

特色专题

基于双签融合机制的商业银行网银抗量子迁移架构与实证研究

沈坤平, 李昆霖, 潘建东

摘要 针对金融行业核心网银系统在抗量子计算密码迁移过程中面临的业务连续性风险、海量终端兼容性差以及高并发性瓶颈等痛点,提出并实现了一种面向大型商业银行的网银全栈抗量子密码迁移架构。该架构采用混合 TLS(transport layer security)安全通道与国密 SM2(商密 2 号)联合 ML-DSA(module-lattice-based digital signature algorithm)的双签融合机制,构建了从底层硬件终端到网络传输,再到后端集群验签的端到端演进路径。依托某商业银行真实网银环境进行的灰度高仿真验证表明,在支撑 1000 TPS(transactions per second)并发交易压力的场景下,混合安全通道建立响应时间优化至 3.5 ms,单次验签耗时约 13.6 ms。本实证研究初步验证了高维格密码算法在本文测试环境与负载下的可用性,为中国银行业关键信息基础设施的平滑抗量子演进提供了可复制的工程示范。

关键词 抗量子密码迁移;双签融合;网银系统;混合 TLS 协议;高并发验证;平滑演进

随着量子计算理论的成熟与物理硬件的快速迭代,现有基于大整数分解与离散对数难题的公钥密码体系正面临失效风险。Shor 算法已被证明可在多项式时间内高效求解上述经典数学难题^[1]。金融网银系统承载着海量资金交易与敏感隐私数据,其底层的身份鉴别与交易抗否认机制高度依赖 RSA(Rivest-Shamir-Adleman)、ECC(elliptic curve cryptography)及国密 SM2 等传统非对称算法。为防范“先收集后解密”及未来量子计算机的直接破解威胁,开展抗量子计算密码(post-quantum cryptography, PQC)迁移已成为保障国家金融基础设施安全的战略任务。

美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)于 2024 年正式发布了 FIPS 203 与 FIPS204 标准,分别确立了基于模块格

的 ML-KEM 和 ML-DSA 算法基准^[2-3]。当前,国际主流金融机构与标准组织已逐步开启混合密码模式的试点^[4]。然而,现有的迁移研究与工程实践大多局限于网络传输层(如纯软件的 TLS 握手测试),缺乏涵盖客户端硬件、应用层协议及后端验签服务器的端到端全栈落地案例^[5]。

商业银行网银系统具有 7×24 h 不间断运行、突发高并发(如秒杀、代发薪)以及存量终端(旧版浏览器、传统 UKey)体量庞大等特征。采取“一刀切”或中断业务式的算法替换在工程上不可行。因此,如何设计一种既能抵御量子攻击,又能向下兼容海量旧终端,且不引发系统性能雪崩的平滑迁移架构,是当前密码工程领域的核心难题。基于上述挑战,本文提出了一种双签融合网银抗量子迁移架构,并在真实商业银行的网银环境中完成了灰度部署与并发性能实测,以为行业提供可靠的技术路径参考^[6]。

江苏银行股份有限公司,南京 210000

收稿日期:2026-05-13;修回日期:2026-08-24

基金项目:国家重点研发计划项目(2023YFC33055, 2025YFE0218100)

作者简介:沈坤平,研究方向为银行业数字化转型、信息安全、科技架构规划等,电子信箱:shenkunping@jsbchina.cn

引用格式:沈坤平,李昆霖,潘建东.基于双签融合机制的商业银行网银抗量子迁移架构与实证研究[J].科技导报,2026,44(16):118-122;

doi:10.3981/j.issn.1000-7857.2026.05.00062

1 双签融合网银系统总体架构设计

为打破 PQC 在单点适配中的局限性,本研究构建了包含硬件、算法、协议、平台与应用 5 大维度的

全栈量子演进架构,实现前后端安全逻辑的完全闭环。全栈量子网银系统的总体架构与数据流向如图 1 和图 2 所示。



图 1 全栈量子网银系统的总体架构与数据流向



图 2 全栈量子网银系统总体架构

终端物理硬件层: 部署具备高维矩阵运算加速能力的混合智能密码钥匙(PQC-UKey)及量子安全网关。作为物理信任根,负责量子密钥的生成、隔离存储与底层签名运算。

混合密码算法层: 以国密 SM2 和 SM3/SM4 为合规基础,深度融合数字签名(module-lattice-based digital signature algorithm, ML-DSA)与密钥封装(module-lattice-based key-encapsulation mechanism, ML-

KEM)。

传输网络协议层: 构建基于 TLS 1.2/1.3 扩展的混合握手模式,支撑传统基于椭圆曲线的临时迪菲-赫尔曼密钥交换 ECDHE(elliptic curve Diffie-Hellman ephemeral)与量子 ML-KEM 算法的并行密钥协商,保障通信链路的前向安全(forward secrecy)。

