明。

一个安全的 TRS 方案需满足正确性、不可伪造性、匿名性、可链接性和可追踪性。

定义 3（正确性）　TRS 方案满足正确性。要求签名者执行 Sign 算法来生成一个消息签名对，它应该以压倒性的概率有效：

$$\Pr\left[\mathrm{Invalid}\leftarrow\mathrm{Verify}(U_n,\ M,\ \sigma)\ \middle|\ \begin{array}{c}\mathrm{msk},\ \mathrm{params}\leftarrow\mathrm{Setup}(1^\lambda)\\ \mathrm{sk}_i\leftarrow\mathrm{KeyGen}\ (\mathrm{params})\\ \sigma\leftarrow\mathrm{Sign}\ (M,\ \mathrm{sk}_i)\end{array}\right]\leqslant \mathrm{negl}(n) \tag{6}$$

定义 4（不可伪造性）　如果对于所有概率多项式时间算法攻击者 A，$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{forge}}(1^\lambda)$ 的优势可以忽略不计，则 TRS 对自适应选择消息和选择公钥攻击具有不可伪造性。

（1）系统建立：输入安全参数 λ，挑战者 C 调用 Setup 算法，将公共参数 params 发送给攻击者 A。

（2）询问阶段：A 可以进行多项式次访问预言机，并以上述方式进行询问。

（3）伪造阶段：A 在消息 M^*、事件 event^* 和用户公钥集合 U^* 上输出一个签名 σ^*，若以下条件均成立，则 A 在不可伪造性游戏中获胜：

①Verify(params^*，event^*，U^*，M^*，σ^*)="valid"；

②A 未询问过公钥集合 U^* 中任一用户的私钥；

③A 未发起过（M^*，event^*，U^*）的签名询问；

④用户公钥集合 U^* 中任一用户的公钥均由 C 给出。

攻击者 A 在不可伪造性游戏中获胜的优势定义为：

$$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{forge}}=\Pr\left[\mathrm{A\ wins}\right] \tag{7}$$

定义 5（匿名性）　如果对于所有概率多项式时间算法攻击者 A，$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{anon}}(1^\lambda)$ 的优势可以忽略不计，则 TRS 是匿名的。

（1）系统建立：输入安全参数 λ，C 调用 Setup 算法，将公共参数 params 发送给 A。

（2）询问阶段：A 可以进行多项式次访问预言机，并以上述方式进行询问。

（3）挑战阶段：A 对元组（event^*，M^*，U^*）进行签名询问，C 随机选取比特 $b\leftarrow_{\$}\{0,\ 1\}$，并利用 KeyGen 算法计算用户 i^* 的私钥 sk_i^*，执行 Sign 算法，将签名 σ_b^* 作为 i^* 在消息 M^* 上的签名值返回给 A。

（4）猜测阶段：A 针对 b 输出一个猜测 b^*，若 $b^*=b$，则 A 在此游戏中获胜。

攻击者 A 在匿名性游戏中获胜的优势定义为：

$$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{anon}}=\left|\Pr\left[b^*=b\right]-\frac{1}{2}\right| \tag{8}$$

定义 6（可链接性）　如果攻击者 A 优势 $\mathrm{Adv}_{\mathrm{A}}^{\mathrm{Tal}}(1^\lambda)\leqslant\mathrm{negl}(\lambda)$，则 TRS 方案满足可链接性：

$$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{Tal}}(\lambda)=\left[\begin{array}{l}(L,\ (M_1,\ \sigma_1),\ \cdots,\ (M_{n+1},\ \sigma_{n+1}))\leftarrow A(1^\lambda)\\ \mathrm{Verify}(\mathrm{params},\ L,\ M_i,\ \sigma_i)=1\\ \mathrm{Trace}(\mathrm{params},\ L,\ M_i,\ \sigma_i,\ M_j,\ \sigma_j)=\mathrm{accept}\end{array}\right] \tag{9}$$

其中，$\forall i,\ j\in n+1,\ i\neq j$。

定义 7（可追踪性）　如果 $n>1$，对于 $\forall M,\ M'\in\{0,\ 1\}^*$，$\forall\,\mathrm{event}\in\{0,\ 1\}^*$，$\pi,\ \pi'\in[N]$，若有压倒性的概率成立，则 TRS 方案满足可追踪性：

$$\Pr\left[\begin{array}{l}\mathrm{accept},\ \pi\neq\pi'\\ \mathrm{link},\ \pi=\pi',\ M=M'\\ \mathrm{pk}_\pi,\ \pi=\pi',\ M\neq M'\end{array}\right\}\leftarrow\mathrm{Trace}\ (\mathrm{params},\ U,\ M,\ \sigma,\ M',\ \sigma')\ \Bigg|\ \begin{array}{l}\mathrm{params}\leftarrow\mathrm{Setup}(1^\lambda)\\ \mathrm{pk}_i,\ \mathrm{sk}_i\leftarrow\mathrm{KeyGen}\ (\mathrm{params})\\ \sigma\leftarrow\mathrm{Sign}\ (M,\ \mathrm{pk}_i)\\ \sigma'\leftarrow\mathrm{Sign}\ (M',\ \mathrm{pk}_i)\end{array}\Bigg]=1-\mathrm{negl}\ (n) \tag{10}$$

