

特色专题

金融基础设施后量子迁移的模块化解耦架构

刘锐^{1,2}, 张彬³, 曾能¹

摘要 量子计算削弱传统公钥体系的安全根基,全球金融市场基础设施(financial market infrastructures, FMIs)因此加快后量子密码(post-quantum cryptography, PQC)迁移。国际清算银行(Bank for International Settlements, BIS)Leap 项目第 2 阶段的实证测试揭示了实时全额结算(real-time gross settlement, RTGS)系统转向混合加密的工程约束:原生方案不支持异构算法并行处理;端到端 PQC 验签约 209.9 ms,为传统密码 28.1 ms 的 7.5 倍。分析表明,该开销主要来自报文解析与验签软件编排等系统级环节,格运算本身并非主因。将其置于高并发结算的同步关键路径会拖低吞吐。为此本研究解耦处理链路,使升级分阶段推进:在业务应用报头构造内层 PQC、外层 RSA(Rivest-Shamir-Adleman)的嵌套签名,使存量网关无须解析 PQC 扩展块,实现零侵入接入;验签耗时以分布式事务的异步回退抵消——预结算挂起消除同步阻塞,补偿事务恢复全局一致;其上叠加异常熔断的量化监控模型。仿真表明,验签移出关键路径后结算决策延迟降至毫秒级,仅软件路径即满足传统 500 ms 监控上限;引入现场可编程门阵列(field-programmable gate array, FPGA)流水线加速(可选优化)抑制抖动后,阈值可收敛至 234 ms。三阶段演进路线的分析亦支持上述判断:解耦得当、异步编排合理,实时吞吐无须牺牲,金融核心系统即可稳步完成抗量子安全升级。

关键词 后量子密码;金融市场基础设施;Project Leap 跨国项目;事务解耦;FPGA 加速;混合签名

支付清算网络关乎全球金融稳定。不法主体利用量子算力实施“先截获、后破解”(harvest now, decrypt later, HNDL)的攻击正由理论走向现实^[1-2],而金融衍生数据通常须满足数十年的合规机密性要求。如何在现役系统中低成本叠加抗量子能力,成为行业亟待解决的过渡难题^[3-4]。国际清算银行(Bank for International Settlements, BIS)创新枢纽主导的 Project Leap,是当前金融系统抗量子化改造的代表性跨国项目。在意大利银行与 SWIFT(Society for World-

wide Interbank Financial Telecommunication)等机构协作下^[5],其第 1 阶段已验证跨系统混合加密可行,确认支付报文机密性保护可抵御量子威胁。第 2 阶段推进到生产级欧元 T2 实时全额结算系统时,传统 IT 设施对后量子密码(post-quantum cryptography, PQC)的不适配随之显现。该阶段把报文中的 RSA(Rivest-Shamir-Adleman)数字签名替换为 CRYSTALS-Dilithium 算法^[6];基础功能虽可运行,但把单算法校验升为并行混合校验,会在底层网关引发互操作性与性能瓶颈。

Project Leap 的扩展测试表明,将 PQC 算法嵌入 ISO 20022 标准报文体系具备可行性^[5];但同批测试也揭示,现役金融市场基础设施若要切换至混合加密,存在如下 3 项难以回避的技术障碍^[5,7]。

1. 西交利物浦大学后量子迁移交叉实验室(PQC-X),苏州 215123
2. 苏州朗空后量子科技有限公司,苏州 215021
3. 云钞金融服务(北京)有限公司,北京 102300

收稿日期:2026-05-12;修回日期:2026-07-24

作者简介:刘锐,硕士,研究方向为后量子计算迁移,电子邮箱:Ruiliu.PT@xjtlu.edu.cn

引用格式:刘锐,张彬,曾能.金融基础设施后量子迁移的模块化解耦架构[J].科技导报,2026,44(16):96-106;doi:10.3981/j.issn.1000-7857.2026.05.00056

1) 组件方案高度固化。现役多数签名验证系统(signature verification system, SVS)早期即将算法硬编码,处理业务应用报头(business application header, BAH)时仅支持单一算法,无法在同一报文空间内并发完成 RSA 与 PQC 鉴权。

2) 协议跨层导致验证逻辑冲突。以欧元单一市场基础设施网关(Eurosystem single market infrastructure gateway, ESMIG)为例:BAH 已嵌入 PQC 认证,外层数据交换协议(data exchange protocol, DEP)却仍封装 RSA;2 套签名无法对应,底层组件即陷入死锁,机构陷入推倒重建或维持现状的两难。

3) 验签拖慢吞吐。Project Leap 报告实测 PQC 验签约 209.9 ms,为传统密码 28.1 ms 的 7.5 倍;Project Leap 归因于后量子算法的高计算复杂度,但本文微基准表明 Dilithium 单次验签实为微秒量级,开销主要来自验签软件编排与系统级处理而非格运算。将这段以百毫秒计的验签置于实时全额结算(real-time gross settlement, RTGS)同步链路,清算引擎单次可并发处理的交易量将大幅下降。

