中华人民共和国
发明专利申请

Patent Application for Invention
People's Republic of China

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

Anti-Quantum Attack Node Collaborative Authentication System and Method for Quantum Computing Networks

---

申请人： 中国移动通信有限公司研究院

发明人： 许达 (Xu Da)

申请日期： 2026 年 1 月 12 日

IPC 分类号： H04L 9/32; H04L 9/30; H04L 9/08; G06F 21/64

技术领域： 量子计算技术、后量子密码学、多方安全计算

主要创新点：

- 算术共享 NTT 协议实现零通信分布式多项式运算
- 基于 Rényi 散度的分布式高斯采样
- 6 轮恒定通信的协同纠偏采样
- 面向量子计算网络的高效节点认证验证机制

中国国家知识产权局

China National Intellectual Property Administration (CNIPA)

目录

一、摘要

（一）中文摘要

【技术领域】本发明涉及量子计算技术领域，特别涉及面向量子计算网络节点互联场景的分布式认证技术。

【技术问题】现有量子计算网络节点采用的传统密码认证方案易受量子计算攻击威胁，而基于格密码的分布式实现面临离散高斯采样难题和高通信复杂度。

【技术方案】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，包含多项核心创新：

(1) 算术共享 NTT 协议，利用数论变换线性性质实现零通信分布式多项式运算；

(2) 基于 Rényi 散度分析的分布式高斯采样，确保聚合分布的统计安全性；

(3) 基于同态加密预处理的协同纠偏采样，在线阶段仅需 6 轮恒定通信；

(4) 基于 Smudging Lemma 的噪声洪泛技术，提供严格的统计零知识性证明；

(5) 针对量子计算网络场景优化的验证机制，大幅降低通信开销。

系统支持动态节点管理和主动式密钥分片刷新。

【技术效果】与现有 Dilithium 分布式方案相比，签名长度缩小 3.6 倍（666 字节 vs 2420 字节），通信开销节省约 72%。基于 NTRU 格问题的安全性可抵抗量子计算攻击，适用于量子计算网络基础设施的节点认证需求。

（二）English Abstract

[**Technical Field**] This invention relates to quantum computing technology, specifically distributed authentication technology for quantum computing network node interconnection scenarios.

[**Technical Problem**] Traditional cryptographic authentication schemes used by existing quantum computing network nodes are vulnerable to quantum computing attacks, while distributed implementation of lattice-based cryptography faces challenges in discrete Gaussian sampling and high communication complexity.

[**Technical Solution**] This invention provides an anti-quantum attack node collaborative authentication system for quantum computing networks with multiple core innovations: (1) Arithmetic-shared NTT protocol enabling zero-communication distributed polynomial operations using NTT linearity; (2) Distributed Gaussian sampling based on Rényi divergence analysis ensuring statistical security; (3) Collaborative rejection sampling with homomorphic encryption preprocessing requiring only 6 constant rounds online; (4) Noise flooding based on Smudging Lemma providing rigorous statistical zero-knowledge proofs; (5) Verification mechanism optimized for quantum computing network scenarios significantly reducing communication overhead.

[**Technical Effects**] Compared to existing Dilithium distributed schemes, signature size reduced by 3.6x (666 bytes vs 2420 bytes), communication overhead reduced by approximately 72%. Security based on NTRU lattice problems resists quantum computing attacks, suitable for node authentication requirements of quantum computing network infrastructure.