3 方案构造

3.1 系统参数与密钥生成

Setup：输入安全参数

（1）随机生成 $k \times l$ 维矩阵 $\boldsymbol{A} \leftarrow R_q^{k \times l}$；

（2）选取两个安全的哈希函数 $H_1: \{0, 1\}^* \rightarrow D$，$H_2: \{0, 1\}^* \rightarrow R_q^{k \times l}$；

（3）输出公共参数 params = $(\boldsymbol{A}, H_1, H_2)$。

KeyGen：输入公共参数 params

（1）选取随机密钥向量 $\boldsymbol{s}_1$，$\boldsymbol{s}_2 \in R_q$，并对其进行均匀采样，即 $(\boldsymbol{s}_1, \boldsymbol{s}_2) \leftarrow S_\beta^l \times S_\beta^k$；

（2）计算 $t = \boldsymbol{A} \cdot \boldsymbol{s}_1 + \boldsymbol{s}_2$，拆分 $t = t_0 + b \cdot t_1$；

（3）输出公私钥对 $(\mathrm{pk}_i, \mathrm{sk}_i)$，其中 $\mathrm{pk}_i = t_i$，$\mathrm{sk}_i = (\boldsymbol{s}_1, \boldsymbol{s}_2)$。

3.2 签名与验证

Sign：输入 params，sk_π 和消息 $M \in \{0, 1\}^*$

（1）计算标签 $L = (\mathrm{pk}_i, \mathrm{event})$。

（2）计算 $T_0 = H_2(M, L) \in R_q^{k \times l}$，$T_\pi = \boldsymbol{A}^{\mathrm{T}}[\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}_1 + \boldsymbol{s}_2$，$h = (T_\pi - T_0)/\pi$，$T_i = T_0 + h \cdot i$，其中 h 通过计算得到，用于闭合环签名。

（3）对于 $i = \pi$：

①随机采样多项式掩码向量 $\boldsymbol{y} \leftarrow S_{\gamma-1}^k$；

②计算 $e_{\pi+1} = H_1(L, M, T_\pi, \boldsymbol{A}\boldsymbol{y}, \boldsymbol{A}^{\mathrm{T}}\boldsymbol{y})$。

（4）对于 $i = \pi + 1, \cdots, N, 1, \cdots, \pi - 1$：

①随机采样 $r_i \leftarrow S_{\gamma-1}^{l+k}$；

②计算 $e_i = H_1(L, M, T_i, \alpha_i, \beta_i)$，其中 $\alpha_i = \boldsymbol{A}r_i - e_i t_i$，$\beta_i = \boldsymbol{A}^{\mathrm{T}}r_i - e_i T_i$。

（5）计算 $r_\pi = \boldsymbol{y} + e_\pi[\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}}$。

（6）若 $\|r_\pi\|_\infty \geqslant \gamma - \kappa \cdot \beta$：

（7）输出签名 $\sigma = (e_i, h, r_i)$。

Verify：输入 params，L，M 和签名 σ

（1）对于 $\|r_\pi\|_\infty < \gamma - \kappa \cdot \beta$：

（2）计算 $T_0 = H_2(L, M)$。

（3）对于 $i \in N$：

①计算 $\alpha_i = \boldsymbol{A}r_i - e_i t_i$，$\beta_i = \boldsymbol{A}^{\mathrm{T}}r_i - e_i T_i$；

②计算 $e_{i+1} = H_1(L, M, T_i, \alpha_i, \beta_i)$。

（4）验证 $e_1 = H_1(L, M, T_n, \alpha_n, \beta_n) = H_1(L, M, T_\pi, \boldsymbol{A}\boldsymbol{y}, \boldsymbol{A}^{\mathrm{T}}\boldsymbol{y}) = e_{n+1}$ 是否成立，成立则签名有效，输出“valid”；反之签名无效，输出“invalid”。

