密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2023, 10(2): 219–245

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

后量子密码迁移趋势下应用于区块链的公钥密码安全*

胡 希[1], 向 宏[1], 丁津泰[2,3], 梁 蓓[3], 夏鲁宁[4], 向 涛[5]

1. 重庆大学 大数据与软件学院, 重庆 401331
2. 清华大学 丘成桐数学科学中心, 北京 100084
3. 北京雁栖湖应用数学研究院 丁津泰实验室, 北京 101408
4. 北京数字认证股份有限公司, 北京 100032
5. 重庆大学 计算机学院, 重庆 401331

通信作者: 向宏, E-mail: xianghong@cqu.edu.cn

摘 要: 自从发现量子算法能够高效求解现今公钥密码依赖的数学困难问题, 能够抵抗量子计算攻击的后量子密码算法成为研究热点, 国际上对后量子密码算法的标准化工作也已相继启动. 现有信息系统为保证自身安全, 势必需要迁移至新一代抗量子公钥加密算法, 迁移过程存在巨大的挑战与机遇. 对迁移过程的研究已在美国、欧盟等国家和地区广泛推动开展、成为趋势. 区块链的安全性依赖于现代密码学, 特别是公钥签名技术, 因此这一迁移也是区块链长效安全的必经之路. 本文介绍了后量子密码迁移策略, 讨论了现有区块链所应用的公钥密码如何向后量子密码进行迁移, 提出下一步研究方向.

关键词: 后量子密码; 密码迁移; 区块链安全

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000595

中文引用格式: 胡希, 向宏, 丁津泰, 梁蓓, 夏鲁宁, 向涛. 后量子密码迁移趋势下应用于区块链的公钥密码安全[J]. 密码学报, 2023, 10(2): 219–245. [DOI: 10.13868/j.cnki.jcr.000595]

英文引用格式: HU X, XIANG H, DING J T, LIANG B, XIA L N, XIANG T. Security of public key cryptography in blockchain under the trend on post-quantum cryptography migration[J]. Journal of Cryptologic Research, 2023, 10(2): 219–245. [DOI: 10.13868/j.cnki.jcr.000595]

Security of Public Key Cryptography in Blockchain under the Trend on Post-quantum Cryptography Migration

HU Xi[1], XIANG Hong[1], DING Jin-Tai[2,3], LIANG Bei[3], XIA Lu-Ning[4], XIANG Tao[5]

1. School of Big Data and Software Engineering, Chongqing University, Chongqing 401331, China
2. Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084, China
3. Ding Lab, Yanqi Lake Beijing Institute of Mathematical Sciences and Applications, Beijing 101408, China
4. Beijing Certificate Authority Co. Ltd., Beijing 100032, China
5. College of Computer Science, Chongqing University, Chongqing 401331, China

Corresponding author: XIANG Hong, E-mail: xianghong@cqu.edu.cn

* 基金项目: 国家重点研发计划 (2021YFB2701300, 2021YFB3100100); 国家自然科学基金 (U20A20176)
Foundation: National Key Research and Development Program of China (2021YFB2701300, 2021YFB3100100); National Natural Science Foundation of China (U20A20176)
收稿日期: 2022-02-07 定稿日期: 2023-01-24

Abstract: Since the proposal of quantum algorithms that can efficiently solve the mathematical hard problems that today's public-key cryptography relies on, research on post-quantum cryptography resisting against quantum computing attacks has begun, and standardization of these algorithms has been in process in the world. In order to ensure the security of existing information systems, it is inevitable to migrate to these new quantum-resistant public key cryptography schemes, which has great challenges and opportunities. Countries and regions such as the United States and the European Union have already initiated research in this migration process, indicating that research on post-quantum cryptography migration has become a trend. The security of blockchain relies on modern cryptography, especially public-key signature technology, so the migration is also necessary to achieve a long-term security of blockchain. This paper first introduces the post-quantum cryptography migration strategies, then proposes the engineering principle of post-quantum cryptography migration in terms of migration goals and migration process. After discussing the existing methodology of transition of public key cryptography used in blockchain according to this principle, some future research directions are proposed.

Key words: post-quantum cryptography; cryptography migration; blockchain security

1 导言

区块链技术起源于中本聪的比特币设计 [1], 后逐渐为加密货币以外的许多不同领域所用, 其中不乏一些关键领域, 如军事、金融 [2], 甚至是网络安全本身 [3]. 在这些关键领域的应用中, 要求区块链系统本身是高度安全的, 而区块链本身具有不可篡改、不可抵赖等特性, 这些特性由区块链架构中的数据层、网络层、共识层、激励层、合约层共同保证 [4]. 其中, 公钥密码算法是保证区块链这些安全特性不可或缺的一部分, 它实现了区块链节点间的互信. 交易中包含的数字签名, 也是交易不可篡改与不可抵赖的一大基础. 此外, 在我国应用较多的联盟链还引入了公钥基础设施 (public key infrastructure, PKI), 提供用户身份认证的功能 [5]. 除公钥密码算法安全外, 区块链安全还包括以下方面: 使用到的 P2P 网络协议、共识协议等协议安全, 如针对 PoW 的 51% 算力攻击; 具体落地的实现安全, 如链上部署的智能合约是否有漏洞等; 应用区块链的交易平台的安全性, 如用户使用上的问题、交易平台内部敏感信息泄露等; 以及以上类型共同影响到的系统安全. 本文聚焦于区块链的公钥密码算法安全, 从公钥密码本身受到的威胁为切入点, 来讨论面向区块链的新一代抗量子公钥密码迁移过程当中会遇到的机遇与挑战.

公钥密码是当今互联网信任链的基础. 通信双方使用 Diffie-Hellman 协议 [6]、RSA [7]、ECDSA [8,9] 等完成密钥协商、加密和数字签名等功能, 是现代公钥基础设施 PKI 乃至整个网络空间的信任基石. 区块链也不例外, 它通过数字签名来保证用户在链上操作的安全性. 然而, Shor 算法 [10] 能够让足够规模的量子计算机完全破解现有基于大数分解和离散对数问题的公钥密码算法, Grover 算法 [11] 则能加速穷举攻击. 随着国际上量子计算机的快速发展, 它对以 DH/RSA/ECC 为代表的第一代公钥密码算法造成的现实威胁也逐渐引起世界各国的高度关注. 为此, 国际学术界、产业界等将注意力投向了能够抵御量子计算机攻击的新型公钥加密算法的研究, 即后量子密码 (post-quantum crytopgraphy, PQC) [12]. Bernstein 等人撰写的专著 [12] 和论文 [13] 以及 Perlner 等人的论文 [14] 对 PQC 算法进行了系统的综述.

现有 PQC 算法可按不同的数学困难问题分类, 如基于编码的算法 [15–17]、基于多变量的算法 [18,19]、基于格的算法、基于安全哈希的算法等. 目前国际上对格密码的综述较多, 如 2006 年的一篇综述 [20] 分析了格密码发展早期阶段提出的一些构造, 如 Ajtai 提出的单向函数 [21]、GGH [22] 和 NTRU [23] 公钥加密机制等. 作为该工作的延续, Peikert [24] 综述了 2006 年至 2016 年格密码领域的主要工作, 包括对短整数解 (short integer solution, SIS) 和容错学习 (learning with errors, LWE) 问题及二者在环代数结构上的变体 (Ring-SIS 和 Ring-LWE) 以及格陷门函数等较新方向的讨论. 近期对格密码的综述则更加细化, 如 Nejatollahi 等人 [25] 对软件实现与硬件实现的综述以及国内何诗洋等人 [26] 专门针对硬件实现的综述, 它们总结了对乘法操作和离散高斯分布取样两个算术操作的优化. 然而需要指出的是, 无论是从第一代公钥密码体制依赖于同一类数学困难问题的教训来讲, 还是从未来互联网、物联网、区块链等各种产业化应

用的角度出发, 今后的 PQC 标准将会基于多种不同数学困难问题的公钥密码算法.

PQC 日趋走向成熟和产业化的标志是对其进行标准化. 美国国家标准技术研究院 (National Institute of Standard and Technology, NIST) 于 2016 年开始率先面向全球征集 PQC 算法, 以便为其后续的标准化工作奠定基础. 目前该工作已经经历了三轮筛选, NIST 已于 2022 年 7 月 5 日公布最终入选标准化的算法以及需留待第四轮进一步讨论的算法 [27]. 作为全球最有影响力的标准化组织之一, NIST 对量子计算带来的威胁和当时已有的 PQC 工作进行了综述 [28]; 在该工作的三轮算法筛选结束后, NIST 针对筛选的结果撰写了分析报告 [29–31]. 在国内, 中国密码学会于 2018 年举办了全国密码算法设计竞赛, 并已公布获奖算法名单. 与 NIST 最终结果类似, 中国密码学会关注的焦点也在格基后量子密码 [32].

表 1 NIST 面向全球征集 PQC 标准化及第四轮入选算法

Table 1 Fourth round candidate and PQC algorithms selected for standardization in NIST PQC project around the world

算法名称	入选类型	算法类型	底层数学问题类型
CRYSTALS-Kyber	入选标准化	PKE/KEM	格
CRYSTALS-Dilithium	入选标准化	数字签名	格
Falcon	入选标准化	数字签名	格
SPHINCS+	入选标准化	数字签名	安全哈希
BIKE	入选第四轮筛选	PKE/KEM	编码
Classic McEliece	入选第四轮筛选	PKE/KEM	编码
HQC	入选第四轮筛选	PKE/KEM	编码
SIKE	入选第四轮筛选	PKE/KEM	超奇异同源

可以看出, 目前对 PQC 算法本身的研究和标准化已有较多前期准备工作, 但现有信息系统要迁移到 PQC 算法, 还需要长期且艰巨的工作. NIST 已经启动了对 PQC 算法迁移的研究项目 [33], 并公开了一份关于 PQC 算法迁移的报告 [34]. 该报告分析了现有信息系统中公钥密码的应用和它们对公钥密码的需求, 提出了 PQC 算法迁移面临的挑战, 分类讨论了识别 PQC 算法迁移对象 (即需要替换的密码算法代码) 的方法. 欧洲电信标准化委员会 (European Telecommunication Standardization Institute, ETSI) 也发布了关于 PQC 算法迁移的报告 [35], 该报告中把迁移过程分为密码算法识别、迁移准备和迁移执行三个阶段, 并分别讨论了每个阶段需要考虑的问题和商业需求.

在算法研究方面, NIST 的 PQC 算法筛选过程即将告一段落, 新的标准制定即将开始. 与此同时, 在面向各种应用领域进行后量子算法的工程技术迁移方面, NIST 正在启动相关项目. 美国政府在 2022 年 1 月 19 日公布的国家安全备忘录中, 也明确要求美国国家安全局负责在 60 天之内审核联邦政府重要信息系统所采用的新型抗量子密码 [36]. 至此, 国际上针对新一代抗量子公钥加密的迁移工作已拉开帷幕.

本文从密码迁移方法论的角度入手, 在第 2 节提出 PQC 迁移的四条工程化原则并根据这些原则对国际上相关研究工作进行综述. 第 3 节以区块链为例, 对现有区块链的 PQC 迁移工作进行介绍. 本文将区块链中需要执行 PQC 算法迁移的部分分为两层, 底层是区块链各节点点对点的安全通信, 综述区块链中常用的两种安全协议 TLS 和 Noise; 上层涉及区块链交易机制中的签名算法, 综述现有新算法设计和迁移现有算法的工作. 第 4 节总结全文, 并提出未来 PQC 迁移的研究方向.

2 后量子密码迁移策略

为保证现有重要信息基础设施 (如 PKI) 在量子计算机大规模应用之后还能继续平稳运行, 需要进行密码算法的迁移工作. 一种直接的初步尝试是把目标信息系统中的密码算法直接替换为 PQC 算法, 实现原型系统并执行各种测试. 然而, 当面向产业界进行算法迁移的时候, 这一算法迁移过程不应仅仅当成是简单的算法替换过程, 而应该视作一次完整的信息安全工程和软件迭代过程, 并仔细执行软件过程中的每

一步. ARM 的报告 [37] 以 ECC 从算法诞生到最后得到广泛支持的过程为例, 指出不应低估这一过程的必要性和所需的工作量及时间. Mosca 等人 [38] 也提出了所谓的 “Mosca 不等式” 来评估 PQC 迁移工作所需要的时间与量子计算机出现的时间竞赛. 由于 PQC 算法家族参数各异, 在面向工程实际应用的迁移过程当中还将面临诸多挑战. 因此制定一套切实可行的迁移策略至关重要.

本节讨论 PQC 算法迁移过程中所涉及的方法论和策略, 为此需给出 PQC 算法迁移需要遵循的原则. 在 NIST 的报告 [34] 中将这一迁移过程称为 “从现有公钥密码算法到能抵抗量子计算机攻击的公钥密码算法的迁移”. ETSI 的报告 [35] 中将 PQC 算法迁移定义为由 “非量子安全” 的状态到 “量子安全” 状态这一变化所需的过程和技术, 其中两个状态分别指 “系统使用经典的、非量子安全的密码算法” 的状态和 “系统中使用的所有密码算法都能抵抗量子计算攻击” 的状态. 本文从安全性、可用性、敏捷性、普适性四个方面给出 PQC 迁移需要满足的原则.

原则 1 (后量子密码算法迁移的目标状态) 若迁移过程完成后, 一个信息系统同时满足如下特征, 则称该系统达到了 PQC 算法迁移的目标:

- 安全性: 能够同时抵抗经典计算攻击和量子计算攻击;
- 可用性: 引入新的密码算法后信息系统仍能正常使用;
- 敏捷性: 系统能够支持未来进一步快速迁移至新的密码算法或安全参数调整;
- 普适性: 系统能够尽量多地适应各种 PQC 标准的要求.

原则 2 (后量子密码迁移) 给定一套无法抵抗量子计算攻击的信息系统, “后量子密码迁移” 是指使该系统同时满足上述安全性、可用性、敏捷性、普适性这一目标状态所执行的开发迭代过程.

2.1 迁移目标

2.1.1 安全性

迁移目标中的安全性要求完成 PQC 迁移的信息系统能够抵抗经典计算攻击和量子计算攻击, 这包括密码算法的安全性以及密码算法在信息系统中使用方式的安全性, 以下分别讨论.

对于密码算法本身的安全性, 首先需要定义何为 “量子安全” 的密码. ETSI 的报告 [35] 中对此给出了粗略的解释, 但为实现密码算法的可证明安全, 需要更加正式的定义. 现有工作中对密码算法 “量子安全” 的定义可从安全假设、安全定义、威胁模型几个方面来考虑, 这也是一般情况下密码学可证明安全考虑的几个要素:

- 安全假设: 虽然量子计算能对某些类型的问题带来显著的加速, 但目前人类仍未找到可以高效求解所有 NP 困难问题的量子算法. 所以对于目前仍未找到能够高效量子求解算法的新的数学困难问题, 则可将其用于公钥密码的构造. 如前所述, 目前 PQC 算法中主要使用的几种困难问题类型分别基于格、编码、多变量、哈希函数、超奇异椭圆曲线同源等.
- 威胁模型: 即对敌手攻击过程中拥有能力的刻画, 在安全证明过程中通常以 “预言机” 的形式定义. 在经典情况下, 我们允许敌手以比特串的形式向预言机输入信息并获得反馈. 然而当敌手拥有量子计算能力时, 为达成目的可能希望以量子叠加态的形式向预言机输入信息. 故在 PQC 背景下建立敌手威胁模型时需要考虑这一点, 允许预言机接收以叠加态形式输入的信息. 对这一点最早的考虑在随机预言机模型 (ROM) 上进行, Boneh 等人 [39] 在 2011 年提出了量子随机预言机模型 (QROM), 并在论文中给出了 ROM 模型下安全性推导到 QROM 模型下安全性的条件. 后来, Song [40] 对此进行了推广, 提出了一个 ROM 下安全推导至 QROM 下安全的模型, 其中包含一系列条件, 作者证明了若 ROM 下的安全归约满足给出的条件, 则该归约的结论在 QROM 下仍然适用. 然而, 从这些工作的结论来看, 存在在 ROM 下可证明安全但在 QROM 下不安全的算法, 在 ROM 下适用的一些证明技术 (如回卷 (rewinding) 方法 [41,42]) 在 QROM 中也需要重新考虑. 在目前将要标准化的 PQC 算法中, 对 QROM 下安全性已有一些考虑. 如 Dilithium 算法, 虽然其底层构造基于使用回卷方法证明安全性的 Fiat-Shamir 变换 [43], 无法直接得到 QROM 下的安全性结论, 但该算法团队在其文档 [44] 中给出了 QROM 模型下安全性的一个粗略描述, 从而展示出目前在标准化进程中对这一问题的考虑.

