中国移动专利申请
检索报告

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
检索人	许达、xudayj@chinamobile.com、+86-13521894156
检索日期	2026.01.12
关联项目	（待填写）

与量子计算的关联说明：

本发明面向量子计算网络中多节点协同认证的安全需求。随着分布式量子计算、量子云计算的发展，量子计算节点间的安全通信和身份认证面临双重挑战：(1) 必须抵御量子计算机对传统密码的攻击（Shor 算法可破解 RSA/ECC）；(2) 分布式架构要求密钥管理具备容错性。本发明采用 NIST 标准后量子算法 Falcon 的门限签名方案，可应用于量子计算集群节点认证、量子-经典混合计算环境安全通道建立、分布式量子计算任务可信调度等场景。

一、使用的中文与外文检索关键词

中文检索关键词： (1) 量子计算网络, 节点认证, 抗量子攻击 (2) Falcon 签名, 门限签名, 格密码 (3) 后量子密码学, NTRU 格, 多方安全计算 (4) 分布式高斯采样, 量子-经典混合计算

外文检索关键词： (1) Quantum computing network, node authentication, quantum-resistant (2) Falcon signature, threshold signature, lattice cryptography (3) Post-quantum cryptography, NTRU lattice, MPC signature (4) Distributed Gaussian sampling, quantum-classical hybrid computing

二、相关专利文献

编号	相关度类别	文献信息 (标题/来源/作者/日期)
1	A (基础技术)	**Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU** NIST PQC Round 3 Submission, 2020 Fouque, P.A., et al.
2	A (基础技术)	**Threshold Cryptosystems From Threshold Fully Homomorphic Encryption** CRYPTO 2018 Boneh, D., et al.
3	Y (相关技术)	**Sharing the LUOV: Threshold Post-Quantum Signatures** IMA 2019 Cozzo, D. & Smart, N.P.
4	Y (相关技术)	**Fast Multiparty Threshold ECDSA with Fast Trustless Setup** CCS 2018 Gennaro, R. & Goldfeder, S.

三、分析评述

1. 与文献 1 (Falcon 标准) 的对比分析：文献 1 定义了标准的 Falcon 签名算法，但其设计仅面向单签名者，未涉及多方计算环境下的私钥分片与协作签名。本发明在文献 1 的基础上，创新性地提出了适用于分布式环境的参数生成与采样方法，解决了标准 Falcon 无法直接应用于门限场景的问题。

2. 与文献 2 (门限 FHE) 的对比分析：文献 2 提出了基于全同态加密构造门限密码系统的通用框架。虽然提供了理论上的可行性，但全同态加密由于涉及复杂的密文计算，其计算和通信开销巨大，并不适合对签名速度有实时性要求的场景。相比之下，本发明直接针对 Falcon 算法的格结构设计分布式协议，避免了全同态加密的昂贵开销，实

现了轻量级、低延迟的量子安全签名。

3. 与文献 3 (门限 Dilithium/LUOV) 的对比分析：文献 3 虽然涉及了后量子门限签名，但其针对的是 Dilithium 等其他格算法，或者通信开销较大 (O(n))。本发明针对 Falcon 特有的 NTRU 结构，利用 NTT 线性性和 Beaver 三元组预处理，实现了 O(1) 的常数轮次通信，在效率上显著优于文献 3 的通用方法。

4. 与文献 4 (门限 ECDSA) 的对比分析：文献 4 是目前主流的门限签名方案，但基于椭圆曲线离散对数问题，不具备抗量子攻击能力。本发明填补了量子安全领域的门限签名空白，提供了与现有系统相当的效率但更高的安全性。

四、检索结论

经检索，未发现与本申请全部技术特征相同的现有技术。本申请提出的基于 Falcon 算法的门限签名系统，特别是结合了分布式高斯采样与常数轮次范数验证的方案，具有显著的新颖性和创造性。