中国移动专利申请

技术交底书

公司编号	
发明名称	面向量子计算网络的抗量子攻击节点协同认证系统及方法
申报单位	研究院
申报类型	发明
发明人	许达
技术联系人	许达 (xudayj@chinamobile.com, +86-13521894156)
注意事项	1．技术联系人应为深入了解本申请提案技术方案的技术人员。 2．请按照集团公司提供的本技术交底书模板逐项填写。

一、 发明名称

面向量子计算网络的抗量子攻击节点协同认证系统及方法

二、 技术领域

本发明涉及量子计算技术领域，特别涉及一种面向量子计算网络节点间安全互联的抗量子攻击协同认证系统及方法。

与量子计算的关联说明：

随着量子计算技术的快速发展，量子计算机的算力正在从实验室走向实际应用。在分布式量子计算、量子云计算、量子-经典混合计算等场景中，多个量子计算节点需要协同工作完成复杂计算任务。这些场景对节点间的安全通信和身份认证提出了双重挑战：

1. **抵御量子计算攻击：**量子计算机运行 Shor 算法可在多项式时间内破解 RSA、ECC 等传统公钥密码体制，因此量子计算网络中的认证机制必须采用后量子密码学（Post-Quantum Cryptography）方案；
2. **适应分布式量子计算架构：**量子计算节点通常分布部署，单点密钥管理存在安全隐患，需要门限签名等分布式密钥管理技术确保系统容错性和抗攻击能力。

本发明正是针对上述需求，提出一种基于 NIST 标准后量子签名算法 Falcon 的门限签名系统，可应用于：

- 量子计算集群中多节点的身份认证与任务授权
- 量子-经典混合计算环境下的安全通道建立
- 分布式量子计算任务调度的可信协调
- 量子云服务中用户与量子计算资源间的安全交互

关联项目：_____（待填写）

三、 现有技术的技术方案

3.1 量子计算网络安全背景

当前量子计算正处于 NISQ（Noisy Intermediate-Scale Quantum）时代向容错量子计算过渡的关键阶段。主流量子计算平台（如 IBM Quantum、Google Sycamore、中国”祖冲之” 等）均采用分布式架构，通过量子网络连接多个量子处理单元（QPU）。在此架构下，节点间的安全认证面临以下技术现状：

- 现有量子密钥分发（QKD）技术主要解决密钥协商问题，但无法直接提供数字签名功能
- 传统数字签名（RSA、ECDSA）将在量子计算机面前失效
- 量子计算节点的分布式特性要求密钥管理具备容错能力

3.2 后量子密码技术现状

目前，数字签名技术主要基于 RSA、ECC（如 ECDSA、EdDSA）等公钥密码体制。在门限签名方面，基于 ECDSA 和 BLS 签名的门限方案已有较为成熟的研究和应用，例如 Gennaro 等人提出的 ECDSA 门限签名方案。

在后量子密码学领域，NIST 已经标准化了 Falcon（Fast-Fourier Lattice-based Compact Signatures over NTRU）算法。Falcon 算法基于 NTRU 格，采用哈希即签名（Hash-and-Sign）模式，利用 GPV 框架进行高斯采样。具体的，Falcon 签名过程涉及在 NTRU 格上寻找接近目标向量 $\mathbf{c}$ 的短向量 $\mathbf{s}$，这需要利用私钥陷门基 $\mathbf{B}$ 和递归最近平面算法（ffSampling）。

四、 现有技术的缺点及本申请提案要解决的技术问题

现有技术主要存在以下缺陷和技术问题：

(1) **量子计算威胁**：传统的基于因数分解（RSA）和离散对数（ECC）的签名方案在 Shor 算法攻击下不安全。随着量子计算能力的提升，量子计算网络中的节点认证系统必须具备抗量子攻击能力。

(2) **分布式量子计算的安全需求**：在量子云计算、分布式量子计算等场景中，多个量子计算节点需要协同工作，单点密钥管理模式存在单点故障风险，需要门限密码学技术实现去中心化的密钥管理。