3.3 追踪

Trace：输入公共参数 params，标签 $L = (\mathrm{pk}_i, \mathrm{event})$ 以及两个签名 σ_1，σ_2

（1）计算 $T_0 = H_2(L, M)$，$T_i = T_0 + h \cdot i$

（2）计算 $T'_0 = H_2(L, M')$，$T'_i = T'_0 + h \cdot i$

（3）若对于所有的 $i \in n$ 都有 $T_i = T'_i$，则链接签名，输出“linked”。若只有一个 $i \in n$ 满足 $T_i = T'_i$，则输出第 i 个位置的 pk_i 公钥；反之则输出“accept”。

3.4 正确性分析

验证 $e_1 = H_1(L, M, T_n, \alpha_n, \beta_n) = e_{n+1}$ 是否成立。

$$\begin{aligned}\alpha_\pi &= \boldsymbol{A}r_\pi - e_\pi t_\pi \\ &= \boldsymbol{A}(\boldsymbol{y} + e_\pi[\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}}) - e_\pi(\boldsymbol{A}\boldsymbol{s}_1 + \boldsymbol{s}_2) \\ &= \boldsymbol{A}\boldsymbol{y}\end{aligned}$$

$$\begin{aligned}\beta_\pi &= \boldsymbol{A}^{\mathrm{T}}r_\pi - e_\pi T_\pi \\ &= \boldsymbol{A}^{\mathrm{T}}(\boldsymbol{y} + e_\pi[\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}}) - e_\pi\left(T_0 + \left(\frac{T_\pi - T_0}{\pi}\right) \cdot \pi\right) \\ &= \boldsymbol{A}^{\mathrm{T}}\boldsymbol{y}\end{aligned}$$

4 安全性证明

定理 1 不可伪造性：在随机预言机模型下，如果 MLWE 问题是困难的，则该方案满足不可伪造性。

证明：假设攻击者 A 以不可忽略的概率 ε 成功伪造签名，则 A 与挑战者 C 之间有以下交互：

（1）系统建立阶段。执行 Setup 算法，挑战者将公共参数 params 发送给 A。

（2）询问阶段。在 L，M，T_i，α_i，β_i 被询问前，进行 $H_1(L, M, T_i, \alpha_i, \beta_i)$，挑战者 C 为了存储询问以及相应的回答，将设置几个初始化为空的列表。

①Hash 询问

（a）H_1 询问。A 随机选择 $k \times l$ 维矩阵 $\boldsymbol{A} \leftarrow R_q^{k \times l}$，并将消息、环成员集合发送至 C，设置列表 List_1。

（b）H_2 询问。C 设置列表 List_2。当 A 发出询问时，C 将 (L, M) 添加到列表 List_2。

②私钥询问。A 输入 (L, M, event) 进行私钥询问，C 询问列表 List_1，并以 $(\mathrm{pk}_i, \mathrm{sk}_i)$ 的形式设置列表 List_3。A 对用户 U_i 进行询问，提取相应的私钥 sk_i 返回至攻击者，并将 $(\mathrm{pk}_i, \mathrm{sk}_i)$ 添加至列表 List_3。

③签名询问。A 对 (M, event) 等发出询问，C 收到请求后，对列表 List_4 的元组展开检查：

（a）检查列表 List_4。

（b）随机选取 $k \times l$ 维矩阵 $\boldsymbol{A} \leftarrow R_q^{k \times l}$。

（c）计算标签 $L = (\mathrm{pk}_i, \mathrm{event})$。

（d）计算 $T_0 = H_2(M, L) \in R_q^{k \times l}$，$T_\pi = \boldsymbol{A}^{\mathrm{T}}[\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}_1 + \boldsymbol{s}_2$，$h = (T_\pi - T_0)/i$，$T_i = T_0 + h \cdot i$。

（e）对于 $i = \pi$：

ⅰ. 随机采样多项式掩码向量 $\boldsymbol{y} \leftarrow S_{\gamma-1}^k$；

ⅱ. 计算 $e_{\pi+1} = H_1(L, M, T_\pi, \boldsymbol{A}\boldsymbol{y}, \boldsymbol{A}^{\mathrm{T}}\boldsymbol{y})$。

（f）对于 $i = \pi + 1, \cdots, n, 1, \cdots, \pi - 1$：

ⅰ. 随机采样 $r_i \leftarrow S_{\gamma-1}^{l+k}$；

ⅱ. 计算 $\alpha_i = \boldsymbol{A}r_i - e_i t_i$，$\beta_i = \boldsymbol{A}^{\mathrm{T}} r_i - e_i T_i$，$e_i = H_1$（$L$，$M$，$T_i$，$\alpha_i$，$\beta_i$）。