针对上述方案冲突与算力占用,本研究将系统划分为若干各司其职的模块,在保障过渡平稳的同时支撑生产级稳定性。以下从架构、性能与监控 3 方面论述。

1) 架构层面,本文采用嵌套签名结构:内层由 PQC 算法承担抗量子保护,外层以 RSA 封装。经此封装,传统网关在混合鉴权时的逻辑死锁得以规避,现有拓扑无须改动核心代码即可接收携带 PQC 载荷的报文。

2) 性能层面,本文引入由分布式控制层调度的异步回退策略:在结算主路径前置一条预挂起指令,将动辄数百毫秒的安全校验从同步阻塞队列剥离,转由独立通道执行;底层引擎即便面对高开销 PQC 验签,峰值吞吐仍可支撑。

3) 监控层面,本文构建动态熔断模型,依据验签耗时的概率分布,对迁移中超时阈值的设定位置与行级锁的保护粒度作出量化判定,避免凭主观经验拍定。

1 研究综述

已有研究集中于 3 个方向:加密敏捷性作为后量

子迁移的前置能力;混合签名主流构造的工程取舍;国内金融基础设施的后量子迁移进展。

1.1 加密敏捷性的前置地位

向量子安全过渡阶段,国际密码学界与安全厂商已把加密敏捷性(cryptographic agility)视为评价替代方案的重要前提^[8],现有迁移路径普遍采用混合密码方案(hybrid cryptography)^[9-11]。美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)等即为一例:推进 PQC 标准的同时保留 RSA/ECC 等经典算法与抗量子机制并行,用双重保险对冲后量子算法所依赖的新数学难题尚未经长期密码分析检验、可能失效的风险^[6,12-13]。

1.2 混合签名构造的工程瓶颈

异构联合签名通常分 2 类。一是串行拼接(concatenation),在同一报文并列附加 2 套签名,实现简单,但载荷增大且易与存量金融网关的单链验证逻辑冲突。二是嵌套封装(nesting),把 A 算法签名作为 B 算法承载体,逻辑隔离较好,但在旧版 SVS 上会增加解析时延并挤占资源;混合密钥交换与 TLS(transport layer security)握手重构的工程代价已有实践^[14-16]。本文的模块化解耦正是为化解嵌套方案在金融核心区的算力与校验矛盾而做的重构。

1.3 公钥基础设施研究

公钥基础设施(public key infrastructure, PKI)层面,Bindel 等^[17]与 Kampanakis 等^[18]讨论抗量子 PKI 过渡与后量子 X.509 证书可行性,但关注证书与信任锚迁移,未触及实时结算的验签时延;传输层面,Stebila 等^[16]与 Schwabe 等^[15]给出 TLS 1.3 的混合密钥交换与无握手签名,重心在链路保密。本文把嵌套混合签名与异步事务编排捆在一起,让验签离开结算关键路径;针对 ISO 20022/ESMIG 的存量约束做到零侵入接入;并给出由敞口与抖动驱动的量化熔断模型——面向 RTGS 生产环境的工程方案,而非密码协议设计。

2 存量支付网络向混合签名过渡的瓶颈

梳理近期公布的基准测试数据^[5]可见,以 T2 系统为代表的现役核心枢纽在抗量子转换中,底层拓扑与算法融合两头难以兼顾(表 1)。

表 1 RTGS 系统中传统加密方案与 PQC 迁移需求的关键瓶颈对比

比较维度	传统架构(RSA/ECC)	后量子迁移需求(PQC/ML-DSA)	性能/架构冲突点
平均验证延迟	<10 ms(估算)	约209.9 ms	延迟增加超过1个数量级,威胁吞吐量
签名校验逻辑	单一算法串行校验	异构混合签名并行校验	现有SVS设计过于僵化,无法并行处理
网关协议支持	固定DEP层核验	BAH层嵌套PQC扩展块	ESMIG无法同时开启异构核验,面临不兼容风险
计算确定性	抖动较小	计算抖动 σ 较高	高抖动导致资源锁定时间长,增加死锁风险

注:表中数据依据BIS Project Leap第2阶段报告整理,ML-DSA为FIPS 204标准化的格基签名算法。

1) 鉴权组件的硬编码约束。SVS 的底层配置往往结构刚性很强。项目观测报告显示,这类部件处理 BAH 时默认只走单通道算法解析,同一报文上并行调用 RSA 与 PQC 双重签名的路径就被堵死。

2) 跨层协议的网关排异。以 ESMIG 为代表的重型基础设施处理跨层协议混合时并不兼容:当底层 DEP 维持 RSA 鉴权、上层 BAH 置入 PQC 载荷时,网关主进程易陷入识别死锁。这一约束在前期实验中难以回避,故只得在旁路部署独立软件模块,以剥离并处理 PQC 验签。

3) 计算开销对吞吐的抑制。端到端看,Project Leap 第 2 阶段将 RSA 签名替换为 CRYSTALS-Dilithium 后实测 PQC 验签约 209.9 ms,约为传统密码 28.1 ms 的 7.5 倍^[5]。Leap 归因于后量子算法的计算复杂度,但本文的微基准显示,ML-DSA-87 单次验签中位约 0.71 ms(AVX2 优化下降至约 53 μ s)、格运算不足端到端耗时的 1%,可见该数字主要源自 ISO 20022 报文解析与厂商验签软件编排等系统级环节。当这段以百毫秒计的验签嵌入 RTGS 同步关键路径时,清算引擎峰值吞吐将大幅下降。由此需在指令预处理与账簿最终确权之间前置一个可原子化提交的回退机制,以消化验签耗时引发的阻塞。

