基于格签名与智能合约的抗量子去中心化密钥恢复方案研究

程亮[1, 2]

1. 三亚学院，海南 三亚 572022

2. 容淳铭院士工作站，海南 三亚 572022

DOI: 10.61369/TACS.2026070026

摘　　要： Web3.0架构下的数字资产托管与去中心化身份（DID）极度依赖用户私钥的安全性，密钥丢失或遗忘将导致资产永久性损失。现有的社交恢复机制多基于Shamir秘密共享（SSS）算法，但该算法在去中心化场景下缺乏强制访问控制层，存在恶意监护人线下合谋还原密钥的安全隐患；此外，传统方案所依赖的经典公钥密码学面临量子计算的潜在威胁。针对上述问题，本文提出了一种结合抗量子格签名与智能合约的改进型密钥恢复机制。该机制采用分片“盲化－托管”双层架构，将多项式分片进行异或拆分，分别由监护人与智能合约分布式持有；同时引入基于容错学习（LWE）问题的格签名算法作为唯一授权凭证。在恢复阶段，系统强制要求用户出示抗量子签名，经由智能合约验证通过后方可释放关键分片。理论分析与评估表明，该方案在不依赖任何可信第三方机构的前提下，从机制上阻断了 t 个监护人的线下合谋攻击，且具备抵抗量子计算攻击的能力，整体交互开销满足实际工程部署需求。

关 键 词： 去中心化身份；Shamir秘密共享；格密码；智能合约；抗合谋攻击

Research on Anti-quantum Decentralized Key Recovery Scheme Based on Lattice Signature and Smart Contract

Cheng Liang[1,2]

1. Sanya University, Sanya, Hainan 572022

2. Academician Rong Chunming's Workstation, Sanya, Hainan 572022

Abstract: Digital asset custody and decentralized identity (DID) under the Web3.0 architecture heavily rely on the security of users' private keys. Key loss or forgetting will cause permanent loss of assets. Most existing social recovery mechanisms adopt the Shamir Secret Sharing (SSS) algorithm, which lacks mandatory access control layer in decentralized scenarios and suffers from security risks that malicious guardians may collude offline to recover keys. Moreover, traditional public key cryptography faces potential threats from quantum computing. To solve the above problems, this paper proposes an improved key recovery mechanism combining anti-quantum lattice signature and smart contract. The mechanism adopts a double-layer architecture of blinded sharding and custody, splits polynomial fragments via XOR operation and stores them separately by guardians and smart contracts. Meanwhile, the lattice signature algorithm based on Learning With Errors (LWE) is introduced as the sole authorization credential. During key recovery, users must submit valid anti-quantum signatures, and critical fragments can only be released after verification by smart contracts. Theoretical analysis and evaluation show that the proposed scheme prevents offline collusion attacks by t guardians without trusted third parties, possesses anti-quantum performance, and its overall interaction overhead meets practical engineering deployment requirements.

Keywords: decentralized identity; shamir secret sharing; lattice cryptography; smart contract; anti-collusion attack

引言

区块链与去中心化架构赋予了用户对数字资产及自我主权身份（SSI）的绝对控制权。但这把“双刃剑”同时也放大了密钥管理的风险——去中心化意味着一旦主密钥遗失，往往面临无可挽回的灾难性后果。社交恢复（Social Recovery）机制是目前缓解此类单点故障

项目信息：
2025年度海南省高等学校（科研自筹）研究项目 (Hnky2025ZC-13)；
三亚学院中青年教师培养（科研类）项目 (USYJSPY24-50)。

的主流方案，其底层大多依赖 Shamir 秘密共享算法[1]。常规做法是将根密钥切分为 n 份交由不同的监护人保管，集齐 t 个门限分片便能通过拉格朗日插值算回原密钥。问题在于，纯数学意义上的秘密共享先天缺乏访问控制手段。在零信任网络语境下，这种无条件恢复特性极易演变成致命的“执行悖论”。具体而言，若有 t 个监护节点被攻陷或恶意串谋，他们完全可以绕开数据所有者，直接在链下私自重组并窃取核心凭证。尽管部分研究试图通过叠加可信执行环境（TEE）或设置中心化网关来拦截此类攻击[2]，但这无疑又退回到了依赖第三方信任机构的老路，与系统去中心化的初衷背道而驰。另一个不容忽视的远期隐患是量子计算威胁。Shor 算法的问世明确宣告了现有区块链普遍依赖的 RSA、ECDSA 等经典公钥体制的脆弱性[3]。一旦攻击者在未来利用量子算力伪造了用户的授权凭证，整个监护人网络的防御体系将形同虚设。立足于上述痛点，本文设计了一种融合抗量子格签名与智能合约的新型密钥恢复方案。机制的核心思路是对原有多项式分片做二次盲化拆解，并将智能合约改造为不可篡改的去中心化“控制阀”。在真正触发恢复动作前，系统强制要求核验基于 NIST 标准的格签名。这种设计在逻辑底层彻底剥离了“分片保管权”与“恢复启动权”，从机制根源上切断了恶意节点线下合谋的可能性。