平台支撑与验证层: 建设并改造量子 PKI(public key infrastructure)体系,实现量子 CA(certificate authority)证书签发与传统证书的双证书同生命周期绑定。部署自适应并发签名验签服务器集群,提供千万级处理能力。

业务应用场景层: 覆盖个人网银与企业网银的全业务流,包括高频的登录鉴权、大额转账、电子合同签署等核心场景。

2 混合加密体系的关键技术机制

在实施网银系统全栈迁移前,必须解决量子算法与网银高并发特性的适配问题。本章重点阐述算法安全性优选框架,以及在此基础上构建的混合通道与验签机制。

2.1 基于高维格密码分析的算法评估与优选机制

当前国际 PQC 标准虽已发布,但面对涉及国家

金融基础设施的核心网银业务,直接引入仍存在潜在底层数理风险。为此,在混合架构设计初,本研究构建了独立于国际标准的算法安全性校验与优选框架。

该框架深入格密码底层的核心数学难题,利用高维最短向量问题(shortest vector problem, SVP)及其派生的带错学习问题(learning with errors/module learning with errors, LWE/MLWE),对候选算法的实际安全冗余进行了量化分析^[7]。依托真实场景下的高维格密码分析平台,本研究团队针对美国 NIST 标准在不同维度的实例(如 Kyber-208、Kyber-256 等),开展了密码安全性的极限压力测试与破译验证^[8]。这种白盒化的理论安全测试,不仅严苛校验了格密码在不同参数维度下的抗击溃能力与安全边界,更为金融级应用提供了自主可控的安全冗余量化依据。

在此安全性校验的基础上,针对商业银行高并发、低延迟的业务场景,对最终选定的标准算法进行了工程化维度的取舍。通过底层多项式乘法与数论变换(number theoretic transform, NTT)的代码级调优,充分发挥了格密码在计算开销上的原生高效优势;同时,针对其公钥尺寸激增带来的网络传输痛点,系统确立了以高安全维度实例为信任根,并在应用层与网络层进行混合协议调优的设计导向。需要说明的是,上述面向服务器端的 NTT/单指令多数据(single instruction, multiple data, SIMD)并行,以及 Montgomery 约简与 Barrett 约简等模约减优化,均属 ML-KEM/ML-DSA 标准算法的公开工程实现范畴,本文实现主要参考代数格密码套件(cryptographic suite for algebraic lattices, CRYSTALS)官方优化实现与 AVX2 优化的 NTT 乘法方案^[9-10],在此基础上完成面向验签集群的工程集成,未对标准算法本身的密码学设计做任何改动。

2.2 混合 TLS 通道协商协议机制

针对网银 B/S(browser/server)与 C/S(client/server)架构中的通道窃听风险,系统在 SSL/TLS 协议的握手阶段引入了混合密钥封装扩展(hybrid key encapsulation)^[11]。在客户端(浏览器或移动端环境)与抗量子 SSL(secure sockets layer)网关交互时,握手机报文(ClientHello)的 supported_groups 扩展中同时携带国密椭圆曲线标识与抗量子 KEM(key-encapsulation mechanism)参数集标识。在密钥交换(key exchange)

阶段,双方并行执行传统 ECDHE 计算与 ML-KEM 封装/解封装操作。最终,将会话密钥推导建立在 2 种算法共享密钥的组合之上。该机制确保了在抗量子算法面临潜在数理缺陷或传统算法被量子攻破的任意单一极端情况下,会话密钥依然保持强前向安全性^[12]。

2.3 强绑定双签机制与自适应验签调度

在应用层交易防篡改环节,系统构建了“同源数据、双重校验”的融合体系。前端 PQC-UKey 输出包含 SM2 与 ML-DSA 签名的混合 PKCS#7 报文后,后端的签名验签服务器集群执行严格的降级防范逻辑^[13]。

验签集群被设计为“自适应调度模式”。当接收到交易请求时,网关代理会解析报文头部特征:对于已升级的白名单灰度用户,系统强制执行“逻辑与(AND)”策略,必须国密与抗量子签名双重验证通过才释放交易请求,彻底根除签名剥离与降级攻击。

对于尚未更换抗量子终端的存量用户,自适应引擎自动识别并降级路由至传统国密验证通道。该机制在实现核心资产高安全防护的同时,最大程度保障了现网业务的连续性与用户无感体验。

3 迁移策略及高仿真环境与并发灰度实证实测

在实施路径上,系统采用“双算法并行、按策略路由、一键回滚”的敏捷演进模式。抗量子应用插件以动态链接库或沙盒隔离的形式下发,网络层旁路部署抗量子网关集群,避免对原有核心网银交易引擎进行侵入式重构。通过控制灰度策略引流,实现了分阶段、分客群的业务流量切割。