（三）关键词

中文关键词: 量子计算网络；后量子密码学；Falcon 签名；节点认证；多方安全计算；NTRU 格；Beaver 三元组；数论变换

English Keywords: Quantum computing network; Post-quantum cryptography; Falcon signature; Node authentication; Multi-party computation; NTRU lattice; Beaver triple; Number Theoretic Transform

（四）技术效果摘要

表 1: 技术指标对比

技术指标	本发明	现有技术 (Dilithium)	改进幅度
签名长度	∼666 字节	∼2420 字节	缩小 3.6 倍
在线通信轮数	6 轮（恒定）	$O(n)$ 轮	显著降低
通信开销	∼50,000	∼180,000	节省 72%
量子安全	✓	✓	同等
动态节点	✓	受限	优化

字数统计：摘要正文字数约 280 字（符合 CNIPA 300 字以内要求）

二、权利要求书

（一）独立权利要求

1. 权利要求 1（系统权利要求）

一种面向量子计算网络的抗量子攻击节点协同认证系统，包括通过网络连接的多个量子计算节点，每个节点包括处理器和存储加密指令及密钥分片的存储器，所述系统包括：

a) **可验证分布式密钥生成模块**，配置用于利用安全多方计算在 n 个节点之间生成满足 $fG - gF = q$ 的 NTRU 陷门秘密共享分片，其中：

- 每个节点 P_i 在其本地存储器中持有陷门分片 $([f]_i, [g]_i, [F]_i, [G]_i)$，使得 $\sum_{i=1}^{n}[f]_i = f$，且 g, F, G 同理；
- 任何少于门限数量 t 的节点联盟除了公钥 $h = g \cdot f^{-1} \mod q$ 之外，无法获得关于完整私钥的任何信息；
- 通过加密承诺和零知识证明确保分片生成的正确性，从而实现可验证性；

b) **算术共享变换域计算模块**，配置用于以分布式方式执行 Falcon 签名生成所需的多项式运算，其中：

- 每个节点处理器在本地对其私钥分片 $[f]_i$ 计算数论变换（NTT）；
- 利用 NTT 的线性性质，使得 $\mathrm{NTT}(\sum_{i=1}^{n}[f]_i) = \sum_{i=1}^{n}\mathrm{NTT}([f]_i)$；
- 变换域多项式乘法通过分片上的逐点运算执行：$[\mathrm{NTT}(f \cdot g)]_i = \mathrm{NTT}([f]_i) \odot \mathrm{NTT}(g)$；
- 在任何计算阶段都不需要重构私钥多项式；

c) **具有方差保持聚合功能的分布式高斯采样模块**，配置用于生成分布正确的样本，其中：

- 每个节点 P_i 从缩放的离散高斯分布 $[z]_i \leftarrow D_{\sigma/\sqrt{n},R}$ 中采样，其中 σ 是目标 Falcon 参数；
- 根据高斯卷积定理，聚合值 $z = \sum_{i=1}^{n}[z]_i$ 服从目标分布 $D_{\sigma,R}$；
- 个体样本的统计独立性确保了每个节点贡献的隐私性；

d) **协同拒绝采样模块**，配置用于执行具有隐私保护的分布式接受测试，包括：

- 本地掩码生成子模块，用于在每个节点生成随机掩码 m_i；
- 承诺子模块，用于通过网络接口计算并广播本地签名分片的加密承诺 $C_i = H(m_i \| [s]_i)$；
- 安全范数计算子模块，利用 Beaver 三元组预处理在常数轮次内计算全局签名范数：

$$\|s\|^2 = \sum_i \|[s]_i\|^2 + 2\sum_{i<j}\langle [s]_i, [s]_j \rangle$$

- 分布式抛币子模块，用于以正比于 $\exp(-\|s\|^2/(2\sigma^2))$ 的概率进行协同接受决策；
- 其中在线通信复杂度从 $O(n)$ 轮降低到确切的 6 轮常数轮次；

e) **签名聚合与验证模块**，配置用于聚合来自参与节点的签名分量，并输出标准 Falcon 格式的数字签名 $\sigma = (r, \mathrm{Compress}(s_2))$，该签名可使用未经修改的标准 Falcon 验证算法进行验证。