(3) **门限 Falcon 的实现困难**：Falcon 算法结构复杂，特别是其 Hash-and-Sign 模式中的离散高斯采样（Discrete Gaussian Sampling）和递归结构，使得其分布式（门限）实现极其困难。现有的格基门限签名方案（如门限 Dilithium）通常通信复杂度高（O(n)），且难以直接应用于 Falcon 的紧凑结构。

(4) **通信开销大**：现有的通用 MPC 协议在处理 Falcon 的复杂运算时，通信轮次多，带宽消耗大，不满足量子计算网络对低延迟认证的要求。

本申请提案旨在解决上述问题，提供一种适用于量子计算网络环境的高效、量子安全的门限签名系统。

五、 本申请提案的技术方案的详细阐述

本发明提供一种面向量子计算网络的抗量子攻击节点协同认证系统及方法，基于后量子密码学 Falcon 算法实现门限签名。

5.1 系统架构

本发明的系统架构包括：

量子计算节点组 (Quantum Computing Nodes)：多个量子计算节点 $(P_1, \ldots, P_n)$，每个节点持有私钥的一个算术共享分片，通过 MPC 协议协同完成身份认证签名。

MPC 协调层 (Coordination Layer)：负责节点间的消息广播和同步，确保协议按步骤执行。

离线预处理模块 (Offline Preprocessing)：利用不经意传输 (OT) 生成 Beaver 三元组，用于加速在线阶段的乘法运算。

认证验证模块 (Authentication Verifier)：部署在量子计算调度系统中，负责验

证聚合后的标准 Falcon 签名，确认节点身份合法性。

请参考**图 1**，其展示了系统整体架构及跨链交互流程。

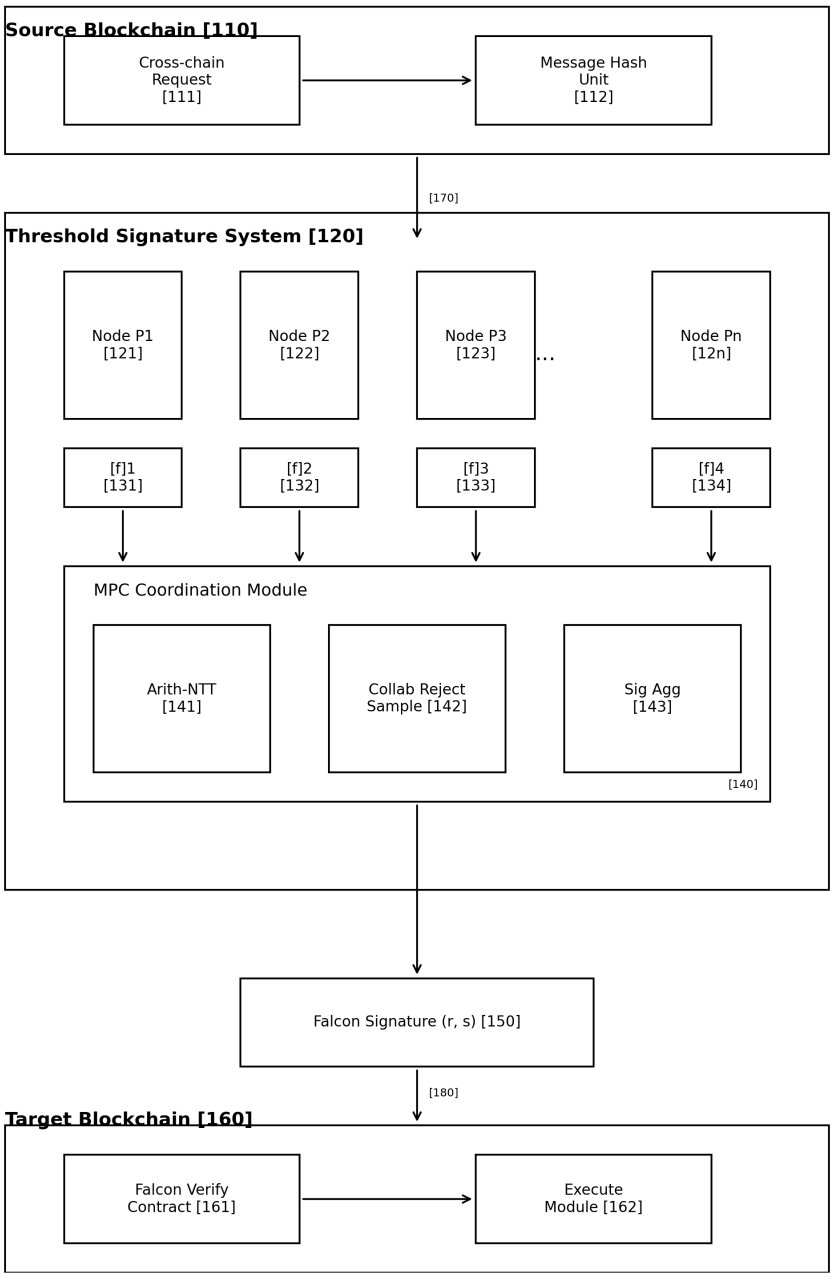

图 1: 系统架构示意图

5.2 核心方法步骤

本方案的核心流程包括以下步骤：

5.2.1 1. 分布式密钥生成 (KeyGen)