（g）计算 $r_\pi = \boldsymbol{y} + e_\pi [\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}}$。

（h）若 $\|r_\pi\|_\infty \geqslant \gamma - \kappa \cdot \beta$：

（i）输出签名 $\sigma = (e_i, h, r_i)$。

（3）伪造阶段。A 输出一个伪造签名 σ^*，并满足定义 4 的条件。

假设攻击者 A 以不可忽略的概率 ε 成功伪造一个有效的签名 $\sigma^* = (e_i^*, h^*, r_i^*)$，通过分叉引理进行重放攻击，由于 $y^* - y'$可忽略，故联立两次签名响应方程消去误差项

$$\begin{cases} r_\pi^* = y^* + e_\pi^* [\boldsymbol{s}_1, \boldsymbol{s}_2]_j^{\mathrm{T}} \\ r'_\pi = y' + e'_\pi [\boldsymbol{s}_1, \boldsymbol{s}_2]_j^{\mathrm{T}} \end{cases} \tag{11}$$

有 $[\boldsymbol{s}_1, \boldsymbol{s}_2]_j^{\mathrm{T}} = (r_\pi^* - r'_\pi)/(e_\pi^* - e'_\pi)$，为最终破解困难问题 MLWE 的解。若 A 成功概率不可忽略，则以 $\varepsilon' = \varepsilon^2/q_H$ 的概率成功破解 MLWE 问题，其中 q_H 为哈希查询次数，与其困难假设矛盾，从而证明本方案在选择消息攻击下满足不可伪造性。

定理 2 匿名性：在随机预言机模型下，如果 MLWE 问题是困难的，则该方案满足匿名性。

证明：挑战者 A 和攻击者 C 之间的游戏用于证明匿名性。对于攻击者两个签名分布在计算上不可区分，则本方案满足匿名性。

（1）系统建立阶段。执行 Setup 算法，挑战者将公共参数 params 发送给 A。

（2）询问阶段。在 L，M，T_i，α_i，β_i 被询问前，进行 H_1（L，M，T_i，α_i，β_i），C 为了存储询问以及相应的回答，将设置几个初始化为空的列表。

①Hash 询问。

（a）H_1 询问。A 随机选择 $k \times l$ 维矩阵 $\boldsymbol{A} \leftarrow R_q^{k \times l}$，并将消息、环成员集合发送至 C，设置列表 List_1。

（b）H_2 询问。C 设置列表 List_2。当 A 发出询问时，C 将（L，M）添加到列表 List_2。

②私钥询问。A 输入（L，M，event）进行私钥询问，C 将私钥返回给攻击者。

③签名询问。A 对（M，event）发出询问，C 通过运行 Sign 算法将签名值返回给攻击者。

（3）挑战阶段。A 提交公共参数，C 随机采样 $r_i \leftarrow S_{\gamma-1}^{k+l}$，计算用户的私钥，运行 Sign 算法，将生成的签名值返回至 A。

（4）猜测阶段。攻击者 A 给出猜想。

分析 A 在赢得匿名游戏中可忽略不计的优势。

挑战者 C 使用 r_{i0} 生成的签名 σ_0 和使用 r_{i1} 生成的签名 σ_1 的分布在计算上不可区分。根据 Sign 算法所生成的签名 $\sigma = (e_i, h, r_i)$，当 $i \neq \pi$ 时，满足 $r_i \leftarrow S_{\gamma-1}^{k+l}$，此时 r_i 在分布 $S_{\gamma-1}^{k+l}$上；当 $i = \pi$ 时，有 $r_\pi = \boldsymbol{y} + e_\pi [\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}}$，由于 $(\boldsymbol{s}_1, \boldsymbol{s}_2) \leftarrow S_\beta^l \times S_\beta^k$ 为均匀采样，服从均匀分布且不可区分，e_π 由安全的哈希函数生成，满足单向性和抗碰撞性，服从均匀分布且不可区分，$\boldsymbol{y} \leftarrow S_{\gamma-1}^k$ 与 $r_i \leftarrow S_{\gamma-1}^{k+l}$ 分布接近，属于同一个随机源，服从均匀分布且不可区分。所以签名 σ 在计算上不可区分。因此，本方案满足匿名性。

定理 3 可链接性：在随机预言机模型下，本方案是不可伪造的，那么对于任意多项式时间攻击者 A 而言，本方案是可链接的。

证明：挑战者 C 和攻击者 A 之间的游戏用于证明可链接性。

（1）系统建立阶段。执行 Setup 算法，C 将公共参数 params 发送给 A。

（2）询问阶段。在 L，M，T_i，α_i，β_i 被询问前，进行 H_1（L，M，T_i，α_i，β_i），C 为了存储询问以及相应的回答，将设置几个初始化为空的列表。