3 面向解耦演进的混合签名架构设计

针对上述结构性死锁,本文的解耦思路是不触动存量系统,而在其旁侧增设增量模块,逐步承接原系统的处理职能,构成一套模块化过渡方案。

3.1 纵深嵌套与报文收敛

BAH 采用向内聚拢的嵌套机制:底层先用 PQC 算法(以 CRYSTALS-Dilithium^[6]为主)确立报文抗量子属性,最外层再叠加标准 RSA 二次封装。这种

PQC 居内、经典公钥居外的布局不影响现网节点解析,又搭起异构复合防线^[11]。安全性分 2 层:通用量子计算达临界能力前,外层 RSA 足以满足金融合规对身份溯源与防抵赖的要求;即便日后攻击者借 Shor 算法攻破外层 RSA,内层抗量子核心(如 ML-DSA 签名)仍能独立保护,HNDL 威胁随之消除^[1]。报文膨胀须盯紧:后量子签名体积偏大,CRYSTALS-Dilithium2 约 2420 字节、近 RSA-2048 的 10 倍,简单叠加会让单条 ISO 20022^[19]指令显著膨胀,可能撞上核心路由器与边界网关的最大传输单元(maximum transmission unit, MTU)上限,引发传输控制协议(transmission control protocol, TCP)分片与重传。方案因此在传输侧压缩:削减 BAH 中非必要扩展元数据,并要求核心网关主干通信改用 ASN.1 或紧凑型可扩展标记语言(extensible markup language, XML)等二进制流规范,把冗余压回标准以太网 MTU 内。

DEP 层的加密隧穿:跨越网络服务边界时,新增的 New NSP 节点在常规公钥封包之外叠加抗量子鉴权,并启用 PQC KEM(key encapsulation mechanism)机制(如 ML-KEM^[12])建立安全隧道;该阶段以签名校验加信封加密 2 道叠加,避开单点组件识别失效的风险(图 1)。

3.2 链路隔离与异步验证

本研究重新界定网络防御组件的处理边界,让验证沿非侵入路径解耦:数据先由 New NSP 节点注入后量子标识并完成密文封装,到对端再由 New ESMIG 预处理集群逆向解封;存量 ESMIG 只核验其原生 RSA 标签,真正决定抗量子级别的解密运算全部分流到末端枢纽节点 PQC-SVS(图 2)。

始发侧由新型网络服务提供节点(new network service provider, New NSP)承担边缘服务延伸,部署在网络边界外侧,截获已加盖标准密钥封装的数据

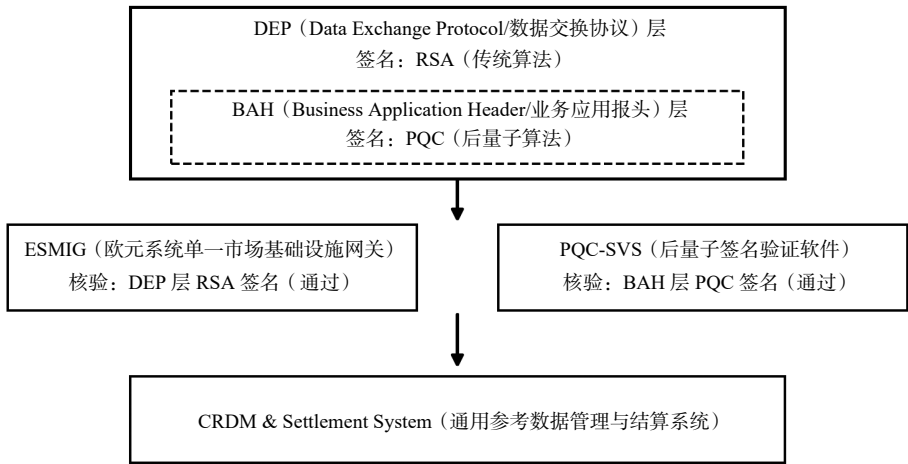


图1 报文嵌套签名与各节点分层验证结构示意图



图2 建议的模块化解耦验证路径与报文结构全景

包,再叠加抗量子签名与 KEM 信封,为出站链路建立抗量子隧道。

入站侧由 New ESMIG 承担前置隔离,把守第 1 道关口,识别并剥离 KEM 隧道封装层,核对外层加

密参数,把无有效抗量子授信的异常流量挡在核心网段之外。

存量核心网关(Eurosystem single market infrastructure gateway, ESMIG)属于不作改动的存量设施,照原有规则运行,只校验 DEP 传输层与 BAH 外层暴露的常规 RSA 标识。

3.2.1 验证与协同控制枢纽(post-quantum cryptography signature verification system, PQC-SVS)