- 安全定义: 受敌手计算能力增强的影响, 原有的安全定义也需增强. 在经典情况下, 我们常用 IND-CPA、IND-CCA、EUF-CMA 等安全记号来表达密码算法具有某种强度的安全性, 它们通过允许敌手访问不同的预言机来进行区分. NIST 在此次征集 PQC 算法的时候, 就采用了上述安全定义对密钥封装、签名等后量子密码算法做出了要求. 同上面讨论, 在量子环境下需要允许敌手以量子叠加态的形式查询这些预言机, 从而得到这些安全记号的变体 IND-qCPA、IND-qCCA、EUF-qCMA 等. 江浩东等人 [45] 系统地综述了后量子时代算法安全定义、证明技术等可证明安全的要素发生的变化, 梁敏等人 [46] 则进一步从安全定义的角度来讨论, 给出了上述量子安全定义之间的关系. 然而, 对于这些量子安全定义, 学术界仍未达成统一看法 (可参见如 Carstens 等人 [47] 对现有各种量子 IND-qCPA 安全定义的分类讨论), 未来还需进一步研究.

NIST 的 PQC 算法征集进程已经进入正式标准化和第四轮评估阶段, 在此过程中 NIST 和全球密码学界对各候选算法进行了密码分析, 并发现其中一些算法不安全. 例如, Ding 等人构造了对 NIST 第一轮算法 HiMQ-3 和第二轮算法 LUOV 的攻击, 使它们安全性低于 NIST 要求的安全性 [48,49]; 第一轮的 McNie 算法则是在原理上完全破解 [50]. 此外, 最近的一些工作表明, 即使是进入第三轮甚至正式标准化阶段的算法, 安全性也面临威胁. 例如, Ward 构建的攻击能够在可行的时间内完全恢复出 Rainbow 算法安全等级 1 的私钥 [51], Castryck 等人构造的攻击能够在约 1 小时内恢复出 SIKE 算法安全等级 1 的私钥 [52], Perlner 等人构造的攻击能够得到 SPHINCS+ 算法安全等级 5 的一种变体的哈希树, 从而伪造合法签名 [53]. 需要强调的是针对格密码的一系列密码分析工作也让其安全性受到广泛关注, 如 Bernstein 等人提出的 S-unit 攻击 [54]、以色列国防军对对偶格攻击提出的改进 [55] 等; NTRU Prime 团队的综述总结了近期格密码安全性有关的一些工作 [56]. 而这些攻击案例, 也促进了一些构造安全 PQC 算法的方法和模型的提出 [57,58]. 另一个需要关注的问题是, 尽管格密码具有理论上的可证明安全性, 但在实际应用当中, 具体的参数选择如何具有可证明安全性, 依然是一个需要进一步研究的问题. 这也是 NIST 下一步在制标过程中非常关心的问题, 应引起全球后量子公钥密码学界的高度重视. 此外, 密码算法所使用的构件也需要考虑安全性, 如伪随机数生成器是否安全, 以及生成随机数种子使用的熵是否可靠等. 最后, 对于每一种 PQC 类型, 都已经发现了侧信道攻击的方法, 算法设计团队和研究人员也针对他们提出的算法提出了反制措施 [59]. 然而, 对 PQC 的侧信道攻击研究还处于早期阶段, 可能还有很多潜在的攻击方式没有发现, 现有的反制措施很多也只能对抗特定攻击, 缺乏对减小整个 PQC 算法侧信道攻击面的研究 [60].

对密码算法在信息系统中使用方式的安全性分析, 可以通过软件测试方法进行, 包括依赖项、调用关系、运行时控制流的追踪, 以及常见安全缺陷 (如 TLS 中的降级攻击) 的识别. 软件测试自动化是软件测试的研究方向之一, 将自动化技术用于 PQC 迁移的安全性分析和测试, 也是值得研究的问题 [61]. 此外, 形式化验证也是一种分析方式, 已有很多针对现有基于经典算法的安全通信协议的形式化验证工作 [62,63], 而 PQC 迁移后的安全通信协议会根据 PQC 的需求发生变化, 所以需要重新进行形式化验证, 保证 “安全通信协议” 的安全性. 目前已有针对密码算法的安全性进行形式化验证的一些工作, 如表 2 所示. 可以看出, 目前已有专门针对 PQC 形式化验证开发的工具 [64], 但作用还很有限; 而大部分工具都仅针对经典密码算法进行过验证, 是否能用于验证 PQC 尚不明确.

2.1.2 可用性

可用性要求完成迁移的系统性能受影响的程度不能影响到用户的正常使用. 为评估 PQC 算法迁移给信息系统带来的性能影响, 可以从算法性能、硬件性能、网络性能三个方面来考虑 [60].

第一层是算法性能, 主要考虑算法本身和软件实现的性能. 针对具体算法, 研究人员提出了很多优化实现, 这些实现可能依赖于特定硬件平台提供的优化指令集 (如 AVX2) [65]. 而由于底层的数学问题不同、涉及算术操作不同, 各个类型的算法本身会固有一些性能特征, 如多变量算法的签名小、密钥大. 所以, 每种算法类型具有不同的性能特点和适用范围, 如时间敏感型应用对算法性能的要求更高, 物联网设备等资源受限设备要求使用设备计算资源尽量小. NIST 在第三轮筛选结束后的报告中给出了该机构对第三轮算法进行的性能测试结果, 该测试在两种典型的 CPU 架构 x86-64 (含 AVX2 扩展) 和 ARM Cortex-M4 上执行 [31].

第二层是硬件性能, 一些信息系统使用专用硬件来加速密码算法, 这能够提升性能, 但降低了普适性, 也提高了 PQC 迁移的成本. 目前 PQC 算法的专用硬件加速已有一些工作支持, 如在可编程逻辑门阵列

表 2 密码算法安全性形式化验证工具包

Table 2 Cryptography scheme security formal verification toolkits

名称	描述	与 PQC 的关系
AutoLWE [66]	基于 AutoG&P [67] 实现, 可用于验证 LWE 假设的格密码安全性	本身即针对格密码开发
CertiCrypt [68]	基于 Coq 工具, 可用于验证 OAEP、FDH 等密码原语的安全性	只给出了 OAEP 和 FDH 等经典密码算法的验证, 若用于 PQC 则需修改
Coq [69]	通用的数学定理证明工具	并非针对密码学安全证明开发
CryptoVerif [70]	计算模型中的加密协议验证器	只给出了 FDH 经典密码算法的验证, 若用于 PQC 则需修改
EasyCrypt [71]	通过建模安全特性和困难性假设为概率程序, 形式化验证密码结构安全属性	本身并非针对 PQC 安全证明开发, 但已有针对 PQC 的扩展
EasyPQC [64]	EasyCrypt 的扩展, 专用于 PQC, 但支持的形式化验证技术有限	本身即针对 PQC 安全证明开发

(field programmable gate array, FPGA) 上的优化实现 [72], 但在实际迁移时, 对于不同硬件平台的支持应该是考虑硬件性能时需要注意的一个方面.

第三层是网络性能, 即考虑算法集成到信息系统之后表现出的整体性能. 硬件性能和算法性能会对网络性能产生一定影响, 但并不绝对, 整体网络性能会根据算法的使用方式和应用类型变化. 现在的探索工作中主要有以下几个方面的考虑 [60]:

- 时延与能耗. 相比经典算法, 引入 PQC 算法给设备带来额外延迟和能源消耗. 从 NIST 第三轮提交文档 [27] 中的数据来看, 相对于第一代公钥密码 RSA 和 ECC, 新一代的 PQC 或者是密钥、签名、密文等参数尺寸增大, 或者是计算所需时长增加, 迁移到信息系统中之后, 大多拖慢整体性能. 整体而言, 格密码的性能最好, Dilithium 签名算法优化后的实现版本, 计算时长能与 ECDSA 基本持平, 但参数尺寸仍然大于第一代算法. 基于编码的算法从参数尺寸和计算时间来看, 性能都有很大下降. 基于同源的算法参数尺寸小于格密码, 基本与第一代算法持平, 但计算时长极长. 基于多变量的算法在第三轮仅有签名算法入选, 它们有优秀的签名长度, 但公钥尺寸和计算时长表现不尽人意. 最后, 基于零知识证明的算法公私钥长度小, 密钥生成耗时短, 但签名长度和签名/验签耗时却是另一个极端. 综上所述, 与第一代公钥密码相比, 入选第三轮的五类 PQC 算法或多或少都有性能下降. 密钥或签名大小增大, 使网络中传输的数据量增大, 可能触发数据包分片, 需要传输的数据包数量增多. 在丢包率高的不可靠网络中, 数据包数量多意味着需要重传的数据包增多, 延迟进一步增大. 所以, PQC 算法迁移到现有信息系统会使得应用加载时间增加, 导致用户体验下降 [73].
- 会话时间与频率. 会话持续时间长、建立频率低的应用场景受影响较小. 受量子计算影响的公钥密码, 在现有安全通信协议中主要用于会话建立时的握手过程. 而在不同的安全通信协议中, 此过程执行的频率不同: 一般来说, 一些用于 Web 浏览的协议 (如 TLS) 建立会话的频率需求高于另外一些用于建立专用信道的协议 (如 VPN) 建立会话的频率需求. 在设备和算法一定的情况下, 会话建立频率低的安全通信协议受 PQC 带来的额外计算量影响相对较小.
- 仿真度. 需要在仿真网络和真实网络条件下全面测量数据. 在仿真网络下测量性能数据, 能让研究人员运用控制变量法研究每一个网络变量对性能的影响, 但是如果仿真网络的仿真度不够高, 那么测量的数据不够真实, 无法代表真实世界网络的情况; 在真实网络条件下测量数据, 就能让研究人员掌握 PQC 迁移后的系统在真实世界中的表现, 但真实网络条件的复杂性让研究人员无法针对特定网络参数的变化进行研究. 因此, 提高测试系统的仿真度是一个颇具挑战的工程学问题.

所以, 在大部分情况下, 信息系统引入 PQC 算法这件事本身不会带来不可接受的开销, 但可能会引起用户体验一定程度的下降. 而面向未来的网络, 如车联网、物联网、工业互联网等则有可能对 PQC 的性能要求更为苛刻. 总之, 在计算性能、存储性能和通信性能等方面, 现在并没有一种单一的 PQC 算法能够“完美” 迁移到信息系统当中, 提供与现有第一代公钥加密算法一致的性能. 所以, 在 PQC 迁移过程当中需要因地制宜, 选择合适的算法、参数集和使用方法.

2.1.3 敏捷性

NIST 指出现有的信息系统缺乏密码敏捷性 [34]. 简单来说, 密码敏捷性旨在达到 “开发者只需更新密码库版本, 即可完成算法更新” 的理想状态 [60], 也就是说要尽量减少信息系统从一种密码算法迁移到另一种密码算法所需的工作量. 很多重要信息系统的基础设施要求在整个生命周期内是长效安全的, 而它所依赖的密码算法是否长效安全则是无法预测的问题, 近期针对 NIST 第三轮的三个 PQC 算法的攻击 [51−53] 就说明了这一点; 甚至量子计算机出现之后, 不排除人们未来可能能够找到解出该密码算法底层数学困难问题的高效算法. 这就构成了一对矛盾: 诸多重要的信息系统要求长时间维持安全且底层安全框架实现尽量稳定不变, 而密码算法长效安全不可预测则要求上层应用做好经常迁移的准备 [74]. 这种不可预测性使整个系统带有复杂系统的特征, 而敏捷开发的原则又能够与复杂系统的特征联系起来 (如敏捷开发要求减少计划、增加版本发布的特性即是源自于复杂系统的多变特征) [75].

所以, 为化解这一矛盾, 就应充分吸收敏捷性的思想, 尽量简化、灵活化密码算法迁移的流程, 这对密码库的实现与迁移过程的管理都提出了要求. NIST 在 AES 标准全球征集的过程中已经对敏捷性有所考虑, 最后发布的 AES 标准也同时支持 128 位、192 位、256 位三种密钥大小, 使算法标准更加灵活 [76]. 在 2016 年 NIST 开始全球征集 PQC 算法的时候也基于同样的考虑, 把 PQC 算法的安全等级划分为五级, 并要求算法团队根据这五个等级提交不同的参数集 [77]. 现有关于密码敏捷性的研究工作主要针对 PQC 迁移后密码库和信息系统应如何实现提出要求, 如 Ott 等人 [61] 提出的密码敏捷性的七条特征:

- 可迁移: 信息系统的架构和密码使用方式能够支持密码算法的迁移.
- 可测量: 测评机构能给密码敏捷性分级, 并能评定特定信息系统位于哪一级.
- 普适性: 密码敏捷性的需求和标准能够适用于现在使用密码算法的各种软件、设备和基础设施.
- 强制性: 相关标准完善, 能强制密码模块满足相关环境.
- 安全性: 密码敏捷性引入后, 信息系统应仍然能应对各种攻击, 安全性不能下降.
- 可用性: 密码敏捷性引入后, 不应该导致信息系统的性能明显下降从而影响正常使用.
- 智能性: 应实现配套工具, 自动判别应用背景并更换密码算法, 减少人工介入.

RFC7696 [78] 为安全通信协议和应用提供指引, 引导这些应用具有足够的敏捷性, 能从一种密码算法集替换到另一种密码算法集. 该文档指出, 为方便适应新算法或算法套件的插入, 信息系统中密码部分的实现应该是模块化的. 从协议的层面来看, 算法的敏捷性意味着必须支持一种或多种算法或套件标识符, 算法集将随着时间的推移而改变, 并且需要一个算法标识符的注册表. 此外, 开发或部署人员和管理员很难删除或禁用弱安全性算法, 专用硬件和资源有限的设备无法支持新的算法, 这导致系统迁移之后, 仍然使用弱安全性算法, 甚至有严重缺陷的算法.

模块化要求设计人员仔细考虑 API 的设计 [60,61]. API 抽象是需要考虑的问题之一, 设计人员需要设计不同等级的 API 抽象, 让实现人员更好地编写实现, 减少重复工作. 此外, 文档编写人员应该提供友好的密码 API 文档, 并附上正确使用的示例代码, 这有助于用户在使用时正确遵循密码敏捷性实现的需求.

密码敏捷性要求更加复杂的密码模块设计, 这可能给信息系统带来新的攻击面. 为了满足安全性, 需要在软件工程过程的每一步都对密码模块进行安全性测试, 提高测试覆盖率 [60,61]. 而密码敏捷性的高智能性则要求信息系统能够根据自身所在环境的不同, 如监管环境不同、地理位置不同、底层平台不同等, 自动切换需要的密码算法. 这样做有利于减少人工介入, 防止用户不能正确配置算法和参数、算法迁移的困难等问题.

实际上, 密码敏捷性提出的背景与现在广泛所知的软件敏捷性的背景是相似的 [75,79]. 软件敏捷性旨在解决需求的快速变化与繁重的开发流程之间的矛盾, 而密码敏捷性旨在解决密码算法的潜在更换需求与

信息系统对底层稳定性的需求, 以及迁移流程耗时太长之间的矛盾. 密码敏捷性的对象是密码产品以及应用密码产品的系统, 而软件敏捷性的对象则是软件开发迭代过程, 但要求系统满足密码敏捷性的最终目的也是使潜在的密码算法迁移过程具有敏捷性. 要使系统满足密码敏捷性, 迭代过程中的需求分析与设计也是需要考虑的重要方面. 所以, 对迁移过程的研究, 对密码敏捷性的研究也大有裨益.

2.1.4 普适性

随着 NIST 的 PQC 算法筛选工作逐渐进入尾声, PQC 算法即将迎来全球标准化大趋势, 相关的国际标准、国家标准、行业标准将会全方位地规定 PQC 在各种情况下的使用, 而各种标准依据自身定义的网络环境和需求的不同而不同, 呈现出多样化的状态. 与这一多样性相适应的特性就是普适性. 普适性要求信息系统在迁移后尽量满足多种 PQC 标准, 进而能够更多地与网络中其他使用 PQC 标准的设备进行适配.

