软件学报 ISSN 1000-9825, CODEN RUXUEW
2025,36(10):4403−4404 [doi: 10.13328/j.cnki.jos.007395] [CSTR: 32375.14.jos.007395]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

抗量子密码与区块链应用专题前言*

翁 健[1], 祝烈煌[2], 赵运磊[3]

[1](暨南大学 网络空间安全学院, 广东 广州 510632)

[2](北京理工大学 网络空间安全学院, 北京 100081)

[3](复旦大学 计算机科学与工程学院, 上海 201203)

通信作者: 赵运磊, E-mail: ylzhao@fudan.edu.cn

中文引用格式: 翁健, 祝烈煌, 赵运磊. 抗量子密码与区块链应用专题前言. 软件学报, 2025, 36(10): 4403–4404. http://www.jos.org.cn/1000-9825/7395.htm

在当今数字化深度融入工作与生活的背景下, 现代公钥密码构筑起守护日常沟通、金融交易及商业安全的坚固防线. 然而, 量子计算的快速发展将对现役公钥密码技术带来颠覆性影响. 如何在量子时代确保网络空间的长远安全和密码技术的战略迁移, 成为全球密码科技代际跨越发展的重大挑战和大国博弈焦点之一. 2019 年起区块链上升为国家战略, 并纳入“新基建”的重要内容和国家十四五和 2035 远景目标纲要, 成为我国未来发展数字经济不可缺少的信任基础设施, 而抗量子安全是下一代区块链基础设施的内在要求和关键指标. 本专题立足于抗量子密码核心技术, 聚焦抗量子密码的数学基础和安全机理, 算法设计优化与软硬件高效安全实现、区块链应用等领域的高水平创新研究成果. 针对抗量子安全的区块链对抗量子密码在安全、尺寸和吞吐率上提出的特别的要求, 重点关注适配抗量子安全区块链系统的共识机制和密码技术等关键技术, 抗量子安全区块链系统的设计原理、范式、架构与经验方面的重要进展, 并探讨其在相关产业和领域的应用前景.

本专题公开征文, 共收到投稿 24 篇. 论文均通过了形式审查, 内容涉及抗量子密码数学基础和安全机理、抗量子密码算法和协议设计、抗量子密码软硬件优化实现、抗量子区块链系统等. 特约编辑先后邀请了 40 多位专家参与审稿工作, 每篇投稿至少邀请 2 位专家进行评审. 稿件经初审、复审、CBCC 2024 会议宣读和终审这 4 个阶段, 历时 6 个月, 最终有 7 篇论文入选本专题.

《半均匀 LWE 问题的紧致归约》针对抗量子格基密码数学基础问题, 通过优化 Hint-LWE 问题困难性的研究技巧, 将欧氏格/理想格/模格中的标准 LWE 问题保维数地归约到相应的半均匀 LWE 问题. 所得的归约结果的误差高斯参数损失较小, 且理想格上对应问题的归约无需用到非标准的困难性假设. 该成果可以应用到 Kyber、Aigis、AKCN-MLWE 等国内外抗量子算法的安全性分析并提供更紧致的理论支撑.

《SM3-OTS: 基于国密算法 SM3 的紧凑型后量子一次签名方案》设计了一种新的基于国密算法 SM3 的紧凑型一次签名方案 SM3-OTS, 解决 SPHINCS+签名方案中 WOTS+一次签名方案生成的签名值长度较大问题. 利用消息摘要值的二进制信息和十六进制信息分别作为前 32 条哈希链和后 16 条哈希链节点位置的索引, 从而缩短了传统基于哈希函数一次签名方案的密钥长度和签名值长度.

《基于 Kyber 公钥加密的高效认证密钥交换协议》直接以公钥加密方案作为基础组件构造 AKE, 相比于基于密钥封装机制的设计在相同安全级别下显著提升协议运行效率, 同时协议能够满足完美前向安全性.

《具有用户自主链接及验证者条件撤销的格基群签名》提出具有用户自主链接及验证者条件撤销的新型群签名, 平衡了用户隐私与平台管理, 并给出格上抗量子实例化方案. 方案满足无私匿名性、可追溯性和不可诽谤性, 可以更好地适应后量子时代下区块链去中心化的需求.

《基于 FPGA 的格基数字签名算法硬件优化实现》针对后量子数字签名算法 Dilithium 提出了一种新型的纯

* 收稿时间: 2025-01-21; jos 在线出版时间: 2025-01-21

硬件实现方案, 核心工作包括细粒度分段式时序控制逻辑、高吞吐率二维多项式运算阵列、并行双核采样运算模块优化设计等. 论文提出的统一型电路结构可支持不同安全等级下的签名运算过程, 同时具备了高性能和高资源复用率两方面的优势, 对于推进格密码方案的工程化和实用化进程有较好的借鉴意义和参考价值.

《抗量子的高效区块链认证存储方案》提出了一种抗量子的高效区块链认证存储方案 (EQAS), 旨在解决量子计算对现有区块链认证存储技术带来的安全威胁. EQAS 通过引入无状态哈希签名, 采用动态随机森林链和超树结构来解耦数据存储和认证, 提升了效率并增强了抗量子攻击能力, 可为量子时代的区块链认证存储提供有效的解决方案借鉴.

《基于多父链辅助工作量证明共识机制的后量子区块链系统》提出一种算力多元化且应用自主可控后量子签名的抗量子安全区块链系统. 系统采用基于素阶数域的后量子数字签名: Dilithium-prime 算法, 相比于国际标准 Dilithium 算法其底层代数结构更少、长远安全性更稳固, 同时具有相当的计算效率. 采用多父链辅助工作量证明共识机制以及难度动态调整算法, 通过复用算力为系统增加更多的算力来源, 增加安全性并提升算力利用率.

本专题主要面向抗量子密码与区块链等领域的研究人员和工程人员, 反映了我国学者在抗量子密码数学基础和安全机理、算法设计、工程实现以及区块链系统应用领域最新的研究进展. 感谢《软件学报》编委会和区块链专委会对专题工作的指导和帮助, 感谢专题全体评审专家及时、耐心、细致的评审工作, 感谢踊跃投稿的所有作者. 希望本专题能够对抗量子密码与区块链应用相关领域的研究工作有所促进.

翁健(1976－), 男, 博士, 暨南大学教授, 博士生导师, CCF 专业会员, 国务院学位委员会网络空间安全学科评议组成员, 网络安全检测与防护技术国家地方联合工程中心主任, 国家杰出青年科学基金获得者. 获国家技术发明二等奖 1 项、省部级一等奖 2 项. 主要研究领域为密码学与信息安全.

祝烈煌(1976－), 男, 博士, 北京理工大学教授, 博士生导师, CCF 杰出会员, 中国计算机学院区块链专委会, 中国人工智能学会智能信息网络专委会主任, 教育部网络空间安全教指委委员. 入选国家高层次领军人才, 主持国家重点研发计划项目、国家自然科学基金重点等国家级项目 40 余项. 主要研究领域为数据安全与隐私保护, 区块链安全与监管, 人工智能安全.

赵运磊(1974－), 男, 博士, 复旦大学教授, 博士生导师, CCF 专业会员. 主持国家级人才基金项目、重点研发项目、国家自然科学基金项目, 发表论文 100 余篇, 授权和公示中国发明专利 30 余项. 获省部级奖励 2 项. 主要研究领域为密码理论与应用, 抗量子密码算法设计与工程实现.