①Hash 询问。

（a）H_1 询问。A 随机选择 $k \times l$ 维矩阵 $\boldsymbol{A} \leftarrow R_q^{k \times l}$，并将消息、环成员集合发送至 C，设置列表 List_1。

（b）H_2 询问。A 设置列表 List_2。当攻击者发出询问时，C 将（L，M）添加到列表 List_2。

②私钥询问。A 输入待签消息、事件和标签进行私钥询问，C 将私钥返回给 A。

③签名询问。A 对消息、事件发出询问，C 通过运行 Sign 算法将签名值返回给 A。

（3）链接。给出两个签名 σ_1 和 σ_2。

A 假设签名 σ_1 和 σ_2 是不可链接的，则链接标签不相等，即 $L_1 \neq L_2$。在上述不可伪造性证明环节中，A 从两个公钥集合中得到了两个秘密值。由于攻击者只允许持有一个秘密值，这与假设中拥有两个签名的私钥相矛盾。因此，本方案满足可链接性。

定理 4 可追踪性：如果对于所有（params，L，M，σ，M'，σ'）满足定义 7 的要求，则本方案满足可追踪性。

证明：（1）当 $M = M'$，$\pi = \pi'$时，有 $T_0 = H_2(M, L) = H_2(M', L) = T'_0$，$T_\pi = \boldsymbol{A}^{\mathrm{T}} [\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}} = T'_\pi$，即 $T_0 + j \cdot (T_\pi - T'_0)/\pi = T'_0 + j \cdot (T'_\pi - T'_0)/\pi$，其中 $j \in n$，此时，追踪算法输出“link”。

（2）当 $M \neq M'$，$\pi = \pi'$时，有 $T_\pi = \boldsymbol{A}^{\mathrm{T}} [\boldsymbol{s}_1, \boldsymbol{s}_2]^{\mathrm{T}} = T'_\pi$，$T_0 = H_2(M, L) \neq H_2(M', L) = T'_0$，此时 T_i 和 T'_i 有共同成分 T_π，追踪算法能够以不可忽略的的概率输

出 pk_{π}。

（3）当 $\pi \neq \pi'$时，可分为两种情况。

①$M = M'$：此时，有 $T_{\pi} \neq T'_{\pi}$，$T_0 = T'_0$，即对于任意 $i \in n$，都有 $T_i \neq T'_i$，故 Trace 算法输出“accept”；

②$M \neq M'$：此时，有 $T_{\pi} \neq T'_{\pi}$，$T_0 \neq T'_0$，同上述情况，对于任意 $i \in n$，都有 $T_i \neq T'_i$，故 Trace 算法输出“accept”。

因此，当 $\pi \neq \pi'$时，Trace 算法输出“accept”。

故本方案满足可追踪性。

5 基于可追踪环签名的跨链交易方案

本方案将跨链技术中的哈希锁定与基于 Dilithium 的可追踪环签名算法相结合，提出了基于可追踪环签名的跨链交易方案。哈希锁定技术易于实现且去中心化高，可避免资金风险。基于 Dilithium 的可追踪环签名算法可隐藏交易发起者身份，抗双花攻击、可抵御量子攻击以及可追溯交易用户恶意操作。在满足匿名性的同时，实现对交易用户的有效监管。

（1）交易初始化阶段

①用户注册

交易方（用户 A）生成随机原像 S，计算其哈希值 $H = \text{hash}(S)$ 公私钥对，并将 H 广播至目标链。用户 A 选取包含自身在内的 n 个节点组成环签名成员组，并生成环成员公钥集合，私钥分片加密存储。在联盟链中注册身份，获取公共参数。

②动态时间锁配置

根据链间通信延迟和历史交易数据，智能合约自动计算时间锁阈值 Time_1（主链锁定时间）和 Time_2（目标链锁定时间），并满足 $\text{Time}_2 < \text{Time}_1$。

③资产锁定

用户 A 在主链部署智能合约。输入哈希值 H、环成员公钥集合以及时间锁 Time_1。合约冻结用户 A 的资产 X。

（2）签名与交易阶段

①环签名构造

用户 A 使用私钥生成相对应签名值，并将其附加至交易。其中签名值中包含可追踪标签的信息。

②跨链交易

接收方（用户 B）验证主链上环签名的有效性，确认哈希值 H 未被篡改且时间锁 Time_1 合理。

（3）资产锁定与解锁阶段

①目标链资产锁定

用户 B 在目标链部署响应合约，输入相同的哈希值 H 以及时间锁 Time_2，冻结等值资产 Y。

②主链资产解锁

用户 B 通过链下通道获取原像 S 后，向主链合约提交 S 验证 $H = \text{hash}(S)$。验证通过后，主链释放资产 X 至用户 B 地址。主链解锁后，触发目标链合约自动释放资产 Y 至用户 A 地址，若任一链超时未完成，双方资产均原路退回。