国际上 PQC 迁移相关标准化工作方面, 美国 NIST 暂时处于领先地位, IETF、ISO、ETSI 等标准化组织也已经开始展开 PQC 迁移的标准化工作. NIST 讨论了算法迁移标准化相关的问题, 包括 NIST 的 FIPS 和 SP 系列标准、ISO/IEC 和 IEEE 的标准、RFC 和协议标准中哪些需要修改 [34]. ISO 于 2020 年 12 月发布了一个标准, 规定了一个通用的包装协议, 为其他协议提供机密性、完整性和认证保护, 且支持向更强安全性的密码算法的平滑迁移 (也包括 PQC 迁移) [80]. RFC6916 [81] 规定了资源公钥基础设施 (resource public key infrastructure, RPKI) 中涉及的各方在迁移到新的密码算法集时需要进行的动作. 然而, 该文档只针对 RPKI 一种应用做出了规定, 整个迁移进程需要花费数年且没有规定更短时间的紧急迁移, 应用范围有限. 可以看出, 现在针对 PQC 算法与 PQC 迁移的标准化工作处于起步阶段, 如何根据系统自身需求满足多样化的 PQC 标准, 是未来 PQC 迁移工作面临的一个挑战.

2.2 迁移过程

信息系统向 PQC 算法的迁移过程, 其核心思想是相关软件系统的适配性, 可以视为软件工程的新一轮迭代过程. 本节从软件工程过程中需求和设计两个方面讨论迁移过程需要满足的原则. 此外, 迁移过程的敏捷性也是值得关注的一个方面, 借鉴软件敏捷开发的方法和框架也可为简化密码算法迁移过程提供思路. 软件敏捷开发最初源于 2001 年提出的敏捷宣言 [79], 现有敏捷开发方法包括极限编程、适应性软件开发、特征驱动开发、Scrum 方法等, 强调减小计划性、增加版本发布频率、加强项目人员之间的交流 [75]. 然而, 敏捷开发具有固定每次迭代时间的特性, 虽然能够有效控制迁移花费的时间, 但同时也可能导致对迁移实现的安全性评估不充分 [82]. 密码库为软件安全的支撑产品, 安全性应放在首要位置, 这又构成一对矛盾, 如何化解这一矛盾是现代密码工程学当中需要解决的问题.

2.2.1 需求分析

使用 PQC 算法的系统, 与使用第一代公钥加密算法 (如 RSA/ECC 等) 的系统, 在需求分析阶段就存在区别. 从算法本身来看, PQC 算法和经典算法的需求有细微的区别 [61]. 二者有共同需求, 但细节可能不同: PQC 算法的计算量大小和密钥、签名的大小普遍大于经典算法, 所以 PQC 算法在信息系统中的计算量需求、存储需求以及网络通信流量需求大于经典算法 [61]. 此外, 根据算法不同, PQC 算法还可能会有经典算法没有的需求, 这些需求可能需要在应用到信息系统时修改现有实现框架. 一些算法中会有状态管理的需求, 如有状态基于哈希的算法 [83]; 算法中会有要求应用额外支持的操作, 如格密码算法中的离散高斯分布取样操作 [25,26]; 一些算法要求应用能够处理解密失败的情况等 [84].

除算法对应用的需求外, 还需要考虑应用对算法的需求. 现有信息系统对密码算法的一些需求可分为两类, 一是对密码算法实现本身的需求, 二是应用业务上的需求 [34]. 信息系统可能会对密钥和签名大小、网络延迟和吞吐量等参数上提出要求, 或要求密码软件是可以升级且密码算法是敏捷的, 这些都是对密码算法实现的需求. 需要保护的数据可能有不同的敏感程度, 这要求不同的算法安全等级; 系统中已有的握手协议和其中的算法协商协议, 以及调用算法的软件所在层次和调用方式 (如通过密码库调用, 通过操作系统调用, 使用第三方服务等) 都可能有需求. 这些需求和前述算法对应用的需求都需要纳入考虑, 所以在执行迁移之前, 要仔细进行需求分析, 选择符合需求的算法、实现和调用方式. 此外, 迁移过程本身还可能带来额外的需求 [60], 如可能要求系统执行迁移时, 用户仍然需要能够访问系统. 系统即便已经完成迁移, 也可能需要与没有完成迁移、仍在使用经典算法的其他系统进行交互, 此时还需要两种系统之间不会产生兼容性问题.

在 PQC 算法迁移需求分析中的一个重要步骤是定位公钥密码在信息系统中的使用模式. 确定有迁移算法的需求之后, 接下来就应定位如何使用它们. 具体来说, 就是要确定应用程序中调用密码算法的位置, 以及使用了需要替换的算法的各种设备和协议. 2022 年 8 月, NIST 在召开的研讨会中提到, NIST 在后量子密码迁移项目中把密码算法定位分类为开发流程、网络流量、操作系统中的密码算法定位, 以及对应的风险分析与评估 [85]. 在上段中曾提到, 信息系统会以密码库、操作系统或者第三方服务等方式调用密码算法, 所以在定位调用之后, 还需要理解调用密码算法的方式, 才能正确分析出应用对密码算法的各种需求. 对这些算法实现本身的理解包括对算法软件实现的理解, 即充分理解现有密码库的数据格式和 API; 以及对硬件实现的理解, 即理解密码算法在硬件上的实现有何种优化, 是否适用于现在待迁移的应用. 根据对这些密码算法使用方式的理解, 就可以确定应用对密码的需求, 从而确定迁移的 PQC 算法和实现, 以及该应用执行算法迁移的优先级 [60].

此外, 如何积极利用自动化技术, 让公钥密码的定位更加智能, 减少人工介入, 也是一个研究方向 [34,60]. 密码算法的定位和识别已有一些研究工作 [86,87]. 但是, 现有识别密码算法的工作, 大多是为解决勒索软件使用密码技术隐藏自身行为的问题展开研究, 而勒索软件有自身的特点以及一般性的执行步骤 [86], 若要将相关方法用于识别不安全的公钥密码算法, 还需要针对需求进行调整.

2.2.2 迁移设计

确认需求之后, 就需要重新设计待迁移信息系统对密码的使用部分. 现有工作中有一种常见的迁移设计, 称作混合模式 [88]. 混合模式的核心是同时使用多种签名算法以克服长效安全的问题, 这一思想在 2002 年就已提出 [89]. IRTF 的一个标准草案 [90] 尝试对混合模式进行标准化. 在 PQC 迁移中, 混合模式的基本思想是, 先不使用 PQC 算法 “完全替换” 现有算法, 而是既保留传统算法, 又加入 PQC 算法, 形式化定义如下 [91].

定义 1 (混合模式) 设有 n 种执行相同功能的密码算法, 记为 $\mathrm{Alg}(K_i, M)$, 其中 $1 \leq i \leq n$ 代表第 i 个算法, K_i 是第 i 个算法使用的密钥, M 是算法处理的消息. 在执行混合模式密码操作时, 先依次执行 $\mathrm{Alg}_1(K_1, M)$ 至 $\mathrm{Alg}_n(K_n, M)$, 再使用算法混合机制进行混合, 得到结果

$$S := \mathrm{Seq}(S_1, S_2, \cdots, S_n),$$

其中 $\mathrm{Seq}(\cdot)$ 是混合机制, S_i 为执行第 i 个算法所得结果.

在反向操作时, 先对混合体 S 执行混合机制的逆函数, 得到 S_1 到 S_n 的序列, 再对序列中每个元素 S_i 执行 $\mathrm{Alg}_i(\cdot)$ 的逆操作 (如解密或验证签名). 这种模式实际上让完整的迁移过程分成了两个阶段, 一是现有系统向混合系统的迁移, 二是混合系统向纯 PQC 系统的迁移 [61].

混合模式能够让整个系统至少保留经典系统提供的安全性, 也就是只要其中有一个算法是安全的, 整个混合机制就仍然是安全的. 此外, 在现有标准没有针对 PQC 迁移过程更新的情况下, 混合模式的使用, 能让完成第一阶段的混合系统仍然符合现有标准对密码算法使用的规定 (如美国 NIST 公布的各类 FIPS).

但是, 使用混合模式也有缺点, 它会大幅增加系统的开销, 降低信息系统的性能 [60]. 混合模式需要在保护系统数据时使用多种密码算法, 而多种密码算法的使用性能低于其中一种密码算法的使用, 且这个总和更多地取决于使用算法中性能最差的, 存在 “短板效应”. 多种密码算法也会增加需要存储、传输的密钥和签名大小, 这样一来就更容易超过应用需求能够容忍的密钥和签名大小.

在使用混合模式进行算法迁移时, 还需要考虑算法混合机制, 也就是如何混合多种不同的密码算法的结果. Crockett 等人 [92] 综述了对称加密、公钥加密、签名和密钥封装机制的混合方法. 现有工作中的混合机制主要有直接连接和密钥派生两种. 直接连接, 顾名思义就是将多种密码算法的结果 (如签名) 连接起来, 可定义为

$$\mathrm{Seq}_{\mathrm{concat}}(S_1, S_2, \cdots, S_n) = S_1 || S_2 || \cdots || S_n,$$

其中 $S_i \,||\, S_j$ 表示 S_i 和 S_j 的连接. 密钥派生主要用于密钥封装机制中, 使用密钥派生函数来处理多种密

钥封装机制得到的共享秘密值, 定义类似于递归, 可写作

$$\mathrm{Seq}_{\mathrm{KDF}}(S_1, S_2, \cdots, S_n) = \mathrm{KDF}(S_n, \mathrm{KDF}(S_{n-1}, \cdots)),$$

其中 KDF(·) 是密钥派生函数.

除混合模式之外, 还可以让系统同时支持多种密码算法, 并允许通信双方协商它们自己可用的算法. 这种协商式协议在以 TLS 为代表的安全通信协议中广泛应用. 可以使用协商式协议, 允许通信双方自行选择如何使用 PQC 算法, 这种机制能够实现后向兼容性. 在设计和实现这种协议时需要预防降级攻击 (downgrade attack) [93], 这种攻击正是利用了这一后向兼容性, 操纵协商参数, 让双方通信时使用不安全的算法, 从而达到攻击的目的. 两种迁移模式各有优缺点, 且可以交叉使用.

3 面向区块链的后量子密码迁移

我国是全球区块链应用的大国. 区块链的安全性, 特别是其底层密码技术的安全对今后区块链健康发展具有非常重要的意义. 因此, 本节以区块链为例, 结合上一节提出的 PQC 算法迁移原则和策略, 讨论现有在区块链上进行 PQC 算法迁移的工作.

区块链是一种复杂的信息系统, 技术架构分为数据层、网络层、共识层、激励层、智能合约层、应用层等多个层次. 此外, 区块链也是现代密码技术一个典型的应用场景, 其技术架构中的各个层次均需密码算法提供安全支持. 此外, 从区块链安全性需求侧来看, 它对密码技术的应用也提出了更高的要求, 国家标准《区块链密码应用技术要求》 [94] 详细讨论了这些需求, 如表 3 所示. 在保证高安全性的同时, 区块链平台还需保证可用性, 所以效率问题也是区块链应用密码技术过程中一个重要的方面, 而在密码应用中, 安全和效率之间往往是相互权衡的关系. 区块链作为一种构建信息系统的技术, 现在已经在各种场景下得到广泛应用, 如金融、知识产权、医疗等领域. 所以这一权衡关系需随着上层应用需求的变化而变化, 这进一步加大了区块链密码应用的复杂度.

表 **3** 区块链密码技术应用需求

Table 3 Application requirements of cryptography in blockchains

名称	描述
交易机密性	防止交易过程中的敏感数据被敌手窃听
交易与账本完整性	确保交易记录与区块链账本数据在全节点网络中的完整性和一致性
不可抵赖性	确保交易完成后, 各交易方无法抵赖已完成的交易
隐私保护	需要保护区块链中用户和交易信息隐私
可监管	保证区块链中交易具有可审计性, 监管部门能够依法依规对区块链平台进行监管

为满足这些安全需求, 区块链中应用了多种密码学技术. 而量子计算对于密码学的威胁主要在于公钥密码, 所以需先讨论公钥密码在区块链中的应用、这些应用对应的区块链安全需求, 以及现有 PQC 算法与这些区块链密码模块之间的相互适配性. 本文把区块链中涉及公钥密码使用的部分分为两类, 一类是区块链中各个节点之间点对点通信所使用的安全通信协议, 另一类是区块链用于保证交易安全的数字签名机制. 这一分类方法来源于区块链技术架构中的分层, 其中前者针对网络层, 其他层中需要加密传输的数据会用到该层的各种安全通信协议进行传输, 而这些安全通信协议中又会大量使用公钥密码来保证传输数据的机密性和完整性; 后者则是针对于数据层, 为保证交易的不可抵赖性, 交易方需对交易进行数字签名. 此外, 还可以交易流程的视角来看这一问题. 在区块链中完成一笔交易的流程大致可分为交易创建、交易验证、上链存储三步: 首先由交易发起方创建交易记录并打包进区块, 这一过程中需由交易发起方进行数字签名, 并加密保护数据的机密性; 然后广播区块至区块链中各参与节点, 各节点使用共识机制同步合法交易, 此时需验证交易发起方的数字签名, 以验证其身份合法性; 最后区块上链, 完成固证操作, 其中区块体中的敏感交易信息需进行加密保护 [94]. 从这一过程可以看出, 在区块链的核心交易过程中, 涉及到的公钥

密码部分就是前面讨论的两个类别.

为了有效保护用户隐私信息, 一些区块链平台尝试使用群签名、环签名、零知识证明 (ZKP) 等密码学技术, 这些技术能够在有效验证区块交易合法性的同时保护用户身份信息不被泄露. 目前已有使用后量子安全假设构建的群、环签名以及 ZKP 方案, 主要基于格上困难问题假设和对称原语假设, 冯瀚文等人 [95] 综述了目前这两类后量子群签名和环签名的一些工作.

3.1 节点间通信涉及的密码算法迁移

传输层安全 (transport layer security, TLS) 是区块链中各节点间通信使用的主要安全通信协议, 目前投入使用的主要是 TLS 1.2 [96] 和 TLS 1.3 [97] 两个版本. 本节主要以该协议为例, 讨论区块链中各节点间通信的算法迁移. 在 TLS 协议中, 公钥算法在握手过程中使用, 握手结束后使用握手过程中分享的对称密钥加密会话数据, 所以本节只讨论 TLS 握手过程中用到的公钥密码算法的迁移. 除 TLS 之外, Noise 协议框架 [98] 也为一些区块链平台所用, 但该协议框架的 PQC 迁移工作目前研究较少.

3.1.1 迁移目标

安全性. 在 TLS 的 PQC 算法迁移研究早期, 有一些工作是建立在其研究团队自行提出的 PQC 算法或协议基础之上的 [99,100]. 这些工作对提出的算法都给出了安全性证明, 但若要在实际的 PQC 迁移过程中使用这些机制, 还需要对它们的安全性进行更多研究. NIST 开始 PQC 全球算法征集活动之后, 特别是第三轮算法筛选完成之后, 对 TLS 的 PQC 算法迁移研究开始聚焦于这些候选算法. 在协议的密钥交换部分, 若要使用 NIST 筛选的算法, 由于 NIST 对算法的功能不包括原有的基于 DH 密钥交换协议, 因此需要将整个密钥交换协议从原来 TLS 中基于 DH 的密钥交换协议换为基于 KEM 的密钥交换协议. 此外, 由于在混合模式下的认证密钥交换 (authenticated key exchange, AKE) 安全性已得到证明 [101], 也有一些工作 AKE 来重新构建 TLS 握手协议, 以减少证书的传输需求 [100,102,103].

可用性. 首先是算法性能. 一些工作在实际执行 TLS 的 PQC 迁移之前, 先对 PQC 算法本身的性能做了一些测量. 不同的工作有不同的算法测量指标, 如各算法的每秒密钥交换次数、每秒签名次数、每秒验证次数 [104]、算法中涉及到的各个数学操作使用的时间. 实验结果显示在格密码算法中取样操作耗时最长 [99]. 此外, 算法的不同实现版本性能也有差异, 例如为预防侧信道攻击实现的常数时间版本和普通的非常数时间版本, 该工作也针对这两种不同的实现版本进行了测量, 并指出常数时间的实现性能略低于非常数时间实现. 测量工具方面, 随着 liboqs 等通用 PQC 密码库的发布, 研究人员也开始尝试使用其中的性能测量工具, 如使用 liboqs 提供的性能测量工具测量算法本身的性能 [105].