PQC-SVS 位于账簿结算系统前端,是本方案的调度核心。为撑住高并发,由现场可编程门阵列(field-programmable gate array, FPGA)搭建的加速单元集成在节点内部,在单个原子事务周期内并行提取内层后量子负载;金融级部署要求 FPGA 板卡与软件调度面保持亚毫秒级热备:一旦硬件降速或停机,调度集群即经冗余降级通道退回纯软件栈,并依托共识机制维持全局事务标识与验签进度的一致映射,使预入账指令不至假死。为把约 209.9 ms 的 PQC 验证耗时移出同步关键路径,该枢纽向 RTGS 核心发送多阶段协同信令,按以下时序异步推进。

步骤 S_1 (报文传送):前置存量网关 ESMIG 将含 PQC 扩展字段的 ISO 20022 报文安全传送至协同枢纽 PQC-SVS。

步骤 S_2 (状态预锁定):PQC-SVS 向 RTGS 核心发出预判指令;RTGS 核心先做金额预扣或行级锁定,把该笔交易标记为挂起待审(pending)。

步骤 S_3 (验签抽离):协同枢纽调用旁路加速资源,单独跑 ML-DSA 多项式验签;按 Project Leap 公

布的算力评估约耗时 210 ms^[5],该验签脱离同步主路径,给 RTGS 核心腾出处理其他高并发订单的空间。

步骤 S_{4a}(校验通过):验签通过后 PQC-SVS 向 RTGS 核心下发成功回调(success callback),RTGS 核心随即唤醒预扣日志、执行数据库 Commit,资产确权完成。

步骤 S_{4b}(回滚防御):一旦检测到验签异常或签名伪造,PQC-SVS 熔断器以最高优先级下发阻断信令;RTGS 核心据先前快照原子化回退额度限制,并生成逆向补账流水。

3.2.2 解耦原理下的性能重构

高阶后量子算法带来约 200 ms 延迟,本方案不靠算力堆叠,而以事务级逻辑的拆分与重排恢复性能,可从 3 个层面理解。

1) 解除同步验证阻塞:传统方案中结算指令须原地等待安全握手返回,并发上限受制于最慢的加密环节;经专属协同控制层(PQC-SVS)解耦后,结算主路径与冗长验签不再强耦合。

2) 乐观预处理。借鉴原子提交(两阶段提交)控制理论^[20],使结算主库在验签正式启动前即完成前置抢占,将约 200 ms 耗时折叠进准备阶段的后台时间轴。

3) 反向补偿维系全局一致性。旁路一旦识别出安全问题,PQC-SVS 在极短时间内下发补偿回执,撤销尚未处理的挂起单据,账本最终状态保持一致(完

整协同时序见图 3)。

3.3 容错与鲁棒性保障

高并发分布式拓扑中,只走理想路径(happy path)保不住生产级稳定。异常处理的核心是控制预挂起期间的资金暴露、守住账本强一致性,需重点拦截的极限工况如下。

场景 A(校验逻辑失效):并行引擎一旦发现签名被篡改、算法握手失败或证书链过期,PQC-SVS 即越过常规时序,向 RTGS 核心下发高优先级回滚。RTGS 核心据此提取被锁定的全局事务 ID 强制干预挂起流水;补偿事务执行后资金排他锁解除,交易状态由 pending 修正为 rejected,并写入审计冲正记录以备追溯。

场景 B(超时熔断与量化界限):受局部网络衰减或瞬时算力竞争影响,PQC 运算周期可能间歇性超过约 209.9 ms 均值。当结算主库发现某挂起事件超过监控上限(限制时段 $T > 500$ ms)时,后台引擎放弃等待并触发保护性熔断,将该交易判为异常并启动资源回退,避免个别长尾异常引发大面积队列崩溃。