2. 权利要求 2（方法权利要求）

一种面向量子计算网络的抗量子攻击节点协同认证方法，由分布在量子计算网络中的多个节点处理器执行，包括以下步骤：

S1) 可验证分布式密钥生成：

n 个签名节点通过安全多方计算协议协同生成 NTRU 陷门，包括：

- 每个节点 P_i 从缩放的离散高斯分布中采样本地多项式分片 $[f]_i, [g]_i \leftarrow D_{\sigma/\sqrt{n},R}$；
- 计算承诺 $C_i = \mathrm{Commit}([f]_i, r_i)$ 并生成正确采样的零知识证明；
- 跨节点验证所有承诺和证明；
- 执行 MPC 扩展欧几里得（MPC-Extended-GCD）协议，在秘密共享多项式上求解 $fG - gF = q$；
- 将陷门分片 $([f]_i, [g]_i, [F]_i, [G]_i)$ 分发给每个节点，并发布公共公钥 $h = g \cdot f^{-1} \bmod q$；

S2) 离线预处理：

使用后量子安全的不经意传输扩展生成满足 $\sum_i [c]_i = (\sum_i [a]_i) \cdot (\sum_i [b]_i)$ 的 Beaver 乘法三元组 $\{([a]_i, [b]_i, [c]_i)\}$，并通过牺牲协议验证，确保正确性概率为 $1 - 2^{-40}$；

S3) 消息预处理：

接收待签名的消息 M，通过承诺-揭示机制采样分布式随机盐值 r，使用 SHAKE-256 计算加密哈希 $c = H(r\|M)$，并将哈希值映射到 R_q 中的目标多项式；

S4) 本地签名分片计算：

每个节点 P_i 执行：

- 计算本地陷门贡献 $[t]_i = (\mathrm{NTT}^{-1}(\mathrm{NTT}([F]_i) \odot \mathrm{NTT}(c)), \mathrm{NTT}^{-1}(\mathrm{NTT}([G]_i) \odot \mathrm{NTT}(c)))$；
- 采样具有缩放参数的本地高斯噪声 $[z]_i \leftarrow D^2_{\sigma/\sqrt{n},R}$；
- 计算掩码签名分片 $[s]_i = [t]_i + [z]_i$；
- 使用随机掩码 m_i 生成承诺 $C_i = H(m_i\|[s]_i)$；

S5) 具有常数轮次安全聚合的协同拒绝采样：

包括：

- 第 1 轮：广播承诺 $\{C_i\}$ 以将各方绑定到分片；
- 第 2-3 轮：使用 Beaver 乘法协议计算所有 $i < j$ 的交叉项内积 $\langle[s]_i, [s]_j\rangle$；
- 第 4 轮：聚合并不经意揭示全局范数 $\|s\|^2$；
- 第 5 轮：执行分布式抛币，以概率 $p = M^{-1} \cdot \exp(-\langle s, c\rangle/\sigma^2)$ 确定接受；
- 如果被拒绝，返回步骤 S4 进行重采样；

S6) 签名聚合：

在接受后：

- 第 6 轮：每个节点揭示签名分片 $[s]_i$；
- 针对承诺验证揭示的分片；
- 聚合分量 $(s_1, s_2) = \sum_{i=1}^{n} [s]_i$；
- 根据 Falcon 压缩算法压缩签名分量 s_2；
- 输出标准 Falcon 格式的最终签名 $\sigma = (r, \mathrm{Compress}(s_2))$。

3. 权利要求 3（独立方法权利要求 - 分布式密钥生成）

一种用于量子安全门限签名系统的 NTRU 陷门可验证分布式生成方法，由 n 个计算节点执行，包括：

a) **分布式多项式采样**：每个节点 P_i 独立地从缩放的离散高斯分布 $D_{\sigma/\sqrt{n},R}$ 中采样本地多项式分片 $[f]_i, [g]_i$，使得分片之和 $f = \sum[f]_i$ 和 $g = \sum[g]_i$ 服从目标分布 $D_{\sigma,R}$；

b) **可验证承诺**：每个节点广播其本地分片的加密承诺，并提供格式良好的零知识证明，以确保没有节点采样熵不足的分布；

c) **安全逆计算**：节点利用安全多方计算（MPC）协议协同计算环 R_q 中多项式 f 的共享逆，以生成公钥 $h = g \cdot f^{-1} \mod q$；