硬件性能方面, Chang 等人 [104] 使用 valgrind 工具测评了迁移前后版本 TLS 在嵌入式设备中的内存使用情况, 在该工作中, 总的内存用量约为 1 MB, 运行时则大约需要 128 KB 的内存. Banerjee 等人 [100] 则评估了迁移前后版本 TLS 运行过程中消耗的能量.

早期一些工作先提出针对某个算法的性能改进方案, 实现后再测量改进方案的性能, 并尝试在 TLS 中实现提出的改进方案. 针对取样操作耗时长的问题, Gao 等人 [106] 提出了更快的高斯取样器方案, 应用到 PQC 算法中并进行测量. 该团队还提出了基于 RLWE 问题的口令认证密钥交换方案的优化实现 [101]. Bernstein 等人 [107] 则通过改进求逆操作的方法, 提高了密钥生成性能.

第三层是网络性能, 这也是现有 TLS 算法迁移工作性能测量的主要方面. 除算法本身之外, 现有工作表明, 网络协议中的各种参数也会对性能造成影响, 尤其是在 PQC 算法迁移后密钥和签名大小明显增大的情况下. Paquin 等人 [108] 调整全局性的网络基础参数并进行测量, 结果显示在高速可靠 (无丢包) 的网络中, 影响性能的主要因素是算法运行时间, 而在不可靠 (丢包率较高) 的网络中, 影响性能的主要因素则是密钥大小; 该工作还尝试调整链路层参数最大传输单元 (maximum transport unit, MTU) 大小并测量该参数造成的影响, 结果表明将 MTU 调大可以改善性能. 但是, 该工作也指出, 调整 MTU 大小会导致兼容性问题, 不适合用在互联网中. 在传输层, TLS 协议扩展配置的使用会造成影响 [105]. Sikeridis 等人 [109] 则研究了修改 TCP 窗口大小对 PQC 迁移后性能的影响, 指出增大 TCP 窗口大小能够明显改善迁移后协议的性能, 但修改参数可能会导致网络拥塞, 这一行为存在争议. 所以, 对网络协议栈中参数的修改需要根据协议标准仔细考虑, 不能随意行事.

网络性能的测量指标和算法性能的测量指标不同. 在现有工作中常见的测量指标有握手时间 (多次平均、密度函数等统计量)、证书传输过程中传输的数据量、握手过程中传输的数据量、证书传输的时间、每

秒能够执行的并行连接数、服务器性能 [99,105] 等. Sikeridis 等人的实验 [105] 表明签名操作的速度对服务器性能的影响大于证书链大小造成的影响, 且客户端距离较近时性能较好. 该工作部署了一个中心服务器, 以及四个与服务器之间跳转数不同的客户端, 以并行连接数作为自变量, 测量每秒 TLS 握手事务数以及握手失败率.

此外, 还有部分工作考虑了网络规模和复杂度对性能的影响, 包括从局域网到全球范围互联网的性能测量 [99,105]. 在全球范围内进行的性能测量, 分两次实验: 一是在几个不同距离的地区执行 1000 次握手并测量平均时间, 二是将 3000 次握手平均分布到 24 小时中执行, 以评估互联网环境的不确定性对性能带来的影响.

普适性. 目前使用较多的 TLS 标准有 1.2 和 1.3 两个版本, 本身就具有多样性. 而 IETF 自 2016 年起提出了多个在 TLS 等安全通信协议中执行 PQC 算法迁移的标准草案. 按时间顺序来看, 先是分别规定了用于 TLS 1.2 和 TLS 1.3 版本的混合模式密码套件 [110,111]; 在 TLS 消息中添加扩展, 支持使用混合模式的密钥交换, 交换额外的共享秘密值 [112]; 单独针对基于超奇异同源的 SIDH 密钥交换协议规定了混合模式的 TLS 协议, 其中传统算法使用 ECDHE [113]; 针对 TLS 1.2 规定了混合模式下使用 KEM 进行密钥交换的方法 [110]; 提出 TLS 1.3 中使用混合密钥交换的一些设计要点 [114]. 此外, PQC 算法在 TLS 使用的网络基础设施中的应用, 以及现有迁移工作暴露出来的问题, 也会影响到未来 TLS 协议的后量子密码标准.

TLS 中涉及到的网络基础设施, 主要是 PKI. PKI 用于签发证书, 而 TLS 握手过程中需要使用证书对服务器进行认证. 证书链包含数据的大小会影响到 TLS 握手过程传输数据的大小, 进而影响 TLS 握手的性能. 签名算法的公钥和签名需要放置在证书中进行传输, 所以公钥和签名大小会直接影响到证书的大小. 证书规模过大, 传输过程中就会需要更多的数据包, 拉长握手时间 [105].

为解决该问题, 除仔细选择算法, 尽量减小证书大小之外, 可采用 “混合证书” 的方式, 在证书链的不同位置放置不同算法的密钥或签名, 以充分利用不同算法的优点 [105], 该工作使用 Dilithium 和 Falcon 两种 PQC 签名算法进行了混合证书的实验, 结果表明该方法能够显著降低握手时间. Paul 等人 [115] 则提出在根证书中使用基于哈希的算法, 其他证书中使用格密码算法的混合证书链, 并基于 wolfSSL 库进行了实验. 作者认为根证书的更新间隔长, 需要尽快开始考虑 PQC 迁移工作, 保证在下次根证书更新时能够执行迁移, 并基于此提出了 “两步走” 迁移策略: 首先迁移根证书使用的签名到哈希签名, 然后迁移其他证书到格签名. 混合证书方法需要验证证书的一方同时支持混合证书中的每一种算法, 签发证书的 PKI 也需要修改. “两步走” 策略旨在平滑迁移整个证书链, 但第一步迁移根证书时, 使用其他证书的系统需要更新对哈希签名验证的支持, 工作量仍然较大.

此外, 有一些针对 TLS 性能进行更新的标准草案也可以用于减少证书大小, 如针对中间证书的缓存 [116,117]. “小型 TLS 1.3” 草案 [116] 提出模板化 TLS 握手配置, 通信双方可以预先定义 TLS 握手配置的 “模板”, 握手过程中只传输这些模板的标识符, 从而减少所需传输的信息. 这种 “模板化” 的过程实际上是减少 TLS 配置的 “自由程度”, 即减少可供协商的 TLS 配置的集合, 这一思想与 Noise 协议框架相似. 证书方面, 该标准草案提出使用预先定义并由通信双方共同维护的词典来免除证书传输, 但如何更新维护这一词典是一个问题. 此外, 上述标准仍处于草案阶段, 以后可能会有更改修订, 需等待至标准稳定后方可进行应用评估. Kampanakis 等人 [118] 提出类似于现有存储器高速缓存的缓存机制来解决更新问题. 作者定义了两个缓存列表, 分别用于缓存中间证书和使用证书的对等方, 同时提出缓存清空和缓存更新算法. RFC8879 [119] 提出了证书压缩的方法, 即在握手过程中使用标准的压缩算法减小传输证书的大小. 在 ClientHello 和 ServerHello 消息中, 双方通过 compress_certificate 扩展协商使用的压缩算法, 并用 CompressedCertificate 消息取代原 Certificate 消息传输压缩后的证书. 证书压缩机制在 PQC 迁移工作中目前未见应用.

可以看出, 由于 PQC 算法嵌入对证书规模和性能造成的影响, 人们提出了模板化 TLS 握手、证书缓存、证书压缩等多种解决方案. 对这些解决方案的研究和标准化会让未来的 TLS 等安全通信协议标准更加多样化, 这样一来就更加需要满足普适性, 以满足系统在不同情况下的使用需求.

3.1.2 迁移过程

需求分析. 这里主要讨论 TLS 中公钥密码使用的定位. 以 TLS 1.3 为例, 握手过程如图 1 所示. 从图中可以看出, 在 TLS 1.3 中, 公钥密码在握手过程中的算法协商、密钥交换和证书链中使用. 在算法协商过程, 通信双方会协商支持的公钥加密算法等内容, 涉及到相关的公钥密码算法标识符和密码套件. 在密钥交换过程, 通信双方会使用密钥交换协议交换生成密钥的共享秘密值, 目前使用的一般是无法抵抗量子攻击的 DH 密钥交换协议. 在证书链中, 会存储签名算法的标识符、公钥和签名, 根据所使用的算法不同而不同; 而进行签名和验证签名的算法, 也是无法抵抗量子攻击的, 需要进行迁移.

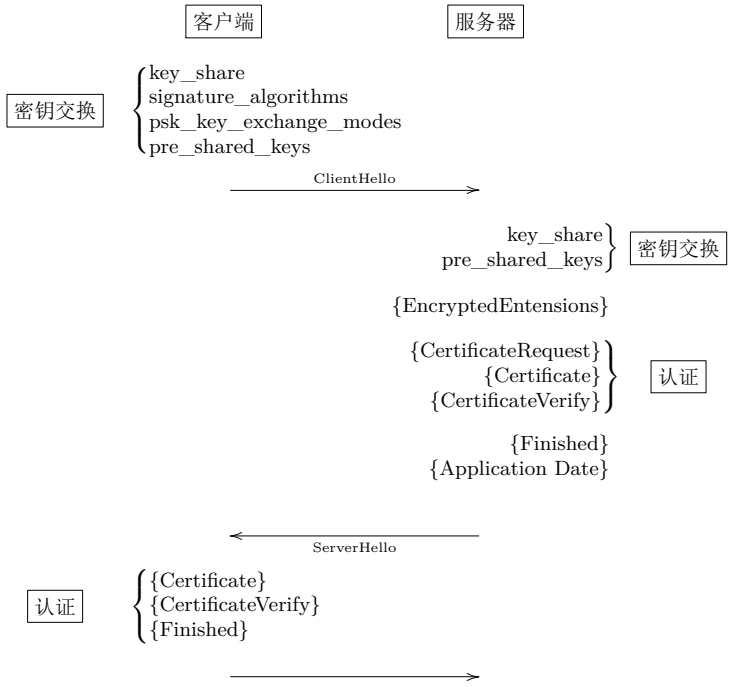


图 1 TLS 1.3 协议握手过程

Figure 1 TLS 1.3 handshake process

密钥交换方面, 客户端和服务器分别使用 ClientHello 和 ServerHello 消息中的 key_share 字段交换生成共享秘密值所需的 DH 密钥交换材料, 若有预共享密钥, 则使用 pre_shared_key 字段交换. 签名方面, 证书中包含签名以及用于验证签名的公钥的数据结构. 现有信息系统对证书的使用形成 “根证书-中间证书-终端实体证书” 的层次结构, 由受信任的根证书开始自上而下签发证书, 构成信任链. 客户端在 ClientHello 消息中放置支持的签名算法包, 服务器在 ServerHello 消息的 Certificate 字段中放置对应算法的证书链, 供客户端验证. 若需要相互认证, 则服务器此时会一并发送 CertificateRequest 消息请求客户端证书. Paul 等人 [115] 研究了需要相互认证的环境下引入 PQC 算法带来的影响.

此外, 在 Web 应用中还常使用签名证书时间戳 (signed certificate timestamps, SCT) 和在线证书状态协议 (online certificate status protocol, OCSP) 等扩展功能, 引入额外的签名传输需求. SCT [120] 用于实现 “证书透明”, 要求维护一个可公开审计的证书签发日志, 需要在传输的证书中加入 SCT 签名. 最近部分浏览器增加了在证书中传输 SCT 签名的需求 [118]. OCSP [121] 用于替代证书撤销列表, 供用户确定证书当前的状态 (是否已经撤销), 需要在 TLS 握手过程中传输一个额外的签名.

迁移和测试的 PQC 算法种类和 PQC 算法数量随时间和现有工作的不同而不同. 在 NIST 开始 PQC 标准化进程之前, 会有一些先提出密码机制再在 TLS 实现中的工作; 而 NIST 的 PQC 算法筛选的不断浓缩使 PQC 迁移工作开始聚焦于第三轮的算法. 算法数量则受通用 PQC 密码库引入的影响. 在通用 PQC 密码库 (如 liboqs [73]) 发布之前, PQC 迁移工作一般只使用单个算法进行迁移和测试, 而 PQC

通用密码库的引入, 为对 NIST 的 PQC 标准化进程中算法的全面测试打下了基础.

现有工作使用的 TLS 实现也不尽相同. OpenSSL 库在现有工作中最常使用, 但也有基于不同考虑使用其他 TLS 库 (如 mbedTLS、wolfSSL、Rustls) 的工作 [102,104,106,118]. mbedTLS 和 wolfSSL 一类轻量级 TLS 库体量小于 OpenSSL, 因此在针对嵌入式系统等小容量设备的现有工作中有一定的应用. 此外, 算法实现硬件优化方面, Sikeridis 等人认为在 TLS 迁移时不考虑算法的硬件优化实现能够让结果更具有普适性 [105].

从算法类型来看, TLS 握手中涉及到签名算法和密钥交换协议. 现有的签名算法包括 RSA 和 ECDSA 等, 都不能抵抗量子攻击, 需要迁移至 PQC 签名算法. 现有的密钥交换协议是 DH 密钥交换协议, 也不能抵抗量子攻击, 需要进行迁移. 对密钥交换协议的迁移, 现有工作中有三种选择方向, 一是以能抵抗量子攻击的数学困难问题为基础的类 DH 密钥交换协议, 如 Bos 等人提出一种基于 Ring-LWE 问题的类 DH 密钥交换协议, 证明了提出的类 DH 密钥交换协议的安全性, 提出该协议集成到 TLS 中的方法, 并使用 TLS 标准安全模型证明该协议集成之后的安全性 [99]. 二是基于身份的密钥交换协议, 如 Banerjee 等人以格上困难问题为数学基础, 提出一种基于身份的密钥交换协议, 减少证书传输大小, 显著增加 TLS 的效率 [100]. 三是密钥封装机制, 在 NIST 的 PQC 标准化进程逐步推进的背景下, 对密钥交换协议的 PQC 迁移研究, 重心逐渐偏向 PQC 密钥封装机制.

还有研究工作只考虑密钥交换的迁移, 认为认证没有前向安全的问题, 攻击者不能伪造已经传输完毕的消息; 而密钥交换则有前向安全的问题, 攻击者可以把密文存储起来, 等有大规模量子计算机之后, 再破解现在使用的密钥交换算法, 得到对称密钥并解密 [92]. 其他工作则全面考虑了密钥交换和签名迁移后对 TLS 协议运行的影响.

迁移设计. PQC 迁移过程使用的策略包括混合模式和算法协商. TLS 协议的握手过程已经带有算法协商, 所以本节重点讨论现有工作对混合模式的考虑. TLS 协议中使用混合模式需要考虑的算法混合机制包括四个方面 [92]:

- 算法协商方式. 在执行算法迁移时, 需要确定 PQC 算法与传统算法是分开协商, 还是一起协商. TLS 只支持协商一次算法套件, 若要分开协商, 则需要修改协议的逻辑. 这样做的缺点是, 若使用混合模式的节点要和只使用传统协议的节点通信, 会产生向后兼容问题, 不能满足互操作性. 如果合并协商, 则不需要修改协议逻辑, 定义 “传统算法 + PQC 算法” 的组合算法标识符即可, 但这样做需要针对每种算法组合定义大量的算法标识符.
- 混合算法数量. 为减少额外开销, 现有工作一般混合一个传统算法和一个 PQC 算法, 一共执行两个算法. 但有些标准草案更加灵活, 允许混合两个以上的算法 [110,111].
- 传递算法参数. 混合模式的使用中还需要考虑如何将多个算法的参数放在协议消息中传输, 如密钥交换时额外的 KEM 公钥和密文的传输. TLS 中的 ClientHello 消息和 ServerHello 消息支持扩展字段, 可以在这些扩展字段中传输额外的参数. 此外, 也可以直接把多个算法的参数连接起来, 放在一个字段中传输, 但要注意放入的字段是否有大小限制.
- 组合算法参数. 例如多种密钥交换协议所得到的共享秘密值要如何组合. Crockett 等人对算法参数的组合进行了综述 [92]. Giacon 等人 [122] 提出了几种 KEM 的组合方式, 并在传统敌手模型下给出了安全性证明, 但证明所做的假设 (如随机预言机) 没有考虑到具有量子计算能力的敌手. 这一点在之后的工作中得以改进, Bindel 等人 [103] 使用新的量子敌手模型对文章中提出的 KEM 组合方式进行了安全性证明.