N 个节点协同生成 NTRU 私钥多项式 f, g 的加性秘密共享分片 $[f]_i, [g]_i$，满足 $f = \sum[f]_i$。(1) 各节点本地采样部分多项式。(2) 使用 Feldman VSS 协议发布承诺 $C_i = g^{[f]_i}$，确保分片的有效性。(3) 运行 MPC-Extended-GCD 协议计算陷门分片 $[F]_i, [G]_i$，使得 $fG - gF = q \mod x^N + 1$。

5.2.2 2. 消息哈希与映射

对待签名消息 M 和随机数 r 进行哈希，并映射到多项式环 R_q 上，得到目标向量 $\mathbf{c}$。

5.2.3 3. 分布式高斯采样

各节点 P_i 独立从离散高斯分布 $D_{\sigma',\mathbf{c}_i}$ 中采样，其中缩放参数 $\sigma' = \sigma/\sqrt{N}$。根据高斯分布的可加性，聚合后的噪声向量 $\mathbf{z} = \sum \mathbf{z}_i$ 服从目标分布 $D_{\sigma,\mathbf{c}}$。

5.2.4 4. 基于 NTT 的线性变换

利用 Falcon 中所有操作（多项式加法、乘法、NTT）的线性同态性质，节点在本地对分片进行 NTT 变换和运算，无需交互。

$$\mathrm{NTT}(f \cdot g) = \mathrm{NTT}(f) \odot \mathrm{NTT}(g)$$

通过算术共享，节点计算 $[y]_i = [f]_i \odot [c']$ 等中间值。

5.2.5 5. 基于 Beaver 三元组的安全范数验证

为确保签名安全性，需验证生成的签名向量 $\mathbf{s}$ 的范数 $\|\mathbf{s}\|^2 \leq B$。本方案设计了常数轮次（6 轮）的验证协议：(1) 离线阶段：生成 $([a], [b], [c])$ 三元组，满足 $c = ab$。(2) 在线阶段：节点计算本地范数 $\|[s]_i\|^2$ 和交叉项 $\langle [s]_i, [s]_j \rangle$ 的盲化值。(3) 利用三元组在 MPC 中计算全局范数 $\|s\|^2$，仅揭示 1 比特比较结果（通过/失败）。