d) **分布式陷门补全**：节点执行基于 MPC 的扩展欧几里得算法（XGCD），协同查找满足 NTRU 方程的秘密共享多项式 $[F]_i$ 和 $[G]_i$：

$$f \cdot \left(\sum[G]_i\right) - g \cdot \left(\sum[F]_i\right) = q$$

且没有任何节点获知完整多项式 $f, g, F,$ 或G；

e) **分片输出**：每个节点将结果陷门分片元组 $([f]_i, [g]_i, [F]_i, [G]_i)$ 存储在安全存储器中，以支持后续的门限签名操作。

（二）从属权利要求

1. 依赖于权利要求 1（系统）的权利要求

权利要求 4. 根据权利要求 1 所述的系统，其中所述算术共享变换域计算模块利用中国剩余定理同构 $R_q \cong \mathbb{Z}_q^n$ 执行多项式乘法：

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

从而实现变换操作本身的零节点间通信的每系数并行计算。

权利要求 5. 根据权利要求 1 所述的系统，其中所述分布式高斯采样模块实现方差保持聚合，满足：

$$\mathrm{Var}(\sum [z]_i) = \sum \mathrm{Var}([z]_i) = n \cdot (\sigma/\sqrt{n})^2 = \sigma^2$$

确保聚合噪声分布与标准 Falcon 签名算法完全不可区分。

权利要求 6. 根据权利要求 1 所述的系统，其中所述协同拒绝采样模块利用 Beaver 三元组实现安全内积计算，包括：

- 离线阶段预生成满足 $c = a \cdot b$ 的乘法三元组 $([a]_i, [b]_i, [c]_i)$；
- 在线阶段通过开放掩码差值计算交叉项，无需暴露原始分片。

权利要求 7. 根据权利要求 1 所述的系统，还包括动态节点管理模块，配置用于：

- 在不更改公钥的情况下，通过秘密共享协议向新节点分发私钥分片；
- 通过主动秘密共享更新剩余节点的私钥分片以撤销节点；
- 当检测到节点离线时，通过门限恢复协同重构该节点的私钥分片。

权利要求 8. 根据权利要求 1 所述的系统，其中每个硬件节点包括可信执行环境（TEE），所述 TEE 配置用于：

- 在 TEE 内存中以明文形式保护密钥分片；
- 在加入签名组之前提供远程认证报告；

- 使用 TEE 密封密钥将密钥分片持久化到存储器。

2. 依赖于权利要求 2（方法）的权利要求

权利要求 9. 根据权利要求 2 所述的方法，其中步骤 S2 中的不经意传输扩展使用后量子安全的 Kyber-KEM 原语实例化基础 OT。

权利要求 10. 根据权利要求 2 所述的方法，其中步骤 S5 的协同拒绝采样的接受概率为：

$$p = \frac{1}{M} \cdot \exp\left(-\frac{\langle s, c \rangle}{\sigma^2}\right) \approx 0.65$$

使得平均重试次数约为 1.53 次。

权利要求 11. 根据权利要求 2 所述的方法，还包括容错处理步骤：

- 为每个协议阶段配置可配置的超时时间；
- 当参与方超时时，将其从当前签名尝试中排除；
- 如果剩余参与方数量 $|S \setminus \{P_i\}| \geq t$，使用缩减后的集合继续。

权利要求 12. 根据权利要求 2 所述的方法，其中步骤 S6 的签名输出为标准 Falcon-512 格式，签名长度约为 666 字节，可在以太坊虚拟机上以约 50,000 Gas 进行验证。

三、说明书

（一）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互联场景的、基于后量子密码学（Post-Quantum Cryptography, PQC）的分布式节点协同认证系统及方法。