并不是所有尝试对 TLS 进行算法迁移的工作都使用了混合模式, 有一些工作直接迁移到纯 PQC 的 TLS 协议 [105,108].

3.2 Noise 协议涉及的密码算法迁移

部分区块链平台使用 Noise 协议框架 [98] 作为节点间的安全通信协议, 如 Diem 区块链 [123] 使用 Noise IK 协议. Noise 协议框架定义了若干消息和消息的组合规则, 用户可根据自己的需要, 按照规则自由组合消息, 形成自己的 Noise 协议; 官方也提供了一些预设的协议集 (如前面提到的 Noise IK 协议). 对于某一应用来说, 使用协议集中何种协议和参数, 在此协议框架中假设为已提前商讨完毕, 故与 TLS 不同,

Noise 协议框架中的协议在握手时不需协商算法等参数. 下以 Noise IK 协议为例说明其握手过程:

Noise IK 协议假设客户端 (图 2 中的 A) 在执行握手之前已知服务器 (图 2 中的 B) 的长期密钥. 握手过程分为两条消息: 第一条由 A 发送给 B, 包含 A 的短期密钥和长期密钥, 且 A 使用 DH 函数计算 A 短期密钥和 B 长期密钥对应的共享秘密值, 以及 A 和 B 短期密钥对应的共享秘密值, B 在收到第一条消息后计算这两个值; 然后由 B 向 A 发送第二条消息, 包括 B 的短期密钥, 且 B 使用 DH 计算 A 和 B 短期密钥对应的共享秘密值, 以及 A 长期密钥和 B 短期密钥对应的共享秘密值, A 在收到第二条消息后计算这两个值.

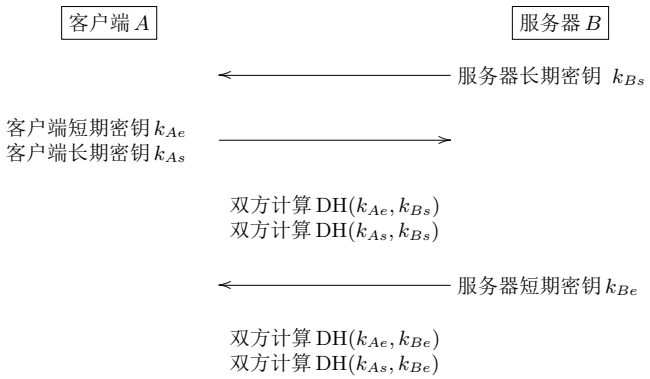


图 2 Noise IK 协议握手过程

Figure 2 Noise IK protocol handshake process

Noise 协议框架本身的密钥交换协议是 DH 密钥交换协议, 而 NIST 正在准备的 PQC 标准化进程中用于密钥交换的算法都是 KEM. 为解决这个问题, 有一个标准草案 [124] 尝试将 KEM 加入 Noise 协议框架中, 并定义同时使用 KEM 和 DH 的混合密钥交换机制. 此外, WireGuard VPN [125] 也将 Noise 协议框架作为底层的安全通信协议, 现在对 Noise 协议框架的 PQC 迁移工作不多, 可以从 WireGuard 的 PQC 迁移工作中看到对 Noise 的 PQC 迁移的考虑. Kniep 等人 [126] 提出了三种对 Noise IK 协议的扩展, 其中第一种与文献 [124] 中定义的一致, 第二种实现身份隐藏, 第三种防御主动攻击. 该工作将提出的三种协议扩展在 WireGuard 中实现, 结果显示在 NIST 第三轮算法中, Kyber 密钥交换机制在 Noise 协议框架和 WireGuard VPN 应用中性能较优. Hülsing 等人 [127] 提出在 WireGuard 的握手过程中, 使用 CCA 安全的 KEM 交换长期密钥, 同时使用稍弱的 CPA 安全的 KEM 交换短期密钥, 能够在保证安全性和匿名性的同时, 尽量减小握手时传输数据的大小, 防止数据包分片.

3.3 区块链交易涉及的密码算法迁移

区块链上层交易中对密码学的应用主要包含共识算法和交易机制中的签名, 本文重点讨论对上层交易签名算法的迁移工作.

3.3.1 迁移目标

Gao 等人 [128] 从区块链这一具体领域入手, 给出了区块链完成 PQC 迁移过程之后要达到的迁移目标, 要求后量子区块链 (post-quantum blockchain, PQB) 结合区块链技术和 PQC 技术, 既有区块链技术的优点, 又能够抗量子攻击; 除此之外, PQB 在传统攻击下也需要保证安全; PQB 交易时使用的签名要有可追溯性.

可用性方面, Holcomb 等人 [129] 对区块链交易使用混合模式签名的性能做了全面分析. 该文指出, 延迟增加主要是因为需要进行混合算法的两次签名和验证, 而不是 PQC 算法引入本身, 且密钥材料的大小对于性能有明显影响 (需要哈希和内存管理). 通过检查 CPU 在各个操作上花费的时间, 发现额外的时间在于 PQC 签名/验证以及哈希上. 哈希计算同样是性能瓶颈, 该文作者希望未来可在区块链中应用哈希并行计算的方案. 所以, 作者认为, 算法本身执行所花费的 CPU 周期并不能说明它在区块链中使用的性能. Fernández-Caramès 等人 [130] 提出用于区块链的 PQC 算法的几个理想特性: 密钥长度小、签名长度

小、执行速度快、计算复杂度低、能源消耗低. 这里需要注意的是, 执行速度快, 计算复杂度不一定低. 某种算法可能只在特定硬件加速的情况下执行速度快, 而由于计算复杂度高, 在其他硬件上执行较慢.

普适性和敏捷性方面, Holcomb 等人 [129] 指出, 机构在执行区块链算法迁移时, 应能够直接在现有链上迁移, 而不应该是需要开一个新链; 现有执行经典算法的客户端应该能与支持混合模式的客户端共存. 此外, 在新的机制中, 替换算法应该更方便, 以应对 NIST 未来 PQC 标准化过程中的快速变化.

3.3.2 迁移过程

需求分析. 区块链上层交易 PQC 迁移过程需要满足的需求, 可以从量子计算对区块链的影响这个方面来讨论. 除节点间通信外, 量子计算对区块链的影响主要可从共识算法和交易机制两个方面来考虑.

对于共识, 刘懿中等人 [131] 对现有区块链共识机制进行了综述, 从不同的角度给出了共识算法的分类. 与密码算法的安全性方法类似, 对共识算法的安全性人们也通过建模方法描述敌手的能力, 通常分为腐化模型 (描述敌手攻击单个节点的能力) 和敌手模型 (描述敌手算力在全网算力中的占比) 两种, 前者主要形式是敌手攻击所需的时间, 后者主要形式是敌手的节点数量, 将敌手加入量子计算能力在这里意义不大. 以现有区块链中使用的主流共识算法为例, 讨论量子计算对这些算法的影响. 对于公链, 以 PoW 共识算法为例, 其底层实际上是要求矿工寻找哈希函数原像的问题, 而人们认为现在主流使用的 SHA2 [132]、SHA3 [133] 等哈希函数的安全性已经足够抵抗 Grover 算法的攻击. 其他针对 PoW 的攻击主要包括日蚀攻击、双花攻击、自私挖矿等, 均为针对网络层的攻击, 敌手在这些攻击中通过巧妙的行为得到网络中节点的控制权, 故为敌手增加量子计算能力不会对这些攻击的效果造成显著影响. 联盟链方面以主流的拜占庭容错协议 [134] 为例讨论. Fischer 等人 [135] 在 1985 年证明了异步网络环境中存在恶意节点的情况下不存在安全的确定性共识算法, 后来的拜占庭协议引入随机性来克服这一困难, 其中一种方式是引入门限签名等密码技术. 而在联盟链中应用较多的授权共识 (permissioned consensus) 机制要求节点在参与共识算法之前需要先通过 PKI 完成身份认证, 对于 PKI 的 PQC 迁移在前面已讨论过. 此外, 有一些共识算法 (如 Ouroboros [136]) 为保证在敌手存在的情况下能够产生可信任的随机数, 尝试使用安全多方计算等方法来产生随机数. 故这些密码技术的安全性成为现有联盟链使用的共识协议安全性的一部分. 综上所述, 区块链共识机制安全与后量子安全的关系目前仍然体现在共识机制中使用的密码原语和协议的安全:

- 对于底层哈希的安全, 人们认为现有哈希算法仍能经受量子计算的攻击, 暂不需要考虑迁移.
- 对于 PKI 的安全, 现在已有很多针对 PKI 迁移的工作, 见 3.1 节的讨论.
- 对于安全多方计算等密码技术的安全, 虽然现在已有一些尝试将这些技术与 PQC 结合的方案 (如 Agarwal 等人基于 LWE 的方案 [137]), 但对于如何对它们进行后量子迁移, 进而对共识算法进行后量子迁移的研究仍不充分.

总体而言, 目前国内外学术界尚未发现量子计算会对区块链共识协议产生实质性威胁. 因此, 后量子时代区块链的安全应将面向现代公钥密码技术的平滑迁移作为重点. 综上所述, 本文暂不将 PQC 迁移对共识协议的影响纳入系统性讨论范围, 而是重点讨论区块链交易机制中涉及的签名技术的迁移.

交易机制方面的问题更加严重. 量子攻击者能使用 Shor 算法, 从公钥恢复出私钥. 这一点会严重影响区块链交易的安全性 [138]: 区块链交易中, 资产与地址绑定, 而地址与用户的公钥绑定. 若与地址绑定的公钥不再安全, 则该地址下的资产也就不再安全. 地址会在交易时公开, 所以如果重用交易的地址, 则之后的交易都不安全. 在交易记录方面, 如果交易已经处理上链, 则量子计算机也无法实现双花; 如果交易还未处理, 攻击者根据公钥计算出私钥后, 用私钥广播一笔将资产转账到自己地址的交易, 若攻击者能让他发起的交易更早上链, 则攻击能够成功.

除此之外, 在迁移过程中, 要密切注意量子计算的发展. 量子计算的瓶颈在于错误校正, 错误校正码仍需要大量传统计算 [139]. 然而, 已有协议尝试将该过程换为量子计算, 这样会极大加速错误校正操作. 此外, 在量子计算机上对 Shor 算法和 Grover 算法本身的优化, 以及量子计算机并行计算的发展也需要关注.

迁移设计. 除混合模式的使用之外, 现有对 PQC 迁移过程的设计工作还可分为两类, 一类是设计新的抗量子区块链, 一类是让现有的区块链抗量子.

ABC 链 [140,141] 基于 Ding 设计的 Rainbow 算法, 该算法是 NIST 第三轮后量子主要候选三个数字

签名之一. 该链的 PoW 基于多变量的 NP-hard 问题, 所以也有很好的抗量子能力. 该链应用了全新的设计理念来处理公钥大的问题从而达到了很高的效率, 已经于 2018 年开始运行. 在 NIST 开始 PQC 的标准化进程前, 研究人员常常针对区块链的特性, 先提出新的 PQC 算法, 再将算法应用在区块链中. 这些算法主要基于多变量、格和哈希. Gao 等人 [128] 设计了一种基于格的签名机制, 安全性可归约到 SIS 问题. Yin 等人 [142] 设计了一种基于格 Bonsai 树的算法. Torres 等人 [143] 设计了一种基于格的一次性可连接环签名, 并应用于门罗币使用的 RingCT 协议中. Esgin 等人 [144] 对 RingCT 协议中的环签名进行了改进, 提出了该协议基于格的版本, 对签名算法中使用的采样方法进行了改进, 并增加了可审计性. 哈希算法方面, Chalkias 等人 [145] 提出一种基于哈希的签名, 能运用区块链链式结构的特点减少开销, 并实现了算法. 该算法具有可扩展性, 允许模块化, 但签名长度随签名次数线性增加. Shahid 等人 [146] 提出基于哈希的一次性签名, 密钥短, 签名速度较快.

也有一些工作专注于设计能抗量子攻击的共识算法和交易机制本身. Chen 等人 [147] 修改 PoW 共识需要解的问题, 要求矿工解基于多变量的问题. 该工作还在交易机制中引入两种方法解决密钥和签名过大的问题, 一是引入身份加密算法 ID-Rainbow [148], 大幅减小密钥大小; 二是引入星际文件系统 (IPFS), 将实际较大的密钥和签名存储在 IPFS 中, 链上只存储哈希. Zhang 等人 [149] 同样引入了 IPFS, 但只讨论了 qTESLA 签名算法在交易签名中的应用, 而该签名算法未能进入 NIST 标准化工作第三轮. 此外, 还有针对特定应用的迁移工作, 如工业敏感数据共享、电子投票等领域 [150,151].

除设计新的能抗量子的区块链外, 也有针对现有区块链平台进行 PQC 迁移的工作. Bitcoin Post-Quantum [152] 是比特币的分支, 使用基于哈希的 PQC 签名算法保护交易安全, 并使用量子安全的零知识证明机制保护用户隐私. Semmouni 等人 [153] 则将 TESLA# 算法应用到比特币中.

以太坊方面, Ethereum 3.0 提出使用抗量子的组件, 如 zk-STARK 来保护隐私 [154]. Shen 等人 [155] 将多变量公钥密码 Rainbow 应用于以太坊中, 并与原有的 ECDSA 算法进行密钥和签名大小, 以及性能上的比较. 该文指出, Rainbow 的密钥长度远大于 ECDSA 的长度, 而使用变体 CycleRainbow 能够减小密钥长度. 性能方面, 引入 Rainbow 后, 签名和验证时间明显增加, 但不影响正常功能的使用. Allende 等人 [156] 在基于以太坊客户端 Hyperledger Besu 实现的 LACChain 中进行了迁移, 使用量子熵生成密钥, 并同时考虑了底层节点间通信和上层交易签名的 PQC 迁移.

以上均是对公链的讨论, 实际上也有工作尝试进行联盟链上的算法迁移. Holcomb 等人 [129] 尝试使用 liboqs 密码库把 NIST 算法征集第三轮中的 PQC 算法和 qTESLA 应用于 Fabric 中, 对混合模式和经典模式的性能进行比较, 并分析了影响混合模式性能的主要因素.

其他区块链平台中, Abelian 使用格密码来使平台能抵抗量子攻击 [157], 而 Corda 则在密码套件中支持 SPHINCS+ 算法 [158].

3.4 讨论

面向区块链的后量子密码迁移不仅仅是简单的算法替换过程, 而是一个颇具挑战的工程学问题, 纵向涉及区块链架构的各个层次, 横向涉及软件工程的各个流程. 根据上面对后量子密码算法本身的讨论、对区块链使用的通信协议和交易签名的迁移工作讨论、对区块链后量子密码迁移原则的讨论, 我们可以得出区块链上的后量子密码迁移具有以下四个挑战:

密码算法敏捷性. 依据 Ott 等人的定义 [61], “密码算法敏捷性” 一词的内涵已经覆盖我们研究 PQC 算法涉及的很多考虑要素, 如安全性、可用性、可配置性等. 国际主流 PQC 算法频频遭到攻破, 安全性难以保证; 相对于经典公钥密码, 现有 PQC 算法也面临通信代价高的问题. 这与区块链的底层稳定性要求, 以及不同场景应用下的性能要求构成一对矛盾, 所以研究能与区块链相适应的后量子密码算法设计理论就显得尤为重要. 经过多年的研究, 国际上已针对 PQC 算法设计形成了一系列主流理论体系, 如格密码; 但从第一代公钥密码应用的经验教训来看, 区块链底层的密码算法应该更加多样化, 同时支持多种基于不同底层问题的算法. 事实上, NIST 在第四轮算法筛选的同时, 还会进行一次专门面向非格基签名的算法征集工作, 这就说明了算法多样性的重要性 [85]. 所以, 适应于区块链的后量子密码算法设计, 应在这些理论体系的基础上, 探索区块链底层密码算法和对应参数集的可配置性方法, 从而产出兼容不同区块链场景需求、灵活可选择配置的算法集与参数集.