针对此看门狗(Watchdog)临界值的量化核心,是在高吞吐与安全完整性之间取得平衡。为确保超过 99% 的合法交易不受算力抖动误判,阈值设定遵循不等式约束

$$T_{\text{timeout}} \geq E[T_{\text{pqc}}] + 2T_{\text{RTT}} + k \cdot \sigma$$

式中, T_{timeout} 为看门狗超时阈值; $E[T_{\text{pqc}}]$ 、 $2T_{\text{RTT}}$ 分别对

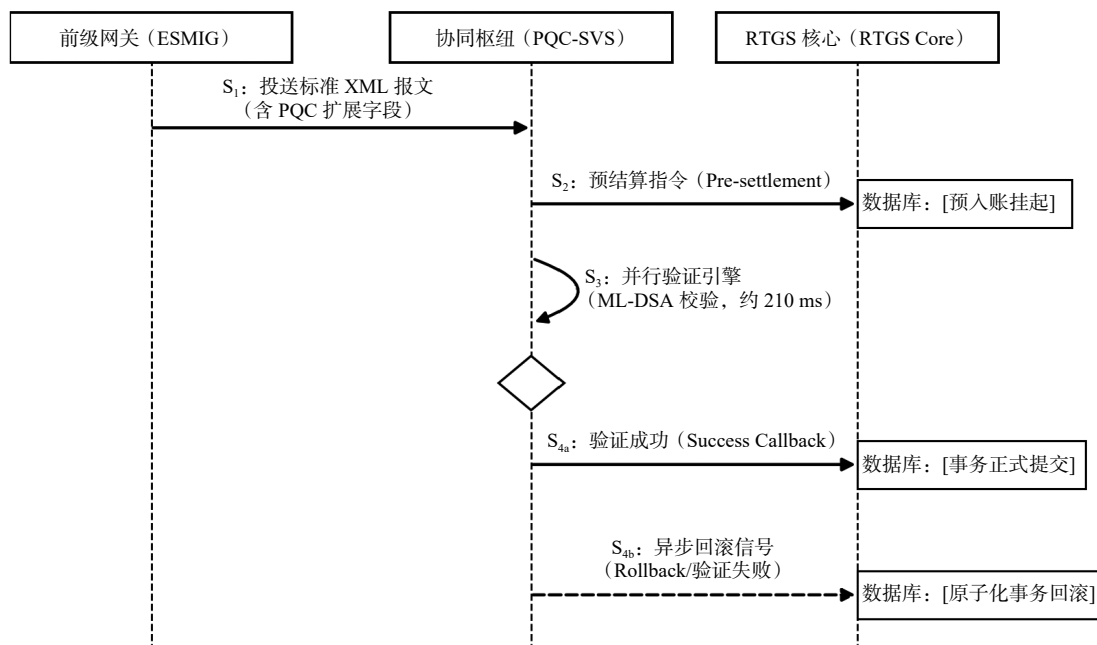


图 3 预结算—异步验证—补偿回滚协同时序(S₁—S_{4b})

应算法验证的统计期望耗时($E[\cdot]$ 表示数学期望,本研究取基准 210 ms)、预授信与确认共 2 次往返信令的物理时延(专用金融骨干网内单次往返不超过 10 ms);由安全系数 k 与标准差 σ 构成的乘积项 $k\cdot\sigma$ 用于吸收中央处理器(central processing unit, CPU)时序波动。

工程测算表明,参数选取主要取决于机构承诺的金融级服务等级协定(service-level agreement, SLA)。若计算抖动近似正态分布,将参数取至 3σ 基本已覆盖 99.7% 的极端工况。需说明,纯软件路径下单次验签已处于亚毫秒至毫秒量级,本身即满足传统 500 ms 监控上限(详见本文第 5 部分的实测与配套成本模型);FPGA 仅为可选优化——协同枢纽引入 FPGA 流水线加速单元后,预期可将抖动离散度降为原来的约 1/40,据此可把监控阈值由 500 ms 收紧至 234 ms 以内。即使采用 500 ms 宽限值,也已为密码解析储备超过 1 倍的冗余安全边界($500\text{ ms}>2T_{\text{pqc}}$),并使系统在物理宕机时能在半秒内释放核心账本资源。

场景 C 与场景 D(信令孤岛与硬件故障):当 PQC-SVS 已裁决却因网络丢包未送达 RTGS 核心时(场景 C),由后台异步对账引擎接管——主库周期性激

活状态清理任务,轮询挂起队列,据定点探询的最新状态强制推进提交或原子化撤销。若协同枢纽在高负载下板卡损坏或内核崩溃(场景 D),则由断点恢复机制处理:备用节点或原进程恢复后,绕过业务总线读取本地固化的预写日志,重建验证参数,再向 RTGS 核心补发宕机期间未发的状态指令。

3.4 2 种方案的对比

本文模块化解耦方案与 Project Leap 第 2 阶段实验方案的定性对比见表 2,涵盖平均验证延迟、签名校验逻辑、网关协议支持与计算确定性等维度。表 3 从量化性能与工程指标 2 个方面比较,检验本方案的实际成效。

以上对照表明,传统直连网关无法承载此类算力密集的密码迭代:Project Leap 虽在沙箱打通功能链路,但 ML-DSA 的格代数运算引入约 209.9 ms 延迟,若直接嵌入 RTGS 主链路,以毫秒级实时性为基础的清算枢纽吞吐将立即受限。

相较而言,本文方案在底层设计与物理算力 2 个方面均给出相应对策。业务逻辑上,基于先挂起后追认的异步回滚,将居主导的漫长安全校验移出核心排队队列,使主链路上 200 余毫秒的等待缩减为接近于