一、预备知识

（一）Shamir 秘密共享

$Shamir(t,n)$ 门限秘密共享基于有限域 IF_p 上的多项式插值原理（ p 为大素数）。为分享秘密 $S \in IF_p$，系统构造一个随机的 $t-1$ 阶多项式：

$$f(x)=S+\sum_{j=1}^{t-1} a_j x^j p \tag{1}$$

其中系数 a_j 为随机选取。系统计算 n 个多项式点 $(i,f(i))$ 作为分片分发。当且仅当收集到不少于 t 个分片时，可通过拉格朗日插值公式恢复常数项 S：

$$S=\sum_{i=1}^{t} f(i)\prod_{j=1,j\neq i}^{t}\frac{-j}{i-j}p \tag{2}$$

（二）基于格的数字签名

本方案采用基于模块容错学习问题（Module-LWE）的抗量子签名算法[4]。该算法的安全性规约至在量子多项式时间内无法求解的格最短向量难题（SVP）。签名方案包含三个多项式时间算法：

（1）$KeyGen()\rightarrow(pk,sk)$：生成抗量子公钥 pk 与私钥 sk。

（2）$Sign(sk,m)\rightarrow\sigma$：使用私钥对消息 m 进行签名，输出签名向量 σ。

（3）$Verify(pk,m,\sigma)\rightarrow\{0,1\}$：验证签名有效性，通过输出1，否则输出0。算法满足存在性不可伪造（EUF-CMA）安全特性。

（三）智能合约（Smart Contract）

作为在区块链底层虚拟机上执行的确定性状态机，智能合约天生自带防篡改与公开可审计的属性。本机制直接利用这一特质，彻底摘除了传统架构中对中心化身份认证服务器（IdP）的信任依赖。我们将智能合约本身改造为一个去中心化的“仲裁者”，由它来严密执行格签名的核验逻辑，并根据校验结果硬性干预分片访问状态的跳转。

二、系统模型与威胁模型

（一）实体角色界定

整个密钥恢复协议的运转主要围绕以下三类实体展开：

（1）用户（User）：作为待托管核心资产密钥 的真正所有者。用户需在其本地设备的安全隔离环境（如硬件安全芯片）中，妥善留存用于发起授权的抗量子私钥 。

（2）监护人（Guardians）：由用户在初始化阶段指定的个协同节点。在本设定中，它们被视为“半可信”实体，仅负责盲目保管那些经过异或混淆与二次加密的密钥残块。

（3）智能合约：部署在去中心化账本上的公开逻辑代码。它不仅充当了用户抗量子公钥的链上注册表，更是拦截非法请求、执行权限下放动作的物理控制枢纽。

（二）安全威胁

假设考虑到零信任网络中的极端破坏场景，本方案的威胁模型引入了能力极强的主动攻击者（Active Adversary）。我们假设了最坏的防御环境：攻击者不仅成功渗透了网络，其劫持的监护人节点数量甚至可以涵盖全部的 n 个节点（这意味着恶意用户手中的碎片数量远远突破了常规设定的重组门限 t）。在此基础上，他们试图通过线下私自合并来套取用户的根密钥 s。与此同时，该模型还前瞻性地赋予了攻击者调用未来大规模量子计算机的假想能力。在面临这种“内部全面合谋”叠加“外部量子打击”的绝境下，本方案所要证明的安全底线是：只要缺乏用户本人的真实签名触发，任何企图越权剥离密钥的行为在密码学层面都将被严格界定为计算不可行。

三、方案设计

本方案的执行生命周期分为三个阶段：系统初始化与分发、基于格签名的恢复授权、以及去中心化分片重组。图1 展示了本文所提出的抗量子去中心化密钥恢复机制总体架构。该机制通过“盲化分片托管—格签名授权—智能合约释放—分片协同重组”的流程，将分片持有权与恢复授权权相分离，使监护人在未获得链上授权前无法仅凭本地盲化分片恢复用户根密钥。

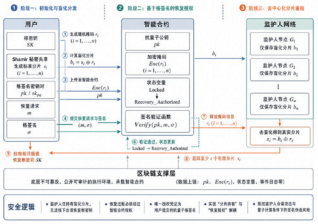

图1 基于格签名与智能合约的抗量子去中心化密钥恢复机制总体架构

（一）系统初始化与盲化分发

在密钥托管阶段，系统不直接向监护人下发具有数学完备性的插值分片，而是采用“盲化 - 拆分”策略。

（1）格密钥生成：用户调用 $KeyGen()$ 生成格密码公私钥对 (pk, sk) ，将公钥 pk 部署至链上智能合约。

（2）多项式构造与求值：用户构造 $t-1$ 阶多项式 $f(x)$ ，使得 $f(0)=S$ 。计算得到 n 个标准分片 $sh_i = f(i)$， $i \in \{1,2,...,n\}$ 。