协议适配性. PQC 密码协议是 PQC 密码算法在区块链中的表现形态之一, 其安全性依赖于底层

PQC 算法的安全性, 所以也面临威胁. 同时, 这种依赖关系也决定了 PQC 协议的通信开销大于经典的密码协议, 以及与区块链之间存在的兼容性问题. 此外, 区块链中的密码协议包括身份认证、安全通信、安全共识、身份隐私保护等多个方面, 这一多样性也加大了适应于区块链的 PQC 协议研究的工作量. 为此, 可提出区块链 PQC 协议的三个考虑要素:

- 安全性证明: 从 PQC 协议的角度来看它的安全性, 需要考虑协议中的密码模块的安全性, 以及协议本身的通用复合安全性, 这要求 PQC 协议在量子攻击和经典攻击的环境下都要维持安全性.
- 通信效率: 可以从传输数据量和协议交互轮数两个方面入手, 考虑结合中间参数共用技术减少需传输的数据量, 并优化协议设计减少通信双方需要交互的轮数, 提高协议的通信效率.
- 与区块链的兼容性: 现有区块链协议的密码模块针对经典密码设计, 迁移至 PQC 算法后输入输出的数据包尺寸可能不匹配. 为此可考虑利用数据压缩技术来减小协议中需要传输的数据包尺寸.

实现高效性. 抽样操作、多项式运算、矩阵运算是目前 PQC 算法实现的主要瓶颈, 为优化实现效率, 可研究 PQC 算法实现中常用的运算模块, 使其安全高效、参数可配; 硬件特性 (如大整数协处理器) 和指令集优化 (如 AVX2) 也可用于优化算法实现. 但区块链部署的硬件环境多样, 所以面向通用计算机处理器和面向特定处理器的 PQC 优化实现方法都应作为未来 PQC 实现的研究方向. 此外, 根据场景不同, 各个区块链节点部署的硬件环境资源可能有所差异, 如何在这种环境下达到最佳优化实现配置, 也是需要注意的方面. 实现安全性方面, 也应研究 PQC 算法实现对侧信道攻击的防御策略.

迁移可行性. 现有区块链架构大多面向经典密码算法和协议设计, PQC 算法的引入, 使 PQC 算法协议与区块链各个模块间的关联性、耦合性不清晰; 而现有的区块链 PQC 迁移工作仍然是算法集成和原型系统构建的阶段, 对适配于 PQC 算法的区块链架构设计方面的工作很少. 所以, 新的区块链架构设计也应作为未来区块链 PQC 迁移的研究方向之一, 从而与算法敏捷性结合, 达到 PQC 算法与区块链系统之间的相互适配. 而区块链应用的长效安全要求和 PQC 算法安全性的不稳定性构成一对矛盾, 这要求未来的区块链架构应具有可插拔、组件化的可扩展特性. 另外, PQC 迁移的涉及面广, 涵盖区块链各层级架构、基本模块及工程实现等方面, 如何兼容原有业务且支持容错处理, 构建平滑的大规模迁移方案, 也是具有挑战性的问题.

我国区块链应用以联盟链为主, 公有链现有模式难以在国内区块链生态复用 [159]. 自 2017 年人民银行等七部门发布《关于防范代币发行融资风险的公告》 [160] 以来, 国内的投融资项目主要以联盟链相关的企业为主. 同时, 近年来公众对数据要素、个人信息隐私保护的关注度进一步提升, 区块链技术被看作是解决数据隐私和安全的解决方案. 在这样的背景下, 各个行业以联盟链为主的区块链应用正在蓬勃发展, 2022 年 7 月, 国家网信办发布第九批区块链信息服务备案清单, 至此已通过备案的区块链信息服务项目的数量已超过 2159 个 [161]. 所以在我国, 加大联盟链 PQC 迁移的研究力度十分重要.

4 结论

为了对未来 PQC 全球性工程化迁移工作做好准备, 本文从迁移目标和迁移过程两个方面, 提出了后量子密码迁移的原则并根据它们对国内外相关研究成果进行了分类阐述, 其中迁移目标要求完成迁移后的信息系统具有安全性、可用性、敏捷性和普适性. 迁移过程方面, 本文指出 PQC 迁移不是简单的算法替换, 需要从工程化的角度, 例如借鉴软件工程的角度系统地对待迁移应用的迁移需求进行分析和迁移设计, 并谨慎安排应用算法迁移工作的优先级, 制定迁移策略. 现有工作中的迁移策略主要包含混合加密模式和算法协商模式, 前者在系统中同时使用第一代和第二代公钥密码, 从而使系统既能满足现有应用场景的安全性, 又能为将来抗量子攻击做好准备. 后者主要用于原本就支持算法协商的安全通信协议, 如 TLS 协议. 在制定并实施迁移策略时, 需要仔细考虑安全和性能, 以及应用和基础设施的复杂性, 并遵循迁移过程的相关流程. 本文最后以区块链为例, 把区块链对公钥密码的使用分为底层节点间通信和上层交易安全两个层次, 并分别进行 PQC 迁移的综述.

在底层, 本文集中讨论了 TLS 协议的 PQC 迁移工作, 简要说明了 Noise 协议框架的 PQC 迁移工作. TLS 协议中对公钥密码的应用位于握手过程中, 密钥交换协议和签名算法都有迁移需求. TLS 协议本

身支持算法协商, 所以本文主要讨论 TLS 上的混合模式应用, 需要考虑算法协商方式、混合算法数量, 以及传递并组合算法参数的方法. 性能测试是目前 TLS 算法迁移工作的一个重点方向, 可细分为算法性能、硬件性能、网络性能三个方向. 一些工作会先对算法本身进行测量再进行迁移, 但也有工作指出算法本身的性能并不能代表它在区块链中的表现. 网络性能则是目前性能测试的主要方向, 已有工作已针对 TLS 协议、TCP 协议和链路层中的参数造成的影响进行研究, 也有针对不同网络大小、服务器性能等方面的多样化实验. Noise 协议框架的迁移则研究较少, 且主要是针对使用它的 WireGuard VPN 的研究.

在上层, 量子计算会对区块链的共识算法和交易机制产生影响, 由于篇幅所限, 以及共识算法与后量子密码的结合尚处于起步阶段, 因此本文重点讨论了 PQC 对交易机制的影响. 对区块链的迁移策略可分为两种, 一是设计新的抗量子区块链, 二是让现有的区块链抗量子计算的攻击, 两种迁移策略都已有一些工作. 前者的工作一般先针对区块链的特点提出基于格或哈希的 PQC 算法, 再围绕该 PQC 算法设计区块链的共识和交易机制; 而后者则一般是将现有的 PQC 算法放入现有的区块链平台中.

需要指出的是, 虽然底层针对 TLS 的迁移研究有一些工作考虑到了各层协议的参数影响, 但在各种情况下的实验评估和讨论还不全面, 文章中提到的一些优化机制也没有得以实现和评估. 而在上层, 现有工作大多研究公链的迁移, 对联盟链和私链迁移的研究还不多. 应用方面, 现在区块链已形成较大的应用生态圈, 涉及各个业务领域, 未来研究应涵盖对这些业务领域的 PQC 迁移需求分析和迁移方案设计.

目前人们对于 PQC 算法和量子计算本身都仍在探索, 即使区块链平台未来迁移到了某种已成标准的 PQC 算法, 量子计算机和量子算法的分析也可能使部署的 PQC 算法不再安全, 这要求区块链平台做好不断对密码算法进行迁移的准备; 但区块链平台希望底层实现尽量稳定, 不应经常变化, 这就形成了一对矛盾并难以协调, 所以只能尽量使迁移过程简单化, 这就让人们逐渐开始重视 “密码敏捷性”. 而 “敏捷” 的概念起源于复杂系统的不可预测性和不可理解性, 若仍使用传统预先计划并固定各个流程安排的模式, 则无法满足复杂系统多变的需求. 所以人们提出敏捷这一模式, 以人为中心, 固定每轮迭代的时间, 灵活各个流程安排. 软件开发过程即由此而来, 传统软件开发过程无法满足市场需求的快速变化, 所以人们引入了敏捷开发. 而密码算法迁移本质上也是软件开发过程的迭代过程, 且区块链等应用要求这一迭代过程轻量化, 故可借鉴软件敏捷性的框架和方法 (如 Scrum 方法、极限编程), 尝试达成密码算法迁移过程的敏捷性. 为达到未来部署 PQC 算法后的信息系统密码敏捷性, 在 PQC 迁移过程中的密码库架构与设计应是本次迁移过程纳入考虑的一个重要方面. 使用敏捷方法会对软件的安全性带来挑战 [82], 而密码库又是保证软件安全的一个重要组件, 所以如何在使用敏捷方法减少迁移开销的同时保证安全性, 应是未来密码工程和软件安全的研究方向之一.

对于下一步 PQC 迁移的研究应包含以下三个方面. 一是 PQC 迁移与各类标准的适配性问题: 即各个国家/组织的标准之间的协调对迁移工作的影响, 包括各国标准化机构对 PQC 算法的标准化组织实施、PQC 迁移过程标准化; 国际标准、国家标准、行业标准, 并在此基础上根据 PQC 标准的地区/国家/行业来确定 PQC 迁移的需求; 根据需求给出各行各业的一些设计原则或最佳实践, 以及各种应用如何能够尽量多地符合 PQC 迁移的标准, 满足 PQC 迁移原则当中的普适性要求. 二是长效安全的问题. 随着密码工程在各个重要信息系统当中占比越来越高, 但这些系统又要求底层实现稳定, 所以人们提出要简化迁移过程. 如何让后量子时代的新一代密码产品和应用满足这一长效安全特征, 同时又维持系统应具有的安全性, 是 PQC 迁移面临的一个重要问题. 最后是面向 PQC 的区块链安全迁移的挑战. 由于区块链承载的业务应用非常丰富, 因此对涉及的现代公钥密码的迁移应当分步、稳妥进行, 以点带面逐步展开. 特别是对于在我国有广泛应用场景的联盟链, 首先应当密切关注国际上正在研究的重点 PQC 算法特点, 例如 NIST 正在制标的算法以及算法选择、参数选取所面临的巨大挑战, 然后结合联盟链本身的技术特征, 寻求最佳的安全与效能平衡点, 并首先通过各类原型系统的验证, 再逐步向实际应用场景过渡的方法不断总结其中的工程化挑战, 探索不同应用场景的 PQC 迁移最佳实践.

参考文献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/bitcoin.pdf. 2008.
[2] SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: Architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969–988. [DOI: 10.11897/SP.J.1016.2018.00969]

邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展 [J]. 计算机学报, 2018, 41(5): 969–988. [DOI: 10.11897/SP.J.1016.2018.00969]

[3] VINCENT C H. Blockchain for Access Control Systems[S/OL]. US Department of Commerce, National Institute of Standards and Technology, 2022. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8403.pdf. [DOI: 10.6028/NIST.IR.8403]

[4] SI X M, XU M X, YUAN C. Survey on security of blockchain[J]. Journal of Cryptologic Research, 2018, 5(5): 458–469. [DOI: 10.13868/j.cnki.jcr.000256]
斯雪明, 徐蜜雪, 苑超. 区块链安全研究综述 [J]. 密码学报, 2018, 5(5): 458–469. [DOI: 10.13868/j.cnki.jcr.000256]

[5] DYLAN Y, PETER M, NIK R, et al. Blockchain technology overview[R/OL]. US Department of Commerce, National Institute of Standards and Technology, 2016.
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf. [DOI: 10.6028/NIST.IR.8202]

[6] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644–654. [DOI: 10.1109/TIT.1976.1055638]

[7] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120–126. [DOI: 10.1145/359340.359342]

[8] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203–209. [DOI: 10.1090/S0025-5718-1987-0866109-5]

[9] MILLER V S. Use of elliptic curves in cryptography[C]. In: Advances in Cryptology—CRYPTO '85. Springer Berlin Heidelberg, 1986: 417–426. [DOI: 10.1007/3-540-39799-X_31]

[10] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303–332. [DOI: 10.1137/S0036144598347011]

[11] GROVER L K. A fast quantum mechanical algorithm for database search[C]. In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. ACM, 1996: 212–219. [DOI: 10.1145/237814.237866]

[12] BERNSTEIN D J. Introduction to Post-quantum Cryptography[M]. In: Post-quantum Cryptography. Springer Berlin Heidelberg, 2009: 1–14. [DOI: 10.1007/978-3-540-88702-7_1]

[13] BERNSTEIN D J, LANGE T. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188–194. [DOI: 10.1038/nature23461]

[14] PERLNER R A, COOPER D A. Quantum resistant public key cryptography: A survey[C]. In: Proceedings of the 8th Symposium on Identity and Trust on the Internet. ACM, 2009: 85–93. [DOI: 10.1145/1527017.1527028]

[15] BALDI M, SANTINI P, CANCELLIERI G. Post-quantum cryptography based on codes: State of the art and open challenges[C]. In: Proceedings of 2017 AEIT International Annual Conference. IEEE, 2017: 1–6. [DOI: 10.23919/AEIT.2017.8240549]

[16] DRAGOI V, RICHMOND T, BUCERZAN D, et al. Survey on cryptanalysis of code-based cryptography: From theoretical to physical attacks[C]. In: Proceedings of 2018 7th International Conference on Computers Communications and Control (ICCCC). IEEE, 2018: 215–223. [DOI: 10.1109/ICCCC.2018.8390461]

[17] LI Z, HAN Y L, LI Y, et al. An overview of code-based encryption schemes[J]. Journal of National University of Defense Technology, 2020, 42(4): 134–142. [DOI: 10.11887/j.cn.202004020]
李喆, 韩益亮, 李鱼, 等. 基于编码的加密体制综述 [J]. 国防科技大学学报, 2020, 42(4): 134–142. [DOI: 10.11887/j.cn.202004020]

[18] DING J T, GOWER J E, SCHMIDT D S. Oil-vinegar Signature Schemes[M]. In: Multivariate Public Key Cryptosystems. Springer Boston, MA, 2006: 63–97. [DOI: 10.1007/978-0-387-36946-4_3]

[19] FELDMANN A. A Survey of Attacks on Multivariate Cryptosystems[D]. Waterloo: University of Waterloo, 2005.