表 2 Project Leap 实验方案与模块化解耦演进方案的深度对比

比较维度	Project Leap第2阶段实验方案	本研究提出的模块化演进方案
业务层	单一算法替换:受配置约束仅接纳单一算法验证,须舍弃并行,仅测单一PQC签名	嵌套混合式签名:BAH层实现PQC与RSA嵌套,兼顾抗量子安全与传统数据完整性
传输层(DEP)	单一算法维持:报文仅在BAH层加PQC签名,DEP信封与出站流量仍仅用RSA	双重混合封装与加密:NSP加RSA签名后,New NSP再加PQC签名并做PQC KEM封装,健全链路抗量子隧道;New ESMIG负责解封
并行验证能力	不可取(not feasible):BIS报告表明当前配置无法并行验证传统与PQC签名,陷入僵局	并行验证机制:协同枢纽配并行引擎,在同一原子操作内并行提取并验证异构双签名,破解死锁
防御深度	单一防御:仅业务报文头抗量子,外层封装仍可能被量子计算机拦截	纵深防御(认证+机密):业务层签名核验身份、传输层PQC KEM加密保机密,抵御先拦截后解密
性能平衡机制	同步阻塞:PQC验证使延迟升至209.9 ms,易引发TPS瓶颈与结算排队	异步回滚防护:预入账挂起+异步验证+事务回滚,吞吐无损,维持RTGS实时性
验证架构逻辑	双路径分流(bypass):进站流量被强制分成传统与PQC 2条独立验证分支,缺乏系统规划	线性解耦验证(layered):新增功能节点按嵌套次序逐层剥离验签,流水线式解耦编排
核心网关影响	需实质性演变:ESMIG无法直接处理异构算法,混合化须对整个系统重建	零干扰防护:New ESMIG解除KEM封装,Legacy ESMIG仅处理原生RSA,全部PQC计算由新增独立节点承担,无须改动核心设施
加密敏捷性	偏低:受配置与供应商版本制约,难在不更新全系统的前提下快速适配多算法并存	极高:新增节点以独立模块运行,可灵活迭代算法或适配国密,快速响应量子威胁变化
演进与工程模式	功能实验性验证:主要在受限环境验证PQC算法集成进ISO 20022报文的基本可行性	新增、替代演进:支持混合双轨平稳过渡到纯PQC,含物理节点移除、信任锚迁移与路径重定向(图4)

注:国密指由国家密码管理部门发布、面向中国境内商用领域的自主可控密码算法体系,以SM2、SM3、SM4、SM9等系列算法为代表。

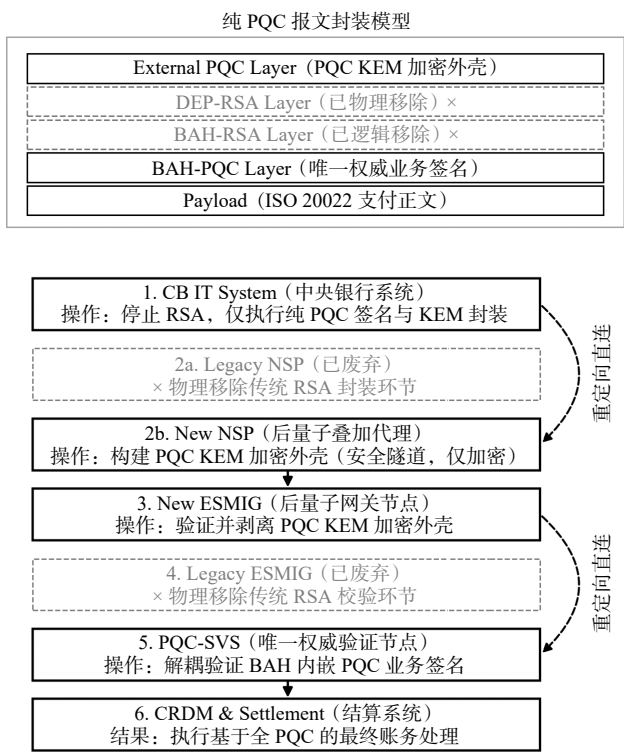


图 4 全量子归一与冗余设施退役的演进示意

零的信令派发时间(仅受限于纳秒级光纤传输),基本消除新旧方案的速率差异。算力与抖动上,若在前端部署 FPGA 流处理单元阵列,预期可把运算峰值控制在毫秒级、将验签计算偏移量 σ 压低为原来的约 1/40,据量化模型把超时容限从 500 ms 收紧至 234 ms 以内,缓解数据库锁资源负荷;在该设计下,面对每秒千笔(1000+transactions per second, TPS)量级的并发高峰,全链路仍可凭异步回滚维持账务一致闭环。可见 Project Leap 侧重验证功能可行性,本研究则通过底层

解耦与算力编排 2 个方面的协同设计,说明大型金融系统如何在不降低处理速度的前提下完成迁移。

4 面向全球金融生态的渐进式演进路径

面向重型金融网络的抗量子切换,路径是先以外挂增量模块承接新功能并辅以仿真验证,待时机合适再剥离存量设施完成更替。这条路径非侵入、可热插拔,既能化解欧洲 T2 主干网前期的验证互斥,又因兼容异构体系而有望融入包括中国在内各区域的金融核心系统^[7,9]。

4.1 双轨期旁路共存

过渡初期,实施方不动现役 NSP 总线、ESMIG 网桥与存量鉴权集群,只按格密码与经典公钥的嵌套顺序,在边缘区域增设承担解析的新节点。这样可避免传统硬编码软件遇双重签名死锁:存量设施把嵌入的 PQC 载荷视为透明、不作解析,仍按常规校验最外层 RSA 封装,代码与拓扑均低摩擦接入。异步控制让复杂验签交出对结算主路径的控制权,系统实时承载上限不再与 209.9 ms 验签时延强相关,即便新旧并轨期也能维持与升级前相当的处理能力。

4.2 全量子化归一与设施退役

新增节点经真实生产流量验证、指标稳定后,迁移进入收尾:新增节点逐步接管存量设备的 RSA 校验职能,直至完全掌控链路。迁移接近完成时,资金发起方停止签发旧式签名,报文不再嵌套、转为单一抗量子加密单元,传输带宽随之下降。时机成熟后,