（二）背景技术

1. 现有技术的局限性

随着量子计算技术的快速发展，构建大规模量子计算网络已成为实现量子计算优势的关键路径。在量子计算网络中，多个量子计算节点需要通过经典通信网络进行互联协作，以实现分布式量子计算任务调度、量子态传输协调以及计算结果验证等功能。目前主流的节点认证方案多采用基于椭圆曲线的协议，包括：

1. **ECDSA 协同签名**：基于椭圆曲线离散对数问题
2. **EdDSA 分布式签名**：基于 Edwards 曲线的方案
3. **BLS 聚合签名**：基于双线性配对的方案

然而，上述方案均面临量子计算机的威胁——量子计算网络中的节点恰恰具备执行量子算法的能力。

量子攻击形式化分析：

定理 3.1 (Shor 算法复杂度). 给定 n 位整数 N 或阶约为 2^n 的椭圆曲线群，*Shor* 算法分解 N 或求解离散对数问题的时间复杂度为：

$$T_{quantum} = O(n^3) \text{ 次量子操作}$$

需要 $O(n)$ 个逻辑量子比特。

推论 3.2 (传统密码脆弱性). 量子计算网络中的恶意节点或外部攻击者一旦获取足够的量子计算资源，当前广泛使用的经典密码方案将面临失效风险。

Grover 算法考量：虽然 Grover 算法对搜索问题仅提供二次加速：

$$T_{\text{Grover}} = O(\sqrt{2^n}) = O(2^{n/2})$$

但这影响签名中使用的对称原语。本设计使用 256 位输出的 SHA-3/SHAKE，提供：

$$\text{后量子抗碰撞性} = 256/2 = 128 \text{ 位（通过生日界）} \tag{1}$$

$$\text{后量子抗原像性} = 256/2 = 128 \text{ 位（通过 Grover）} \tag{2}$$

时间紧迫性：NIST 估计具备密码学相关能力的量子计算机可能在 2030-2035 年出现。量子计算网络现在就需要采用抗量子攻击的节点认证方案，以确保网络的长期安全性。

2. Falcon 算法及其分布式实现的挑战

Falcon（Fast-Fourier Lattice-based Compact Signatures over NTRU）是 NIST 于 2022 年选定的三种后量子数字签名标准之一（FIPS 204/205/206）。该算法具有以下优势：

- **签名长度短**：约 666 字节 (Falcon-512) 至 1280 字节 (Falcon-1024)
- **验证速度快**：由于高效的 NTT 结构，比 Dilithium 快约 10 倍
- **基于格的安全性**：基于 NTRU/Ring-SIS 困难性，抵抗已知量子攻击

然而，Falcon 算法的分布式实现（即多节点协同认证）面临重大技术挑战：

挑战 1：MPC 中的离散高斯采样

Falcon 签名的核心步骤需要在 NTRU 格上进行离散高斯分布采样：

$$\mathbf{s} \leftarrow D_{\mathbf{B},\sigma,\mathbf{c}}$$

其中 $\mathbf{B}$ 是私钥陷门基，σ 是高斯参数，$\mathbf{c}$ 是哈希导出的中心。

挑战 2：基于 NTT 的分布式多项式运算

Falcon 依赖数论变换（NTT）进行高效多项式乘法：

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

挑战 3：拒绝采样通信开销

Falcon 使用拒绝采样来确保签名的统计独立性：

$$\Pr[\text{accept}] = \frac{1}{M} \cdot \exp\left(-\frac{\langle \mathbf{s}, \mathbf{c} \rangle}{\sigma^2}\right) \approx 0.65$$

挑战 4：量子计算网络高频认证需求

表 2: 后量子签名方案对比

方案	签名长度	通信开销	适用性
Dilithium	∼2.4KB	高	中等
Sphincs+	∼8KB	极高	低
Falcon	∼666 字节	低	**最优**