[20] REGEV O. Lattice-based cryptography[C]. In: Advances in Cryptology—CRYPTO 2006. Springer Berlin Heidelberg, 2006: 131–141. [DOI: 10.1007/11818175_8]

[21] AJTAI M. Generating hard instances of lattice problems[C]. In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. ACM, 1996: 99–108. [DOI: 10.1145/237814.237838]

[22] GOLDREICH O, GOLDWASSER S, HALEVI S. Public-key cryptosystems from lattice reduction problems[C]. In: Advances in Cryptology—CRYPTO '97. Springer Berlin Heidelberg, 1997: 112–131. [DOI: 10.1007/BFb0052231]

[23] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: A ring-based public key cryptosystem[C]. In: Algorithmic Number Theory—ANTS '98. Springer Berlin Heidelberg, 1998: 267–288. [DOI: 10.1007/BFb0054868]

[24] PEIKERT C. A decade of lattice cryptography[J/OL]. IACR Cryptology ePrint Archive, 2015: 2015/939. https://eprint.iacr.org/2015/939.pdf

[25] NEJATOLLAHI H, DUTT N, RAY S, et al. Post-quantum lattice-based cryptography implementations: A survey[J]. ACM Computing Surveys (CSUR), 2019, 51(6): 1–41. [DOI: 10.1145/3292548]

[26] HE S Y, LI H, LI F H. A survey on high-efficiency hardware implementation for lattice-based cryptosystem[J]. Journal of Cryptologic Research, 2021, 8(6): 1019–1038. [DOI: 10.13868/j.cnki.jcr.000494]
何诗洋, 李晖, 李凤华. 面向格基密码体制的高效硬件实现研究综述 [J]. 密码学报, 2021, 8(6): 1019–1038. [DOI: 10.13868/j.cnki.jcr.000494]
[27] National Institute of Standard and Technology. Post-quantum cryptography[EB/OL]. 2021. https://csrc.nist.gov/projects/post-quantum-cryptography
[28] CHEN L, JORDAN S, LIU Y K, et al. Report on post-quantum cryptography[R/OL]. US Department of Commerce, National Institute of Standards and Technology, 2016. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf. [DOI: 10.6028/NIST.IR.8105]
[29] ALAGIC G, ALPERIN-SHERIFF J, APON D, et al. Status report on the first round of the NIST post-quantum cryptography standardization process[R/OL]. Washington, DC: US Department of Commerce, National Institute of Standards and Technology, 2019. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303. [DOI: 10.6028/NIST.IR.8240]
[30] ALAGIC G, ALPERIN-SHERIFF J, APON D, et al. Status report on the second round of the NIST post-quantum cryptography standardization process[R/OL]. US Department of Commerce, NIST, 2020. https://www.gps949.com/pdf/NIST.IR.8309.pdf. [DOI: 10.6028/NIST.IR.8309]
[31] ALAGIC G, APON D, COOPER D, et al. Status Report on the third round of the NIST post-quantum cryptography standardization process[R/OL]. US Department of Commerce, NIST, 2022. [DOI: 10.6028/NIST.IR.8413]
[32] Chinese Association for Cryptologic Research. Notice of National Cryptographic Algorithm Design Competition[EB/OL]. 2019.
中国密码学会. 全国密码算法设计竞赛通知 [EB/OL]. 2019. https://sfjs.cacrnet.org.cn/site/content/309.html
[33] BARKER W, POLK W, SOUPPAYA M. Getting ready for post-quantum cryptography: Explore challenges associated with adoption and use of post-quantum cryptographic algorithms[R/OL]. NIST Cyber Security White Paper (DRAFT), CSRC.NIST.GOV, 2020, 26. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932330. [DOI: 10.6028/NIST.CSWP.04282021]
[34] BARKER W, SOUPPAYA M. [Project Description] Migration to post-quantum cryptography[R/OL]. National Institute of Standards and Technology, 2021. https://www.nccoe.nist.gov/sites/default/files/legacy-files/pqc-migration-project-description-final.pdf
[35] European Telecommunications Standards Institute. Migration strategies and recommendations to quantum safe schemes[R/OL]. 2020. https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
[36] The White House. Memorandum on improving the cybersecurity of national security, department of defense, and intelligence community systems[EB/OL]. 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
[37] BECHER H, Post-quantum cryptography[R/OL]. 2020. https://community.arm.com/arm-research/m/resources/1002
[38] MOSCA M. Cybersecurity in a quantum world: Will we be ready?[EB/OL]. 2015. https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf
[39] BONEH D, DAGDELEN Ö, FISCHLIN M, et al. Random oracles in a quantum world[C]. In: Advances in Cryptology—ASIACRYPT 2011. Springer Berlin Heidelberg, 2011: 41–69. [DOI: 10.1007/978-3-642-25385-0_3]
[40] SONG F. A note on quantum security for post-quantum cryptography[C]. In: Post-Quantum Cryptography—PQCrypto 2014. Springer Cham, 2014: 246–265. [DOI: 10.1007/978-3-319-11659-4_15]
[41] POINTCHEVAL D, STERN J. Security proofs for signature schemes[C]. In: Advances in Cryptology—EUROCRYPT '96. Springer Berlin Heidelberg, 1996: 387–398. [DOI: 10.1007/3-540-68339-9_33]
[42] BELLARE M, NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[C]. In: Proceedings of ACM Conference on Computer & Communications Security. ACM, 2006: 390–399. [DOI: 10.1145/1180405.1180453]
[43] LYUBASHEVSKY V. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures[C]. In: Advances in Cryptology—ASIACRYPT 2009. Springer Berlin Heidelberg, 2009: 598–616. [DOI: 10.1007/978-3-642-10366-7_35]
[44] DUCAS L, KILTZ E, LEPOINT T, et al. CRYSTALS-Dilithium—Algorithm specifications and supporting documentation (Version 3.1)[EB/OL]. 2021. https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf

[45] JIANG H D, LIU Y M. On post-quantum provable security[J]. Journal of Cyber Security, 2018, 4(2): 13–19. [DOI: 10.19363/j.cnki.cn10-1380/tn.2019.03.02]
江浩东, 刘亚敏. 后量子可证明安全研究 [J]. 信息安全学报, 2018, 4(2): 13–19. [DOI: 10.19363/j.cnki.cn10-1380/tn.2019.03.02]

[46] LIANG M, LUO Y Y, LIU F M. A survey on quantum-secure symmetric cryptography[J]. Joournal of Cryptologic Research, 2021, 8(6): 925–947. [DOI: 10.13868/j.cnki.jcr.000488]
梁敏, 罗宜元, 刘凤梅. 抗量子计算对称密码研究进展概述 [J]. 密码学报, 2021, 8(6): 925–947. [DOI: 10.13868/j.cnki.jcr.000488]

[47] CARSTENS T, EBRAHIMI E, TABIA G, et al. On quantum indistinguishability under chosen plaintext attack[J/OL]. IACR Cryptology ePrint Archive, 2020: 2020/596. https://eprint.iacr.org/2020/596.pdf

[48] DING J T, DEATON J, SCHMIDT K, et al. Cryptanalysis of the lifted unbalanced oil vinegar signature scheme[C]. In: Advances in Cryptology—CRYPTO 2020, Part III. Springer Cham, 2020: 279–298. [DOI: 10.1007/978-3-030-56877-1_10]

[49] DING J T, ZHANG Z, DEATON J, et al. A complete cryptanalysis of the post-quantum multivariate signature scheme Himq-3[C]. In: Information and Communications Security—ICICS 2020. Springer Cham, 2020: 422–440. [DOI: 10.1007/978-3-030-61078-4_24]

[50] SAMARDJISKA S, SANTINI P, PERSICHETTI E, et al. A reaction attack against cryptosystems based on LRPC codes[C]. In: Progress in Cryptology—LATINCRYPT 2019. Springer Cham, 2019: 197–216. [DOI: 10.1007/978-3-030-30530-7_10]

[51] BEULLENS W. Breaking rainbow takes a weekend on a laptop[J/OL]. IACR Cryptology ePrint Archive, 2022: 2022/214. https://eprint.iacr.org/2022/214.pdf

[52] CASTRYCK W, DECRU T. An efficient key recovery attack on SIDH (preliminary version)[J/OL]. IACR Cryptology ePrint Archive, 2022: 2022/975. https://eprint.iacr.org/2022/975.pdf

[53] PERLNER R, KELSEY J, COOPER D. Breaking category five SPHINCS+ with SHA-256[J/OL]. IACR Cryptology ePrint Archive, 2022: 2022/1061. https://eprint.iacr.org/2022/1061.pdf

[54] BERNSTEIN D J, LANGE T. Non-randomness of S-unit lattices[J/OL]. IACR Cryptology ePrint Archive, 2021: 2021/1428. https://eprint.iacr.org/2021/1428.pdf

[55] The Center of Encryption and Information Security—MATZOV. Report on the security of LWE: Improved dual lattice attack[R/OL]. 2022. https://zenodo.org/record/6412487#.YwXYty5By3A

[56] NTRU Prime Risk-Management Team. Risks of lattice KEMs[R/OL]. 2021. https://ntruprime.cr.yp.to/latticerisks-20211031.pdf

[57] PERLNER R, SMITH-TONE D. A classification of differential invariants for multivariate post-quantum cryptosystems[C]. In: Post-Quantum Cryptography—PQCrypto 2013. Springer Berlin Heidelberg, 2013: 165–173. [DOI: 10.1007/978-3-642-38616-9_11]

[58] JAQUES S, SCHANCK J M. Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE[C]. In: Advances in Cryptology—CRYPTO 2019, Part I. Springer Cham, 2019: 32–61. [DOI: 10.1007/978-3-030-26948-7_2]

[59] CHOWDHURY S, COVIC A, ACHARYA R Y, et al. Physical security in the post-quantum era[J]. Journal of Cryptographic Engineering, 2021, 12(3): 267–303. [DOI: 10.1007/s13389-021-00255-w]

[60] WIESMAIER A, ALNAHAWI N, GRASMEYER T, et al. On PQC migration and crypto-agility[OL]. arXiv preprint arXiv:2106.09599, 2021. https://arxiv.org/abs/2106.09599

[61] OTT D, PEIKERT C. Identifying research challenges in post quantum cryptography migration and cryptographic agility[OL]. arXiv preprint arXiv:1909.07353, 2019. https://arxiv.org/abs/1909.07353

[62] CREMERS C, HORVAT M, HOYLAND J, et al. A comprehensive symbolic analysis of TLS 1.3[C]. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 1773–1788. [DOI: 10.1145/3133956.3134063]

[63] KOBEISSI N. Formal Verification for Real-world Cryptographic Protocols and Implementations[D]. Université Paris Sciences et Lettres, 2018.

[64] BARBOSA M, BARTHE G, FAN X, et al. EasyPQC: Verifying post-quantum cryptography[C]. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2021: 2564–2586. [DOI: 10.1145/3460120.3484567]

[65] SEILER G. Faster AVX2 optimized NTT multiplication for Ring-LWE lattice cryptography[J/OL]. IACR Cryptology ePrint Archive, 2018: 2018/39. https://eprint.iacr.org/2018/039.pdf

[66] BARTHE G, FAN X, GANCHER J, et al. Symbolic proofs for lattice-based cryptography[C]. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 538–555. [DOI:

10.1145/3243734.3243825]
[67] BARTHE G, GREGOIRE B, SCHMIDT B. Automated proofs of pairing-based cryptography[C]. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 1156–1168. [DOI: 10.1145/2810103.2813697]
[68] BARTHE G, GREGOIRE B, ZANELLA B S. Formal certification of code-based cryptographic proofs[C]. In: Proceedings of the 36th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. ACM, 2009: 90–101. [DOI: 10.1145/1480881.1480894]
[69] BERTOT Y, CASTERAN P. Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of Inductive Constructions[M]. Springer Berlin Heidelberg, 2013, 1–11.
[70] BLANCHET B. CryptoVerif: A computationally-sound security protocol verifier[R/OL]. 2017. https://bblanche.gitlabpages.inria.fr/CryptoVerif/cryptoverif.pdf
[71] BARTHE G, DUPRESSOIR F, GRÉGOIRE B, et al. EasyCrypt: A Tutorial[M]. In: Foundations of Security Analysis and Design VII. Springer Cham, 2013: 146–166. [DOI: 10.1007/978-3-319-10082-1_6]
[72] DANG V B, MOHAJERANI K, GAJ K. High-speed hardware architectures and FPGA benchmarking of CRYSTALS-Kyber, NTRU, and Saber[J/OL]. IACR Cryptology ePrint Archive, 2021: 2021/1508. https://eprint.iacr.org/2021/1508.pdf
[73] STEBILA D, MOSCA M. Post-quantum key exchange for the Internet and the open quantum safe project[C]. In: Selected Areas in Cryptography—SAC 2016. Springer Cham, 2016: 14–37. [DOI: 10.1007/978-3-319-69453-5_2]
[74] BUCHMANN J, MAY A, VOLLMER U. Perspectives for cryptographic long-term security[J]. Communications of the ACM, 2006, 49(9): 50–55. [DOI: 10.1145/1151030.1151055]
[75] MESO P, JAIN R. Agile software development: Adaptive systems principles and best practices[J]. Information Systems Management, 2006, 23(3): 19–30. [DOI: 10.1201/1078.10580530/46108.23.3.20060601/93704.3]
[76] FIPS 197. Advanced Encryption Standard (AES)[S/OL]. 2021. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
[77] NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process[EB/OL]. 2016. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf
[78] HOUSLEY R. Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms[S/OL]. RFC7696, 2015. https://datatracker.ietf.org/doc/html/rfc7696
[79] FOWLER M, HIGHSMITH J. The agile manifesto[J]. Software Development, 2001, 9(8): 28–35.
[80] ISO, ISO/IEC 9594-11:2020. Open Systems Interconnection Directory[S/OL]. 2020. https://www.iso.org/standard/75417.html
[81] GAGLIANO R, KENT S, TURNER S. Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI)[S/OL]. RFC6916, 2013. https://datatracker.ietf.org/doc/html/rfc6916
[82] OUESLATI H, RAHMAN M M, BEN O L. Literature review of the challenges of developing secure software using the agile approach[C]. In: Proceedings of 2015 10th International Conference on Availability, Reliability and Security. IEEE, 2015: 540–547. [DOI: 10.1109/ARES.2015.69]
[83] HUELSING A, BUTIN D, GAZDAG S L, et al. XMSS: eXtended Merkle Signature Scheme[S/OL]. RFC 8391, 2018. https://datatracker.ietf.org/doc/html/rfc8391
[84] D'ANVERS J P, VERBAUWHEDE I. On the impact of decryption failures on the security of LWE/LWR based schemes[OL]. 2018. https://lirias.kuleuven.be/retrieve/602448
[85] National Cybersecurity Center of Excellence. NCCoE learning series webinar: Preparing for the migration to post-quantum cryptography[EB/OL]. 2022. https://www.nccoe.nist.gov/get-involved/attend-events/nccoe-learning-series-webinar-preparing-migration-post-quantum
[86] BERRUETA E, MORATO D, MAGANA E, et al. A survey on detection techniques for cryptographic ransomware[J]. IEEE Access, 2019, 7: 144925–144944. [DOI: 10.1109/ACCESS.2019.2945839]
[87] ZHAO C X, KANG F, YANG J, et al. A review of cryptographic algorithm recognition technology for binary code[C]. In: Journal of Physics: Conference Series, 2021, 1856(1): 012015. [DOI: 10.1088/1742-6596/1856/1/012015]
[88] ETSI. Quantum safe cryptography and security: An introduction, benefits, enablers and challenges[R/OL]. 2014. https://docbox.etsi.org/workshop/2014/201410_crypto/quantum_safe_whitepaper_1_0_0.pdf
[89] MASEBERG J S. Fail-Safe-Konzept für Public-Key-Infrastrukturen[D]. Technische Universität, 2002.
[90] BARNES R L, BHARGAVAN K, LIPP B, et al. Hybrid Public Key Encryption[S/OL]. Internet-draft, Internet Research Task Force, 2021. https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hpke-12
[91] OUNSWORTH M, PALA M. Composite Signatures for Use in Internet PKI[S/OL]. Internet-draft, Internet

Research Task Force, 2021. https://www.ietf.org/archive/id/draft-ounsworth-pq-composite-sigs-05.txt

[92] CROCKETT E, PAQUIN C, STEBILA D. Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH[J/OL]. IACR Cryptology ePrint Archive, 2019: 2019/858. https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/stebila-prototyping-post-quantum.pdf

[93] BHARGAVAN K, BRZUSKA C, FOURNET C, et al. Downgrade resilience in key-exchange protocols[C]. In: Proceedings of 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016: 506–525. [DOI: 10.1109/SP.2016.37]

[94] GM/T 0111-2021. Technical Requirements for blockchain Cryptography Application[S]. Beijing: State Cryptography Administration. 2021.
GM/T 0111-2021. 区块链密码应用技术要求 [S]. 北京: 国家密码管理局. 2021.