（4）追踪监管阶段

正常交易中，环签名隐藏实际签名者身份，外部观察者无法区分用户 A 在群组中的具体位置。若检测到双花攻击等欺诈行为，监管方联合密钥持有者解密环签名中的追踪标签，定位恶意节点并冻结其资产。

6 效率分析

本文将所提方案与文献［15］、［17］和［19］方案分别进行计算和通信开销上的对比分析。

由于本方案是基于 Dilithium 算法，为了更符合 PQC 标准化，本文采用表 2 中与 Dilithium 中 NIST Level 2 安全级别相同的参数，为了评估总运行时间，本文结合 CRYSTALS-Dilithium 的官方实现和数论库 Python3 - cypari2 实现了基本操作[15]。符号说明及执行时间如表 3 所示。

表 2 参数设置和大小

参数设置	参数大小
安全等级	NIST Level 2（128 bits）
q	8 380 417
d	256
k	4
l	4
κ	39
β	2
γ	2^{17}

表 3 符号和执行时间

符号	说明	时间/μs
T_{H1}	计算 H_1 从 D 中获得挑战值的时间	281.3
T_{H2}	计算 H_2 的时间	40.5
T_q^{sp}	从 R_q 中随机采样	11.4
T_{β}^{sp}	从 S_{β} 中随机采样	2.56
$T_{\gamma-1}^{sp}$	从 $S_{\gamma-1}$ 中随机采样	9.02
T_{klMl}	$R_q^{k\times l}$ 中矩阵与 R_q^l 中向量相乘	186.7
T_{lkMk}	$R_q^{k\times l}$ 中矩阵与 R_q^k 中向量相乘	186.7
T_A	两个元素相加	0.97
T_M	两个元素相乘	3.14

在计算开销方面，本文主要对系统初始化、密钥生成、签名生成以及签名验证阶段进行分析。设 n 为环成

员大小。在系统初始化阶段，随机采样 $k \times l$ 维矩阵 $\boldsymbol{A} \leftarrow R_q^{k \times l}$，其运行时间为 $kl \cdot T_q^{sp}$。在密钥生成阶段，随机采样 $(\boldsymbol{s}_1, \boldsymbol{s}_2) \leftarrow S_\beta^l \times S_\beta^k$，运行时间为 $(l+k)\ T_\beta^{sp}$。故 $T_{\text{Setup + KeyGen}} = kl \cdot T_q^{sp} + (l+k)\ T_\beta^{sp}$。

在签名生成阶段，可分为以下步骤计算运行时间：

（1）计算哈希值与 T_i，运行时间为 $T_{H2} + T_{klMl} + kT_A + (k+l)(T_A + T_M) + (k+l)(T_A + T_M)$。

（2）计算签名环中用户 π 的下一个值 $e_{\pi+1}$，运行时间为 $kT_{\gamma-1}^{sp} + T_{klMl} + T_{lkMk} + kT_A + T_{H1}$。

（3）计算环中其他用户

①随机采样运行时间为 $(n-1)(k+l)\ T_{\gamma-1}^{sp}$；

②计算 e_i 运行时间为 $(n-1)[T_{H1} + (T_{klMl} + 2kT_A + kT_M) + (T_{lkMk} + 2lT_A + lT_M)]$。

（4）计算 r_π 运行时间为 $(l+k)(T_A + T_M)$。

根据步骤（1）~（4），可以计算出签名生成总时间为：

$$T_{\text{Sign}} = nT_{H1} + T_{H2} + [nk + (n-l)\ l]\ T_{\gamma-1}^{sp} + (n+1) \cdot T_{klMl} + nT_{lkMk} + [(2n+1)\ k + (2n-1)\ l]\ T_A + (n+2)\ T_M = (745.52n + 89.16)\ \mu\text{s} \quad (12)$$

在签名验证阶段，验证者检查 $\|r_\pi\|_\infty < \gamma - \kappa \cdot \beta$ 是否成立，计算哈希值的运行时间为 T_{H2}。计算 α_i、β_i 的运行时间为 $n[(T_{klMl} + 2kT_A + kT_M) + (T_{lkMk} + 2lT_A + lT_M)]$。计算 e_{i+1} 的运行时间为 T_{H1}。因此，签名验证总时间为：

$$T_{\text{Verify}} = T_{H2} + n[T_{H1} + T_{klMl} + T_{lkMk} + 2(k+l)\ T_A + (k+l)\ T_M] \quad (13)$$