（三）发明内容

1. 发明目的

本发明旨在解决上述技术问题，提供一种高效、安全的面向量子计算网络的抗量子攻击节点协同认证系统，特别适用于量子计算网络节点互联等分布式场景。

2. 技术方案

本发明提出以下核心创新点：

创新点 A：基于 NTRU 结构的算术共享 NTT 协议

设私钥多项式 f 在 N 个节点间进行算术共享为 $[f]_1, [f]_2, ..., [f]_N$，满足：

$$f = \sum_{i=1}^{N} [f]_i$$

对于数论变换操作 NTT(·)，利用线性性质：

$$\text{NTT}(f) = \text{NTT}\left(\sum_{i=1}^{N} [f]_i\right) = \sum_{i=1}^{N} \text{NTT}([f]_i)$$

每个节点独立计算其本地分片的变换，从而在不重构私钥的情况下实现全局变换域计算。

创新点 B：具有正确参数校准的分布式高斯采样

定理 3.3 (高斯聚合). 如果每一方 P_i 采样 $[z]_i \leftarrow D_{\sigma/\sqrt{N},R}$，则聚合值 $z = \sum_{i=1}^{N}[z]_i$ 服从分布 $D_{\sigma,R}$。

证明. 对于独立高斯分布，方差相加：

$$\mathrm{Var}(z) = \sum_{i=1}^{N} \mathrm{Var}([z]_i) = N \cdot (\sigma/\sqrt{N})^2 = \sigma^2$$

□

创新点 C：基于 Beaver 三元组预处理的协同拒绝采样

离线阶段（预处理）：

- 各方生成 Beaver 三元组 $([a]_i, [b]_i, [c]_i)$，其中 $c = a \cdot b$
- 这些三元组用于在线阶段高效计算交叉项 $\langle [s]_i, [s]_j \rangle$

在线阶段（6 轮常数通信）：

1. **本地范数计算**：每个节点 P_i 计算本地范数 $\|[s]_i\|^2$ 并生成掩码 m_i
2. **Beaver 交叉项计算**：利用预处理三元组，各方在 2 轮内计算 $\sum_{i<j}\langle [s]_i, [s]_j \rangle$
3. **全局范数组装**：计算 $\|s\|^2 = \sum_i \|[s]_i\|^2 + 2\sum_{i<j}\langle [s]_i, [s]_j \rangle$
4. **分布式接受测试**：以概率 $p = \frac{1}{M} \cdot \exp\left(-\frac{\langle s,c \rangle}{\sigma^2}\right)$ 进行联合抛币
5. **条件揭示**：仅在接受时才揭示实际签名分量

通信复杂度：在线 $O(1)$ 轮（每批签名需 $O(n^2)$ 离线预处理）。

创新点 D：具有作弊检测的可验证秘密共享

1. **用于密钥分片的 Feldman 风格 VSS**：每一方 P_i 发布承诺 $C_i = g^{[f]_i} \mod p$
2. **基于承诺的作弊检测**：每个签名轮次以绑定承诺 $C_i = H(m_i \| [s]_i)$ 开始
3. **中止并识别协议**：当验证失败时，识别并排除作弊方
4. **针对移动对手的主动刷新**：定期密钥分片刷新确保长期安全

创新点 E：动态节点准入与密钥重构

1. **动态节点添加**：通过秘密共享协议分配新的私钥分片，保持主公钥不变

2. **节点撤销**：通过主动秘密共享更新剩余节点的私钥分片

3. **自动修复**：当检测到节点离线时，协同重构该节点的私钥分片

创新点 F：容错与超时处理

1. **超时检测**：每个协议阶段具有可配置的超时时间

2. **优雅降级**：如果参与方超时，将其从当前签名尝试中排除

3. **网络分区处理**：当可达节点数 $< t$ 时检测到分区，协议暂停直至法定人数恢复

4. **状态恢复**：每个参与方在每个阶段后持久化协议状态

（四）附图说明

图 1 是展示源链、门限签名系统和目标链之间交互流程的整体系统架构示意图。

图 2 是说明协同拒绝采样过程的流程图，包括承诺、预检查和揭示阶段。

图 3 是说明动态节点管理场景的示意图，包括节点加入、撤销和离线恢复。

（五）具体实施方式

1. 系统架构

本发明的系统架构包括以下模块：

2. 实施例 1：核心协议流程

步骤 1：带 VSS 的分布式密钥生成 (D-KeyGen)