为全面评估所提架构的工程可行性,本研究将该方案部署于某区域性大型商业银行的网银生产副中心,开展了面向企业与个人网银白名单客户的真实灰度验证。

1) 压测环境与集群拓扑。实证测试平台后端采用 5 台配置为 8 核 CPU(central processing unit)、16 GB 内存的常规 x86 物理服务器作为集群节点。前端模拟及真实灰度节点涵盖 PC 端主流浏览器与专用客户端,网络环境覆盖银行内网专线与公共互联网链路。测试核心目标在于验证高维格密码引入后,网络带宽膨胀与服务器 CPU 密集型计算对 TPS(transactions

per second)及延迟的极限影响。

2) 高并发性能指标与混合通道实测分析。根据灰度实测数据及极限压测结果,在单台物理节点(8核/16 GB)面对 1000 TPS 的基础并发压力下,系统表现出优异的稳定性。依托后端验签集群的动态并发调度机制,该架构具备应对突发超高并发场景的扩展潜力,在保障抗量子运算性能的同时,严守现网业务的连续性。

针对混合 TLS 握手阶段计算与内存开销密集的密钥封装与解封装环节,本研究进行了专项并发性能优化^[14]。测试结果表明,得益于底层网关网络栈的异步 I/O 优化、指令集加速,以及混合 TLS 握手状态的精细化缓存管理,高频并发的抗量子 KEM 请求并未造成服务器集群 CPU 的阻塞或内存溢出。在此极限工况下,现网银建立安全通道并反显用户名的端到端响应时间优化至 3.5 ms。

在应用层双签验证环节,服务器集群通过内存池复用与多线程并发调度,将包含 ML-DSA 签名的单次验签平均耗时稳定控制在 13.639 ms。该耗时指标对前端网银用户的感官体验完全透明,表明本方案通过底层协议与系统架构调优,可将高维格密码引入的额外计算开销控制在对前端用户基本无感的水平,在本文测试环境与负载下表现出良好的工程可行性。

为对照双签机制相对单签机制在算法层的性能代价,本文在同一 x86 测试节点上测得单 SM2(SM3)验签与 SM2+ML-DSA-44 双签的算法层耗时(表 1)。由表 1 可见,引入 ML-DSA-44 后,双签相对单 SM2 的额外验签开销小于 1%、签名开销约 5%,主要原因是 ML-DSA-44 的验签(约 29.5 μs)与签名(约 72.7 μs)耗时相对 SM2 自身开销较小;在密钥封装侧,ML-

表 1 单 SM2 与 SM2+ML-DSA-44 双签的算法层耗时对比

指标	算法层耗时/μs		相对增量/%
	单SM2(SM3)	SM2+ML-DSA-44双签	
验签 p50	1002.0	1010.9	+0.9
验签 均值	1011.7	1018.7	+0.7
验签 p95	1237.9	1239.6	+0.1
签名 p50	864.8	910.0	+5.2
签名 均值	868.7	917.6	+5.6

注: p50、p95为相应分位值。

KEM-768 封装/解封装耗时均值约为 13.7/10.5 μs。以上均为算法层微基准结果。

需要说明的是,受生产环境数据披露限制,本文系统级实测结果以脱敏后的统计口径给出,时延指标按 p50、p90、p95 和 p99 分位统计,样本取自灰度期间的真实交易与极限压测。同时,本文尚未在同一系统级测试床上完成“传统 ECDHE/SM2 通道与 ECDHE+ML-KEM 混合通道”“单 SM2 验签集群与 SM2+ML-DSA 双签集群”在不同并发梯度下吞吐量、延迟、错误率与资源占用的完整对照,此类系统级对比实验列为后续工作。因此,本文结果为在特定 x86 AVX2 软件实现、ML-DSA-44/ML-KEM-768 参数集以及本文测试环境与负载下的方案设计与初步验证,不宜无条件外推至 ARM/NEON(advanced RISC machines/new enhanced operations for multimedia)等其他部署平台(如移动终端与信创服务器),相应平台的性能仍需另行专门验证。

4 结论

针对金融行业在抗量子时代面临的系统级密码换代挑战,本文提出了一种基于双签融合模式的商业银行网银全栈 PQC 迁移架构。本研究打破了此前业界仅停留在传输层或单点终端测试的局限,从硬件、协议、网络到集群验签,构建了逻辑严密、防降级攻击的端到端防御体系。

依托江苏省某商业银行的现网实证表明,该架构通过自适应调度与混合并行协议,在不改造银行核心业务引擎的前提下,实现了国密算法与 NIST PQC 标准算法的高效融合。在 1000 TPS 的高并发生产级压力下,系统在本文测试环境与负载下表现出毫秒级的响应延迟与良好的稳定性,成功实现了存量用户的平滑兼容与灰度过渡。本研究不仅为高维格密码在大型金融分布式系统中的工程化落地提供了真实的测试数据,也为中国关键金融基础设施模块化、敏捷化的抗量子安全演进提供了可供参考的工程实践案例。