计算开销对比如表4所示。图1显示随着用户数量的增大，与方案［15］、［17］和［19］相比，本方案效率有显著提升，计算开销明显降低。

表4　计算开销分析　（μs）

方案	Setup + KeyGen	Sign	Verify	总运行时间
文献［19］方案	531.80	5 381.70n + 26.30	5 380.30n	107 620n + 558.10
文献［15］方案	250.10	2 066.20n + 9 429.90	1 938.90n	4 005.10n + 9 680.00
文献［17］方案	250.10	1 990.04n + 8 521.74	1 865.30n	3 855.34n + 8 771.84
本方案	202.88	745.52n + 89.16	695.34n + 40.50	1 440.86n + 129.66

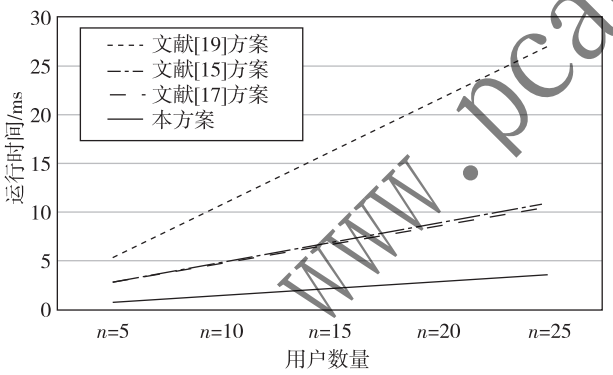

图1　计算开销

在通信开销方面，本文主要对公钥大小、私钥大小以及签名大小进行分析。

公钥：$\text{pk}_i = t_i$，$t_i \in R_q^k$，$R_q = Z_q[x]/(x^d + 1)$，因此公钥大小为：$k \cdot d \cdot \lfloor \log_2 q \rfloor / 8$ B。

私钥：$\text{sk}_i = (\boldsymbol{s}_1, \boldsymbol{s}_2)$，$(\boldsymbol{s}_1, \boldsymbol{s}_2) \leftarrow S_\beta^l \times S_\beta^k$，其中，$S_\beta$ 由 $f \in R = Z[x]/(x^d + 1)$ 组成，使得 $\|f\|_\infty \leqslant \beta$，因此私钥大小为：$(k+l) \cdot d \cdot (\lfloor \log_2 \beta \rfloor + 1 + 1)/8$ B。

签名：$\sigma = (e_i, h, r_i)$，其中，$e_i \in D = \{d \in R_q, \|d\|_\infty \leqslant 1, \|d\| \leqslant \kappa\}$，$h \in R_q^k$，$R_q = Z_q[x]/(x^d + 1)$，$\|r_i\|_\infty \leqslant \gamma - \kappa \cdot \beta$，因此签名大小为：$n \cdot k \cdot d \cdot (\lfloor \log_2 q \rfloor + 1)/8 + d \cdot (\lfloor \log_2 \kappa \rfloor + 1)/8 + n \cdot (k+l) \cdot d \cdot (\lfloor \log_2 (\gamma - \kappa \cdot \beta) \rfloor + 1 + 1)/8$ B。

将表2各参数大小带入公钥私钥以及签名中，可得本方案公钥大小为2.816 KB，私钥大小为0.75 KB，签名大小为7.552n + 0.192 KB。由于文献［19］方案是基于离散对数问题的，因此在分析通信开销时，本方案仅与文献［15］和［17］方案进行对比，结果如表5、图2所示，本文方案公钥小于文献［15］、［17］两方案，但签名效率还有待提升。故本方案通信开销还需进一步优化。

表5　两种方案通信开销分析　（KB）

方案	公钥大小	私钥大小	签名大小
文献［15］方案	2.944	0.750	7.000n + 6.470
文献［17］方案	2.944	1.120	5.888n + 2.912
本方案	2.816	0.750	7.552n + 0.192

7　结束语

本文将后量子 Dilithium 数字签名算法与可追踪环签名结合，提出了一种基于 Dilithium 的可追踪环签名方案，在随机预言机模型下证明了其安全性。同时，本文基于 Dilithium 可追踪环签名方案设计了一种可控监管跨链交