[95] FENG H W, LIU J W, WU Q H. Group signatures and ring signatures with post-quantum security[J]. Journal of Cryptologic Research, 2021, 8(2): 183–201. [DOI: 10.13868/j.cnki.jcr.000430]
冯翰文, 刘建伟, 伍前红. 后量子安全的群签名和环签名 [J]. 密码学报, 2021, 8(2): 183–201. [DOI: 10.13868/j.cnki.jcr.000430]

[96] DIERKS T, RESCORLA E. The Transport Layer Security (TLS) Protocol Version 1.2[S/OL]. RFC5246, 2008. https://www.hjp.at/doc/rfc/rfc5246.html

[97] RESCORLA E, DIERKS T. The Transport Layer Security (TLS) Protocol Version 1.3[S/OL]. RFC8446, 2018. https://www.hjp.at/doc/rfc/rfc8446.html

[98] PERRIN T. The Noise Protocol Framework[S/OL]. 2018. http://www.noiseprotocol.org/noise.pdf

[99] BOS J W, COSTELLO C, NAEHRIG M, et al. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem[C]. In: Proceedings of 2015 IEEE Symposium on Security and Privacy. IEEE, 2015: 553–570. [DOI: 10.1109/SP.2015.40]

[100] BANERJEE U, CHANDRAKASAN A P. Efficient post-quantum TLS handshakes using identity-based key exchange from lattices[C]. In: Proceedings of 2020 IEEE International Conference on Communications (ICC 2020). IEEE, 2020: 1–6. [DOI: 10.1109/ICC40277.2020.9148829]

[101] GAO X W, DING J T, LI L, et al. Efficient implementation of password-based authenticated key exchange from RLWE and post-quantum TLS[J/OL]. IACR Cryptology ePrint Archive, 2017: 2017/1192. https://eprint.iacr.org/2017/1192.pdf

[102] SCHWABE P, STEBILA D, WIGGERS T. Post-quantum TLS without handshake signatures[C]. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2020: 1461–1480. [DOI: 10.1145/3372297.3423350]

[103] BINDEL N, BRENDEL J, FISCHLIN M, et al. Hybrid key encapsulation mechanisms and authenticated key exchange[C]. In: Post-Quantum Cryptography—PQCrypto 2019. Springer Cham, 2019: 206–226. [DOI: 10.1007/978-3-030-25510-7_12]

[104] CHANG Y A, CHEN M S, WU J S, et al. Postquantum SSL/TLS for embedded systems[C]. In: Proceedings of 2014 IEEE 7th International Conference on Service-oriented Computing and Applications. IEEE, 2014: 266–270. [DOI: 10.1109/SOCA.2014.23]

[105] SIKERIDIS D, KAMPANAKIS P, DEVETSIKIOTIS M. Post-quantum authentication in TLS 1.3: A performance study[J/OL]. IACR Cryptology ePrint Archive, 2020: 2020/071. https://eprint.iacr.org/2020/071.pdf

[106] GAO X W, LI L, DING J T, et al. Fast discretized Gaussian sampling and post-quantum TLS ciphersuite[C]. In: Information Security Practice and Experience—ISPEC 2017. Springer Cham, 2017: 551–565. [DOI: 10.1007/978-3-319-72359-4_33]

[107] BERNSTEIN D J, BRUMLEY B B, CHEN M S, et al. OpenSSLNTRU: Faster post-quantum TLS key exchange[OL]. arXiv preprint arXiv:2106.08759, 2021. https://arxiv.org/abs/2106.08759

[108] PAQUIN C, STEBILA D, TAMVADA G. Benchmarking post-quantum cryptography in TLS[C]. In: Post-Quantum Cryptography—PQCrypto 2020. Springer Cham, 2020: 72–91. [DOI: 10.1007/978-3-030-44223-1_5]

[109] SIKERIDIS D, KAMPANAKIS P, DEVETSIKIOTIS M. Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH[C]. In: Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies. ACM, 2020: 149–156. [DOI: 10.1145/3386367.3431305]

[110] CAMPAGNA M, CROCKETT E. Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)[S/OL]. Internet-draft draft-campagna-tls-bike-sike-hybrid-05, Internet Engineering Task Force, 2021. Work in Progress. https://datatracker.ietf.org/doc/html/draft-campagna-tls-bike-sike-hybrid-07.

[111] WHYTE W, ZHANG Z, FLURHER S, et al. Quantum-safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) Version 1.3[S/OL]. Internet-draft draft-whyte-qsh-tls13-06, Internet Engineering Task Force, Oc-

tober 2017. Work in Progress. https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls13-06
[112] SCHCNCK J M, STEBILA D. A Transport Layer Security (TLS) Extension for Establishing an Additional Shared Secret[S/OL]. Internet-draft draft-schanck-tls-additional-keyshare-00, Internet Engineering Task Force, April 2017. Work in Progress. https://datatracker.ietf.org/doc/html/draft-schanck-tls-additional-keyshare-00.
[113] KIEFER F, KWIATKOWSKI K. Hybrid ECDHE-SIDH Key Exchange for TLS[S/OL]. Internet-draft draftkiefer-tls-ecdhe-sidh-00, Internet Engineering Task Force, November 2018. Work in Progress. https://datatracker.ietf.org/doc/html/draft-kiefer-tls-ecdhe-sidh-00.
[114] STEBILA D, FLUHRER S, and GUERON S. Hybrid Key Exchange in TLS 1.3[S/OL]. Internet-draft draft-ietf-tls-hybrid-design-04, Internet Engineering Task Force, January 2022. Work in Progress. https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design.
[115] PAUL S, KUZOVKOVA Y, LAHR N, et al. Mixed certificate chains for the transition to post-quantum authentication in TLS 1.3[J/OL]. IACR Cryptology ePrint Archive, 2021: 2021/1447. https://eprint.iacr.org/2021/1447.pdf
[116] RESCORLA E, BARNES R, TSCHOFENIG H. Compact TLS 1.3[S/OL]. Internet-draft draft-ietf-tls-ctls-04, Internet Engineering Task Force, October 2021. https://datatracker.ietf.org/doc/html/draft-ietf-tls-ctls
[117] THOMSON M. Suppressing Intermediate Certificates in TLS[S/OL]. Internet-draft draft-thomson-tls-sic-00. Internet Engineering Task Force, March 2019. https://datatracker.ietf.org/doc/html/draft-thomson-tls-sic-00
[118] KAMPANAKIS P, KALLITSIS M. Speeding up post-quantum TLS handshakes by suppressing intermediate CA certificates[R/OL]. 2021. https://assets.amazon.science/00/f8/aa76ff93472d9b55b6a84716e34c/speeding-up-post-quantum-tls-handshakes-by-suppressing-intermediate-ca-certificates.pdf
[119] GHEDINI A, VASILIEV V. TLS Certificate Compression[S/OL]. RFC8879. https://www.hjp.at/doc/rfc/rfc8879.html
[120] LAURIE B, LANGELY A, KASPER E. Certificate Transparency[S/OL]. RFC6962. https://www.hjp.at/doc/rfc/rfc6962.html
[121] SANTESSON S, MYERS M, ANKNEY R, et al. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP[S/OL]. RFC6960. https://www.hjp.at/doc/rfc/rfc6960.html
[122] GIACON F, HEUER F, POETTERING B. KEM combiners[C]. In: Public-Key Cryptography—PKC 2018, Part I. Springer Cham, 2018: 190–218. [DOI: 10.1007/978-3-319-76578-5_7]
[123] Diem Association. Diem Association: Home Page[EB/OL]. 2020. https://www.diem.com/en-us/
[124] PERRIN T. KEM-based Hybrid Forward Secrecy for Noise[S/OL]. 2021. https://github.com/noiseprotocol/noise_hfs_spec/blob/master/output/noise_hfs.pdf
[125] DONENFELD J A. WireGuard: Next generation kernel network tunnel[C]. In: NDSS. 2017: 1–12. [DOI: 10.14722/ndss.2017.23160]
[126] KNIEP Q M, MULLER W, REDLICH J P. Post-quantum cryptography in WireGuard VPN[C]. In: Security and Privacy in Communication Networks—SecureComm 2020. Springer Cham, 2020: 261–267. [DOI: 10.1007/978-3-030-63095-9_16]
[127] HÜLSING A, NING K C, SCHWABE P, et al. Post-quantum WireGuard[J/OL]. IACR Cryptology ePrint Archive, 2020: 2020/379. https://eprint.iacr.org/2020/379.pdf
[128] GAO Y L, CHEN X B, CHEN Y L, et al. A secure cryptocurrency scheme based on post-quantum blockchain[J]. IEEE Access, 2018, 6: 27205–27213. [DOI: 10.1109/ACCESS.2018.2827203]
[129] HOLCOMB A, PEREIRA G C C F, DAS B, et al. PQFabric: A permissioned blockchain secure from both classical and quantum attacks[OL]. arXiv preprint arXiv:2010.06571, 2020. https://arxiv.org/abs/2010.06571
[130] FERNÁNDEZ-CARAMÈS T M, FRAGA-LAMAS P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks[J]. IEEE Access, 2020, 8: 21091–21116. [DOI: 10.1109/ACCESS.2020.2968985]
[131] LIU Y Z, LIU J W, ZHANG Z Y, et al. Overview on blockchain consensus mechanisms[J]. Journal of Cryptologic Research, 2019, 6(4): 395–432. [DOI: 10.13868/j.cnki.jcr.000311]
刘懿中, 刘建伟, 张宗洋, 等. 区块链共识机制研究综述 [J]. 密码学报, 2019, 6(4): 395–432. [DOI: 10.13868/j.cnki.jcr.000311]
[132] National Institute of Standards and Technology. Secure Hash Standard (SHS)[S/OL]. 2021. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
[133] National Institute of Standards and Technology. SHA-3 Standard: Permutation-based Hash and Extendable-output Functions[S/OL]. 2021. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
[134] LAMPORT L, SHOSTAK R, PEASE M. The byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382–401. [DOI: 10.1145/ 357172.357176]

[135] FISCHER M J, LYNCH N A, PATERSON M S. Impossibility of distributed consensus with one faulty process[J]. Journal of the ACM, 1985, 32(2): 374–382. [DOI: 10.1145/3149.214121]

[136] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol[C]. In: Advances in Cryptology—CRYPTO 2017, Part I. Springer Cham, 2017: 357–388. [DOI: 10.1007/978-3-319-63688-7_12]

[137] AGARWAL A, BARTUSEK J, GOYAL V, et al. Post-quantum multi-party computation[C]. In: Advances in Cryptology—EUROCRYPT 2021, Part I. Springer Cham, 2021: 435–464. [DOI: 10.1007/978-3-030-77870-5_16]

[138] AGGARWAL D, BRENNEN G K, LEE T, et al. Quantum attacks on bitcoin, and how to protect against them[OL]. arXiv preprint arXiv:1710.10377, 2017. https://arxiv.org/abs/1710.10377

[139] GHEORGHIU V, GORBUNOV S, MOSCA M, et al. Quantum proofing the blockchain[R/OL]. Blockchain Research Institute: University of Waterloo, 2017. https://evolutionq.com/quantum-safe-publications/mosca_quantum-proofing-the-blockchain_blockchain-research-institute.pdf

[140] ABCMint Foundation. ABCMint Foundation[EB/OL]. 2017. www.abcmint.org

[141] DING J T. A new proof of work for blockchain based on random multivariate quadratic equations[C]. In: Applied Cryptography and Network Security Workshops—ACNS 2019. Springer Cham, 2019: 97–107. [DOI: 10.1007/978-3-030-29729-9_5]

[142] YIN W, WEN Q Y, LI W M, et al. An anti-quantum transaction authentication approach in blockchain[J]. IEEE Access, 2018, 6: 5393–5401. [DOI: 10.1109/ACCESS.2017.2788411]

[143] TORRES W A A, STEINFELD R, SAKZAD A, et al. Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1.0)[C]. In: Information Security and Privacy—ACISP 2018. Springer Cham, 2018: 558–576. [DOI: 10.1007/978-3-319-93638-3_32]

[144] ESGIN M F, ZHAO R K, STEINFELD R, et al. MatRiCT: Efficient, scalable and post-quantum blockchain confidential transactions protocol[C]. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019: 567–584. [DOI: 10.1145/3319535.3354200]

[145] CHALKIAS K, BROWN J, HEARN M, et al. Blockchained post-quantum signatures[C]. In: Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018: 1196–1203. [DOI: 10.1109/Cybermatics_2018.2018.00213]

[146] SHAHID F, KHAN A, JEON G. Post-quantum distributed ledger for Internet of things[J]. Computers & Electrical Engineering, 2020, 83: 106581. [DOI: 10.1016/j.compeleceng.2020.106581]

[147] CHEN J H, GAN W S, HU M C, et al. On the construction of a post-quantum blockchain for smart city[J]. Journal of Information Security and Applications, 2021, 58: 102780. [DOI: 10.1016/j.jisa.2021.102780]

[148] CHEN J H, LING J, NING J, et al. Identity-based signature schemes for multivariate public key cryptosystems[J]. The Computer Journal, 2019, 62(8): 1132–1147. [DOI: 10.1093/comjnl/bxz013]

[149] ZHANG P J, WANG L H, WANG W, et al. A blockchain system based on quantum-resistant digital signature[J]. Security and Communication Networks, 2021, 2021: 6671648. [DOI: 10.1155/2021/6671648]

[150] PREECE J D, EASTON J M. Towards encrypting industrial data on public distributed networks[C]. In: Proceedings of 2018 IEEE International Conference on Big Data (Big Data). IEEE, 2018: 4540–4544. [DOI: 10.1109/BigData.2018.8622246]

[151] GAO S Y, ZHENG D, GUO R, et al. An anti-quantum e-voting protocol in blockchain with audit function[J]. IEEE Access, 2019, 7: 115304–115316. [DOI: 10.1109/ACCESS.2019.2935895]

[152] ANHAO N. Bitcoin post-quantum[R/OL]. 2021. https://bitcoinpq.org/download/bitcoinpq-whitepaper-english.pdf

[153] SEMMOUNI M C, NITAJ A, BELKASMI M. Bitcoin security with post quantum cryptography[C]. In: Networked Systems—NETYS 2019. Springer Cham, 2019: 281–288. [DOI: 10.1007/978-3-030-31277-0_19]

[154] Ethereum Foundation. Ethereum's official roadmap[EB/OL]. 2020. https://eth.wiki/en/sharding/sharding-roadmap

[155] SHEN R P, XIANG H, ZHANG X, et al. Application and implementation of multivariate public key cryptosystem in blockchain (Short Paper)[C]. In: Collaborative Computing: Networking, Applications and Worksharing—CollaborateCom 2019. Springer Cham, 2019: 419–428. [DOI: 10.1007/978-3-030-30146-0_29]

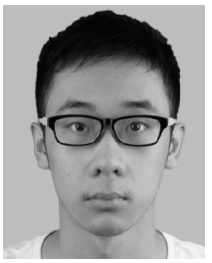
[156] ALLENDE M, LEON D L, CERON S, et al. Quantum-resistance in blockchain networks[OL]. arXiv preprint arXiv:2106.06640, 2021. https://arxiv.org/abs/2106.06640

[157] Abelian Foundation. Abelian Foundation website[EB/OL]. 2019. https://www.abelianfoundation.org

[158] R3. Cipher suites supported by Corda[EB/OL]. 2021.

https://docs.r3.com/en/platform/corda/4.8/open-source/cipher-suites.html
[159] China Academy of Information and Communications Technology. Whitepaper on blockchain (2021)[R/OL]. 2021
中国信息通信研究院. 区块链白皮书 (2021 年) [R/OL]. 2021.
https://www.caict.ac.cn/kxyj/qwfb/bps/202112/t20211222_394418.htm
[160] The People's Bank of China. Announcements of seven departments including the People's Bank of China on preventing the risk of token issuance and financing[EB/OL]. 2017
中国人民银行. 人民银行等七部门关于防范代币发行融资风险的公告 [EB/OL]. 2017.
http://www.gov.cn/xinwen/2017-09/04/content_5222657.htm
[161] Cyberspace Administration of China. Announcement of the Cyberspace Administration of China on the issuance of the ninth batch of domestic blockchain information service filing numbers[EB/OL]. 2022
中华人民共和国国家互联网信息办公室. 国家互联网信息办公室关于发布第九批境内区块链信息服务备案编号的公告 [EB/OL]. 2022. http://www.cac.gov.cn/2022-07/25/c_1660369837207693.htm

作者信息



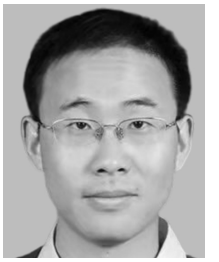
胡希 (1999–), 重庆人, 硕士研究生. 主要研究领域为密码工程与应用.
huxicqu@cqu.edu.cn

向宏 (1964–), 四川成都人, 博士, 教授. 主要研究领域为密码工程与应用.
xianghong@cqu.edu.cn

丁津泰 (1967–), 博士, 教授. 主要研究领域为多变量密码和格密码、量子证明区块链.
dinglab@bimsa.cn

梁蓓 (1985–), 湖北安陆人, 博士, 助理教授. 主要研究领域为公钥密码学、可证明安全密码体制.
lbei@bimsa.cn

夏鲁宁 (1977–), 山东济宁人, 博士, 正高级工程师. 主要研究领域为密码应用和电子认证技术.
xialuning@bjca.org.cn



向涛 (1980–), 湖北荆门人, 博士, 教授, 主要研究领域为隐私保护、区块链、多媒体安全.
txiang@cqu.edu.cn