（3）分片盲化拆分：针对每一个标准分片 sh_i ，用户生成一个等长 的随机掩码向量 r_i 。计算盲化分片：

$$c_i = sh_i \oplus r_i \tag{3}$$

（4）托管部署：用户将 c_i 通过安全信道发送给第 i 个监护人本地存储；随后，将掩码集合 $R=\{r_1, r_2, ..., r_n\}$ 使用监护人的公钥分别加密后，作为状态变量存储在智能合约中。合约初始状态设为 Locked。

（二）基于格签名的恢复授权

当用户遗失密钥 S 需要启动恢复时，无法直接向监护人索要分片（因监护人仅持有毫无意义的 c_i ）。

（1）生成请求与签名：用户使用备用设备（或冷存储介质），构造包含当前时间戳 T 、恢复目标地址 $Addr_{new}$ 在内的恢复请求消息 Req 。用户利用本地的抗量子私钥 sk 计算格签名：

$$\sigma = Sign(sk, Req) \tag{4}$$

（1）上链验证：用户向智能合约广播交易，提交元组 (Req, σ) 。

（2）合约鉴权：智能合约调用链上部署的格签名验证算法 $Verify(pk, Req, \sigma)$ 。若验证通过且时间戳有效（防重放），合约将自身状态从 Locked 更新为 Recovery_Authorized，并将对应加密的掩码分片 R 状态置为可读。

（三）去中心化分片重组

（1）获取掩码：监护人网络监听到智能合约抛出的 Recovery_Authorized 事件后，向合约请求属于自己的加密掩码 r ，并在本地解密。

（2）解除盲化：监护人执行异或逆运算，还原出真实的标准多项式分片：

$$sh_i = c_i \oplus r_i \tag{5}$$

（3）协同插值：t 个在线的监护人通过安全信道将还原后的 sh_i 发送至用户的目标地址 $Addr_{new}$ 。用户端执行拉格朗日插值计算，无损恢复出根密钥 S 。为保障前向安全，恢复完成后智能合约应销毁原有 pk 并强制要求重新执行“系统初始化与盲化分发”。

四、安全性与性能分析

（一）监护人合谋抵抗分析

在标准 SSS 中， t 个监护人合谋可直接恢复 S 。但在本架构中，监护人在未获得智能合约授权前，仅持有盲化分片 c_i 。由于 $c_i = sh_i \oplus r_i$ ，且 r_i 为依均匀分布生成的真随机掩码，根据信息论安全中的一次性密码本（One-Time Pad）原理，单凭 c_i 无法提取出任何关于 sh_i 的有效信息。即使 n 个监护人全部线下合谋，其成功推导 S 的概率严格等于随机猜测的概率。系统安全性从单一的“数学插值门槛”转化为“插值门槛 + 智能合约状态门槛”的双重防御，从根本上消除了线下串谋隐患。

（二）抗量子与抗重放分析

协议中唯一具备访问控制决定权的是用户生成的格签名 σ 。由于 Dilithium 等晶体算法底层依赖 LWE 难题，即使攻击者部署 Shor 算法，也无法在多项式时间内逆向推导出用户的私钥 sk ，从而保证了授权凭证的抗量子伪造性，这符合下一代抗量子区块链的防御需求[5]。同时，恢复请求 Req 中强制绑定了当前时间戳 T 或区块链高度，智能合约对过期签名予以拒绝，从协议层阻断了攻击者截获旧签名并二次发起恢复的重放攻击（Replay Attack）。

（三）性能可行性评估

本方案的计算开销主要集中在智能合约端的格签名验证操作。以以太坊虚拟机（EVM）架构为例，虽然 Dilithium 签名的公钥与签名尺寸相比 ECDSA 较大（约数 KB 级别），导致链上存储与通信 Gas 成本上升；但数字资产恢复属于低频次操作，其安全属性的优先级远高于单次交易开销。结合 Layer 2扩容方案或专用的零知识证明（zk-SNARKs）签名压缩技术，可进一步将链上验证时间控制在百毫秒级以内，完全满足实际工程中的可用性需求。

五、结论

本文针对 Web3与去中心化身份体系中密钥托管方案的合谋漏洞与量子威胁，提出了一种抗量子去中心化密钥恢复机制。该机制创新性地采用盲化多项式拆分架构，并依托智能合约执行基于格签名的访问控制。分析表明，该方案在规避中心化可信机构引入的同时，彻底阻断了恶意监护人的线下合谋，且具备抵抗后量子时代算力攻击的理论安全性，为高价值数字资产的安全管理提供了一种具备较强前瞻性与实用价值的系统方案。

参考文献

[1]SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[2]KOSBA A, MILLER A, SHI E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016: 839-858.

[3]SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE, 1994: 124-134.

[4]DUCAS L, KILTS R, LEPOINT T, et al. CRYSTALS-Dilithium: A lattice-based digital signature scheme[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018(1): 238-268.

[5]FERNÁNDEZ-CARAMÉS T M, FRAGA-LAMAS P. Towards post-quantum blockchain: A review on cyberattacks and defense strategies[J]. IEEE Access, 2020, 8: 21092-21116.