表 3 本研究方案与 Project Leap 第 2 阶段实验方案的量化性能与工程指标对比

评估维度	Project Leap第2阶段方案	本研究方案(模块化解耦)	优化效益/工程价值
结算主路径延迟	约209.9 ms(同步阻塞模式)	<10 ms(验签移出关键路径)	延迟降低超过95%,满足实时结算需求
系统吞吐量(TPS)	严重退化(受限于PQC验证耗时)	生产级维持(异步回滚保护机制)	实现后量子迁移下的“性能对等”
核心网关侵入度	高(需实质性重新开发ESMIG)	零侵入(通过New NSP/ESMIG节点外挂)	极大地降低了存量设施的迁移风险与成本
计算确定性(σ)	抖动较大(纯软件模拟执行)	高(软件即达标, FPGA为可选优化)	抖动有望降低约40倍(设计预期),确保系统稳定性
安全防御深度	单层防御(仅BAH签名)	纵深防御(BAH嵌套签名+DEP KEM加密)	有效抵御HNDL威胁
监控阈值(T_{timeout})	需>500 ms(容忍软件计算抖动)	可收紧至<50 ms (受益于抖动抑制,设计预期)	降低数据库行级锁竞争,提升并发能力

注: Project Leap数据依据其第2阶段报告;本研究数据来源于第5章节实验与验证, σ 为验签耗时标准差, T_{timeout} 为Watchdog超时阈值。

运维中心可将仅具兼容职能的存量网关(legacy ESMIG)与旧网络服务部件纳入物理下线或逻辑隔离清单。

迁移完成后,节点间数据连接整体置于新一代PQC KEM 构建的抗量子防护层之下。信任锚代际迁移须谨慎,建议同时部署双根信任(dual-root)体系^[17-18];拆除旧 ESMIG 网关的时机,取决于全网确认所有机构均已挂载新信任链,且证书吊销列表(certificate revocation list, CRL)与在线证书状态协议(online certificate status protocol, OCSP)一致性通过审计,否则贸然切换可能引发系统级失联。需特别指出,无论架构如何精简,依靠异步回滚保障吞吐的机制不可弃用:后量子算法的高计算开销不会因架构收敛而消失,一旦缺失事务补偿,金融核心仍无法承受生产环境的高负载冲击。

5 实验与验证

本研究在统一平台上构建并运行该架构,考察有效性、实时性与稳定性。关注 3 点:嵌套后报文是否突破以太网 MTU、超出同步链路上限;嵌套结构面对对抗输入能否被识别并拒绝;单次嵌套签名/验签的耗时分布。为排除单一平台偶然因素,另在其他平台对密码学原语复测。环境为 x86-64 Ubuntu 22.04 云虚拟机(2 vCPU)与 Windows 10 桌面端(MSVC v142, Release|x64),密码学实现采用自带原生 RSA、不依赖 OpenSSL 的 LK LEGO PQC 库。用例覆盖 64 B 至 1 MB 的 5 档 BAH 负载,在 3 处篡改位置各做 1000 次随机位翻转,运行 200 次嵌套 sign+verify 循环;每组先热身 5 次,密钥与随机种子固定,结果可复现。下文 Bench A—C 依次给出报文尺寸敏感性、篡改鲁棒性与阶段耗时分解。

5.1 报文大小敏感性(Bench A)

ISO 20022 实际报文从约 1 KB(典型转账)到 1 MB(大型批处理),跨 4 个数量级。为确认嵌套签名在全跨度下不击穿网关 MTU 假设,对 5 档典型 BAH 负载逐档实测端到端验签延迟、报文传输总字节与标准以太网(MTU=1500)下所需 TCP 分片数(表 4)。嵌套验签延迟在 64 B 至 1 MB 内基本平稳(中位约 540 μs),与负载大小无关——ML-DSA 与 RSA 验签代价只取决于签名长度而非报文长度,仅摘要阶段随报文线性

变化、占比不足 1%。1 MB 负载即便产生 722 个分片,也仍在生产 RTGS 网卡常规处理能力之内;启用 Jumbo Frame(MTU=9000)后降至约 120。

表 4 嵌套 PQC-RSA 签名在不同 BAH 负载下的工程指标

负载/B	嵌套验签 耗时/μs	报文传输 总字节/B	标准以太网 (MTU=1500)下 TCP分片数
64	622	5 035	4
1 K	552	5 995	5
10 K	529	15 211	11
100 K	550	107 371	74
1 M	541	1 053 547	722

注:数据来源于本文实测(LK LEGO PQC 平台,x86-64 Ubuntu 22.04, 2 vCPU),分片数按标准以太网(MTU=1500)估算。

5.2 篡改鲁棒性矩阵(Bench B)

工业部署中验签器要对抗大量来自网络的位错与对抗输入。为量化嵌套结构的拒识能力,对内层 Dilithium-5 签名、外层 RSA-2048 签名、报文摘要 3 处各施加 1000 次随机位翻转,结果见表 5;3 处共 3000 次扰动全部 100% 被正确拒识、零误受,未扰动基线则 1/1 被正确接受。可见嵌套结构具备双层独立失效的可靠性——任一层被破坏都会被另一层验签门挡下,符合 EUF-CMA 强组合子设计目标。