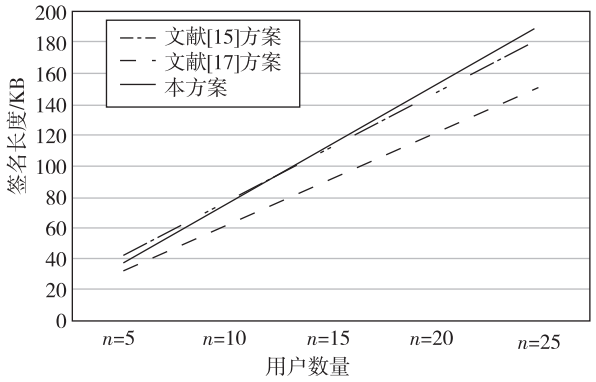

图 2　通信开销

易方案。通过与现有方案进行计算开销和通信开销分析比对，本文所提方案更加高效，并且能够抵抗量子攻击。但仍有一定的局限性，即签名长度随环成员数量线性增长的问题可能限制其在大规模场景中的应用。下一步的工作重点则是减小签名长度，进一步提升实现效率。

参考文献

[1] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C]// Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 552 – 565.

[2] FUJISAKI E, SUZUKI K. Traceable ring signature [C]//Proceedings of 10th International Conference on Practice and Theory in Public-Key Cryptography. Berlin: Springer, 2007: 181 – 200.

[3] FUJISAKI E. Sub-linear size traceable ring signatures without random oracles [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, 95 (1): 151 – 166.

[4] ZHANG Y, WANG Q, LU N, et al. Traceable ring signature schemes based on SM2 digital signature algorithm and its applications in the evidence-storage system [C]//Blockchain and Trustworthy Systems: 4th International Conference, BlockSys 2022. Singapore: Springer Nature Singapore, 2022: 122 – 133.

[5] 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.

[6] LANYON B P, WEINHOLD T J, LANGFORD N K, et al. Experimental demonstration of a compiled version of shor′s algorithm with quantum entanglement [J]. Physical Review Letters, 2007, 99 (25): 250505.

[7] BRANCO P, MATEUS P. A traceable ring signature scheme based on coding theory [C]//Post-Quantum Cryptography: 10th International Conference, PQCrypto 2019. Springer International Publishing, 2019: 387 – 403.

[8] SCAFURO A, ZHANG B. One-time traceable ring signatures [C]// Computer Security-ESORICS 2021: 26th European Symposium on Research in Computer Security. Springer International Publishing, 2021: 481 – 500.

[9] 叶青，陈晴晴，豆永鹏，等. 格上身份基可追踪环签名方案 [J]. 西安电子科技大学学报，2023，50 (2)：161 – 168.

[10] YE Q, LANG Y, GUO H, et al. Efficient lattice-based traceable ring signature scheme with its application in blockchain [J]. Information Sciences, 2023, 648: 119536.

[11] BOS J, DUCAS L, KILTZ E, et al. CRYSTALS-KYBER: a CCA secure module-lattice-based KEM [C]//Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2018: 353 – 367.

[12] DUCAS L, KILTZ E, LEPOINT T, et al. CRYSTALS-Dilithium: a lattice-based digital signature scheme [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018 (1): 238 – 268.

[13] BERNSTEIN D J, HÜLSING A, KÖLBL S, et al. The SPHINCS + signature framework [C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 2129 – 2146.

[14] LYUBASHEVSKY V. Fiat-Shamir with aborts: applications to lattice and factoring-based signatures [C]// International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2009: 598 – 616.

[15] WEN J, BAI L, YANG Z, et al. LaRRS: Lattice-based revocable ring signature and its application for VANETs [J]. IEEE Transactions on Vehicular Technology, 2023, 73 (1): 739 – 753.

[16] 杨亚涛，常鑫，史浩鹏，等. CDBS：基于 CRYSTALS-Dilithium 算法的盲签名方案 [J]. 通信学报，2024，45 (7)：184 – 195.

[17] 常鑫. 基于 CRYSTALS-Dilithium 的特殊数字签名算法设计与实现 [D]. 西安：西安电子科技大学，2024.

[18] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions [C]//Proc of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008: 197 – 206.

[19] ZHANG X, LIU J K, STEINFELD R, et al. Revocable and linkable ring signature [C]//Information Security and Cryptology: 15th International Conference. Springer International Publishing, 2020: 3 – 27.

（收稿日期：2025 – 04 – 08）

作者简介：

刘健（1983 – ），男，博士，正高级工程师，主要研究方向：信息系统管理、信息安全。

王伊婷（1999 – ），通信作者，女，硕士，助理工程师，主要研究方向：数据安全、密码协议设计。E-mail：wangyiting@itstec.org.cn。

严妍（1979 – ），女，本科，高级工程师，主要研究方向：计算机应用、信息系统与信息安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部