参考文献(References)

[1] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM

- Review, 1999, 41(2): 303–332.
- [2] National Institute of Standards and Technology. FIPS 203: Module–Lattice–Based key–encapsulation mechanism standard[S]. Washington, D. C. : U. S. Department of Commerce, 2024.
- [3] National Institute of Standards and Technology. FIPS 204: Module–Lattice–Based digital signature standard[S]. Washington, D. C. : U. S. Department of Commerce, 2024.
- [4] Joseph D, Misoczki R, Manzano M, et al. Transitioning organizations to post-quantum cryptography[J]. *Nature*, 2022, 605(7909): 237–243.
- [5] 丁津泰, 向宏, 刘锐. 全球金融银行业抗量子安全迁移白皮书(2025)[R/OL]. 苏州: 西交利物浦大学后量子迁移交叉实验室(PQC-X), 2025 [2026–09–10]. https://www.xjtlu.edu.cn/wp-content/uploads/2025/06/Global-Financial-Banking-Post-Quantum-Security-Migration-White-Paper2025_ZH_v1.0.1.pdf.
- [6] Newhouse W, Souppaya M, Barker W, et al. Migration to post-quantum cryptography: NIST SP 1800–38A[R/OL]. Gaithersburg, MD: National Institute of Standards and Technology (NCCoE), 2023[2026–09–11]. <https://www.nccoe.nist.gov/sites/default/files/2023-04/pqc-migration-nist-sp-1800-38a-preliminary-draft.pdf>.
- [7] Barker E, Polk W. NIST Special Publication 1800–38A: Migration to Post-Quantum Cryptography[R]. Rockville, MD: National Cybersecurity Center of Excellence (NCCoE), 2023.
- [8] Bos J W, Ducas L, Kiltz E, et al. CRYSTALS–Kyber: A CCA–secure module–lattice–based KEM[C]//2018 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway, NJ: IEEE, 2018: 353–367.
- [9] Stebila D, Fluhrer S, Gueron S. Hybrid key exchange in TLS 1.3[R]. Internet Engineering Task Force (IETF), 2026[2026–09–09]. <https://www.rfc-editor.org/info/rfc9954>.
- [10] 国家密码管理局. GM/T 0038–2014 SSL VPN技术规范[S]. 北京: 中国标准出版社, 2014.
- [11] 国家密码管理局. GM/T 0003.1~0003.5–2012 SM2椭圆曲线公钥密码算法[S]. 北京: 中国标准出版社, 2012.
- [12] Paquin C, Stebila D, Tamvada G. Benchmarking post-quantum cryptography in TLS[C]//Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020. Cham: Springer, 2020: 72–91.
- [13] Seiler G. Faster AVX2 optimized NTT multiplication for Ring–LWE lattice cryptography[R]. Cryptology ePrint Archive, Report 2018/039, 2018[2026–09–09]. <https://eprint.iacr.org/2018/039>.
- [14] Ducas L, Kiltz E, Lepoint T, et al. CRYSTALS–Dilithium: A lattice–based digital signature scheme[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018, 2018(1): 238–268.

Dual–signature based quantum–resistant migration architecture and empirical study for commercial bank online banking

SHEN Kunping, LI Kunlin, PAN Jiandong

Bank of Jiangsu Co., Ltd., Nanjing 210000

Abstract To address the critical challenges faced by core online banking systems in the financial industry during post-quantum cryptographic migration—including business continuity risks, poor compatibility across massive terminal devices, and high-concurrency performance bottlenecks—this paper proposes and implements a full-stack quantum-resistant cryptographic migration architecture for large commercial banks. The architecture adopts a dual-signature fusion mechanism that combines a hybrid TLS (transport layer security) secure channel with the Chinese national cryptographic standard SM2 and the ML–DSA (module–lattice–based digital signature algorithm). This design establishes an end-to-end evolutionary path spanning from underlying hardware terminals to network transmission and further to backend cluster signature verification. Gray-scale high-fidelity validation conducted in a real online banking environment of a commercial bank demonstrates that, under a concurrent transaction pressure of 1000 TPS (transactions per second), the hybrid secure channel establishment response time is optimized to 3.5 ms, and the single signature verification latency is approximately 13.6 ms. This empirical study preliminarily validates the feasibility of high-dimensional lattice-based cryptographic algorithms under the test environment and workload described herein, providing a replicable engineering demonstration for the smooth post-quantum evolution of critical information infrastructure in China's banking sector.

Keywords post-quantum cryptographic migration; dual-signature fusion; online banking system; hybrid TLS protocol; high-concurrency verification; smooth evolution ●



(责任编辑 王志敏)