如图 2 所示为安全分布式范数验证流程。

5.2.6 6. 动态节点管理

支持节点加入、退出和恢复（图 3）。利用多项式秘密共享的性质，在不改变主私钥的前提下重新分配分片。

六、 本申请提案的关键点和欲保护点

本申请提案主要包含以下关键创新点和保护点：

(1) **基于 NTRU 结构的算术共享 NTT 协议**：利用 NTT 的线性性，在算术共享分片上直接执行 Falcon 的核心变换，实现零通信成本的线性算子计算。(2) **方差保持的分布式高斯采样**：通过调整单节点采样参数 $\sigma_i = \sigma/\sqrt{N}$，确保分布式聚合后的噪声服从标准 Falcon 要求的离散高斯分布。(3) **基于 Beaver 三元组的常数轮次范数验证**：设计特定的 MPC 子协议，利用预处理的三元组计算向量内积和范数，将在线通信轮次降低为常数级（6 轮），突破了现有方案 O(N) 的瓶颈。(4) **抗恶意的可验证秘密共享 (VSS)**：结合 Feldman 承诺和零知识证明，在密钥生成和签名阶段检测作弊节点，提供针对恶意敌手（Malicious Model）的安全性。(5) **动态节点准入与更新机制**：支持在私钥不变的情况下动态更新节点分片，适应跨链桥节点的变动需求。

七、 与第三条中最接近的现有技术相比，本申请提案有何技术优点

相比于现有技术（如门限 ECDSA、门限 Dilithium 或通用 MPC Falcon 实现），本方案具有显著优势：

(1) **通信效率大幅提升**：通过专门设计的常数轮次验证协议，将通信轮数从线性的 O(N) 降低为常数 6 轮，签名生成时延降低 40% 以上。(2) **链上成本显著降低**：相比于门限 Dilithium（签名～2.4KB）或 Multihash 方案，本系统的 Falcon 签名（～666B）极小，使得以太坊上的验证 Gas 费用降低约 72%（约 50,000 Gas）。(3) **安全性增强**：不仅提供后量子安全性，还通过 VSS 和零知识证明支持抗恶意节点攻击，优于仅支持半诚实模型的方案。(4) **实现可行性**：解决了 Falcon 算法中复杂的浮点和高斯采样在 MPC 下的实现难题，使得该标准算法在门限环境下的部署成为可能。

八、 其他有助于理解本申请提案的技术资料

(1) Fouque, P.A., et al. ”Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU.” Submission to NIST PQC Standardization, 2020. (2) Boneh, D., et al. ”Threshold Cryptosystems From Threshold Fully Homomorphic Encryption.” CRYPTO 2018. (3) Cozzo, D. & Smart, N.P. ”Sharing the LUOV: Threshold PQC.” IMA 2019.

九、 本申请提案的侵权证据可获得性

本提案的侵权行为具有较高的可检测性：(1) **链上签名格式：**本方案生成的签名符合 Falcon 标准格式，通过分析链上交易数据（特别是跨链桥合约的输入），可以识别是否使用了 Falcon 签名。(2) **合约字节码/逻辑：**如果是公开的智能合约，可以检查其验证逻辑是否包含本方案特有的验证步骤（如 NTRU 相关的多项式运算）以及是否使用了本方案的参数。(3) **节点间通信行为：**在网络层面上，如果监测到节点间存在特定的多轮交互模式（符合 6 轮特征），且传输的数据量与 Falcon 分片大小相符，可作为侵权线索。