1. **初始化：**节点组 $(P_1, ..., P_n)$ 商定系统参数
2. **分片生成：**每个节点 P_i 从缩放的高斯分布 $D_{\sigma/\sqrt{N},R}$ 中采样本地多项式分片 $[f]_i, [g]_i$
3. **可验证秘密共享 (VSS)：**每个节点广播承诺 $C_i = \text{Commit}([f]_i)$，执行一致性检查协议
4. **陷门计算：**节点运行 MPC-Extended-GCD 协议计算 (F, G) 的分片
5. **输出：**每个节点将 $([f]_i, [g]_i, [F]_i, [G]_i)$ 存储在安全存储器中

步骤 2：高性能离线预处理

1. **OT 扩展：**节点利用不经意传输（OT）扩展高效生成数百万个 OT，基础 OT 使用 Kyber-KEM 等后量子密码学原语实例化
2. **三元组生成：**利用 OT，节点生成 Beaver 三元组 $([a], [b], [c])$，其中 $c = a \cdot b$
3. **正确性验证：**执行" 牺牲" 步骤，确保恶意安全性概率为 $1 - 2^{-40}$
4. **存储：**验证后的三元组存储在" 三元组队列" 中

步骤 3-6：消息预处理、本地签名分片计算、协同拒绝采样、签名聚合（详见权利要求书）。

3. 实施例 2：硬件强制安全（TEE 集成）

1. **Enclave 保护：**密钥分片永远不会以明文形式离开 TEE 内存
2. **远程认证：**节点必须提供远程认证报告
3. **密封存储：**使用 TEE 密封密钥将密钥分片持久化到磁盘
4. **侧信道缓解：**利用恒定时间算术和高斯采样

4. 实施例 3：Gas 优化验证

1. **预计算常数**：验证合约中硬编码预计算的 NTT 常数
2. **汇编优化**：关键路径采用内联汇编（Yul）实现，Gas 消耗降低约 30%
3. **批量验证**：支持将多个跨链请求聚合为单个 Merkle 根

（六）技术效果

1. 量子安全性

本发明基于 NTRU 格问题构建安全证明，具体依赖于以下困难问题：

- **NTRU 问题**：给定公钥 $h = g/f \mod q$，求解短向量 (f, g)
- **SIS 问题**（短整数解）：在格中寻找短向量

这些问题被认为在量子计算环境下仍然是困难的。

2. 高性能与经济可行性

本发明实现了格基门限密码学中此前被认为无法实现的技术效果：拒绝采样阶段的**常数轮次通信复杂度**。

表 3: 技术指标对比

指标	本发明	Dilithium 门限	改进幅度
签名长度	∼666 字节	∼2420 字节	缩小 3.6 倍
签名生成	∼15 ms (在线)	∼25 ms	快 40%
通信轮数	**6 轮 (常数)**	$O(n)$ 轮	**可扩展性突破**
Gas 费用 (以太坊)	**∼50,000 Gas**	∼180,000 Gas	**节省 72% 成本**

3. 硬件实现与物理转换

该系统在多个物理计算节点上实现，每个节点包括：

- **硬件处理器**（CPU、FPGA 或 ASIC），配置用于执行加密操作
- **非易失性计算机可读存储器**，存储秘密多项式分片
- **网络接口**，用于节点之间的安全点对点通信

4. 系统健壮性

- 支持 (t, n) 门限结构，典型配置为 $(5, 7)$ 或 $(7, 11)$
- 可容忍多达 $n - t$ 个节点故障或攻击
- 支持动态节点加入和离开
- 支持私钥分片的主动刷新，限制攻击窗口