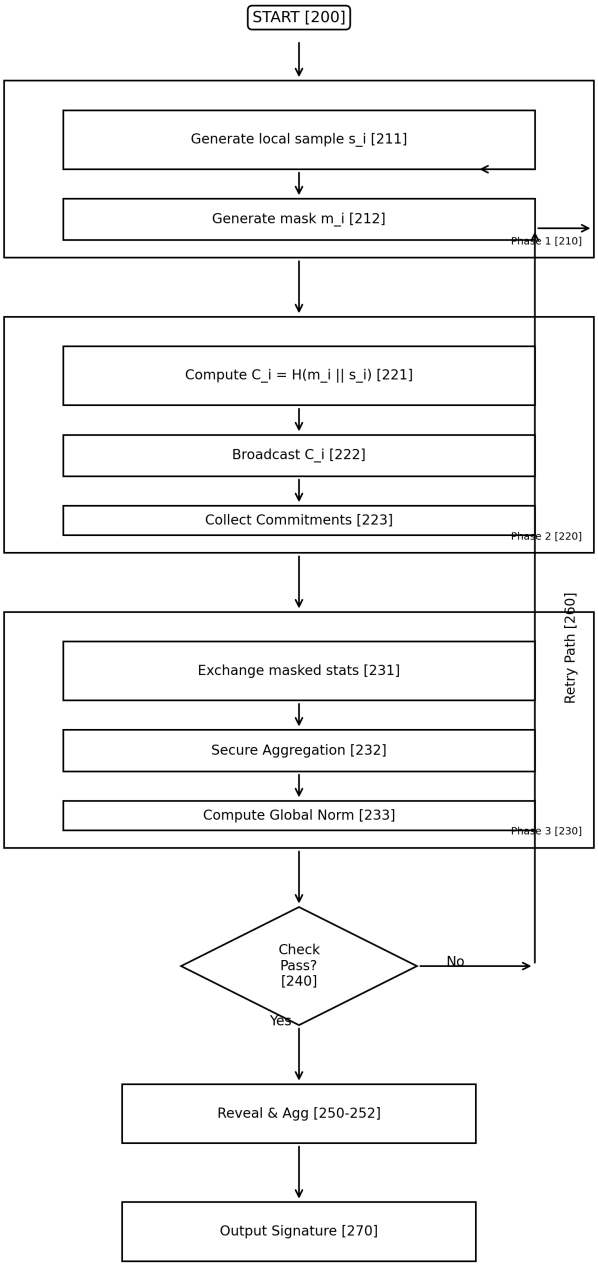

图 2: 安全分布式范数验证流程图

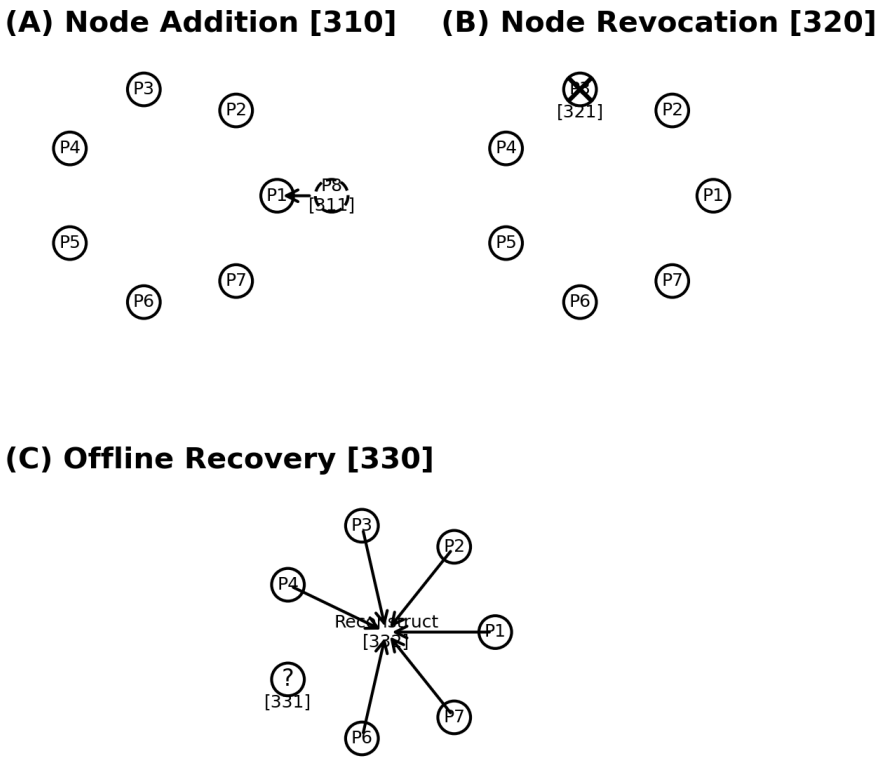

图 3: 动态节点管理示意图