表 5 嵌套验签拒识矩阵(每个篡改位置 1000 次随机位翻转)

篡改位置	试验数/次拒识数/次误受数/次拒识率/%			
内层Dilithium-5签名	1000	1000	0	100.0
外层RSA-2048签名	1000	1000	0	100.0
报文摘要(Hash)	1000	1000	0	100.0
未篡改对照(基线)	1	0	1	0

注:数据来源于本文实测,每个篡改位置施加1000次随机位翻转。

5.3 协议阶段耗时分解(Bench C)

相对于并置(concatenation),嵌套签名的工程优势在于外层 RSA 验签充当快速门控,内层 ML-DSA 仅在外层通过后才执行。为量化该门控,将单次嵌套 sign+verify 循环分解为 7 个阶段计时(表 6):外层 RSA 验签仅占 2.5%(63.6 μs),是开销极低的预过滤,一旦判失败,41.8% 的内层 ML-DSA 签名与 20.1% 的内层 ML-DSA 验签即可全部规避。换言之,面对

表 6 单次嵌套 sign+verify 循环的 7 阶段耗时分解
(mean of 200)

阶段	名称	嵌套验签耗时均值/s	占比/%
1	内层 SHA-256 摘要	1.9	0.1
2	内层 ML-DSA-87 签名	1076.9	41.8
3	外层负载拼装(memcpy)	0.2	0
4	外层 SHA-256 摘要	31.5	1.2
5	外层 RSA-2048 签名	883.5	34.3
6	外层 RSA-2048 验签(门)	63.6	2.5
7	内层 ML-DSA-87 验签	517.0	20.1
合计	单次 sign+verify 循环	2 574.7	100

注:数据来源于本文实测(单次嵌套 sign+verify 循环,200 次均值,LK LEGO PQC 平台)。

被篡改的外层签名,验证器在 64 μ s 内即可拒识,无须进入耗时的内层路径——此即嵌套相对并置的关键效率优势。

5.4 跨平台 AVX2 实证:KEM 与签名

前述 Linux 云虚拟机平台(Ubuntu 22.04, 2 vCPU 共享)上 Dilithium-5 中位约 706 μ s,其中或含平台偏置。为排除该因素,本研究在 Windows 10 桌面端(MSVC v142, Release|x64, 启用 AVX2 优化)上,采用同一份 LK LEGO 代码库对 KEM 与签名原语性能进行独立复测。

KEM 端每项测量 1000 次迭代。ML-KEM-512/768/1024 封装中位 6.7/8.6/11.8 μ s,解封装中位 5.9/8.5/11.3 μ s, p99(99 分位)全部 $\leq$ 20 μ s;单核 3 s 紧密循环可持续 87384/56488/39012 封装-解封装对/秒。签名端每项 500 次迭代,ML-DSA-44/65/87 密钥对生成(keypair)中位 27.0/36.4/54.5 μ s,签名(sign)中位 58.2/73.2/78.6 μ s,验签(verify)中位 28.1/36.6/52.7 μ s,验签 p99 $\leq$ 107 μ s,单核验签吞吐 42554/27161/17177 次/s。18 个 KEM 配置与 12 个 Dilithium 配置的功能正确性零错误通过。可见 PQC 验签的密码学内核在优化构建下只需数十微秒(ML-DSA-87 约 53 μ s),这与上文判断一致:Project Leap 报告的 209.9 ms 来自协议外壳^[21]——报文解析、验签软件编排,而非格运算本身。本文实验验证了所提架构的有效性、实时性与稳定性;完整的协议级可复现测试床,含多容器部署、网络整形与故障注入,留待另文讨论。

6 国密融合可行性与局限性分析

1) 国密融合与本土化部署。本架构抗量子能力来自模块化新增节点与算法解耦,便于与中国商用密码体系融合;中国在后量子迁移的顶层规划、技术储备与标准化方面已有系统性进展^[22]。工程上,New NSP/New ESMIG 与 PQC-SVS 的相应职能均可改由或并行由国密算法承担:外层签名与密钥交换用 SM2^[23],报文摘要用 SM3^[24],会话对称加密用 SM4,需标识密码时引入 SM9^[25]。该方案符合《商用密码管理条例》^[26]与《中华人民共和国密码法》^[27]对关键信息基础设施使用商用密码的要求,也契合《金融科技发展规划(2022—2025 年)》^[28]的安全可控导向。ML-KEM/ML-DSA 与国密可在双根信任下并行部署,待国家后量子标准发布后再切换。

2) 方案局限性。本方案在工程落地中仍有 2 个局限。一是报文体积膨胀:嵌套签名与 PQC KEM 封装增大报文,大批量场景下对带宽与 MTU 要求更高,须配合元数据削减与二进制编码优化,必要时启用巨帧(jumbo frame)。二是异步对账复杂度上升:预授信——异步验签——补偿回滚引入挂起态与对账流程,对幂等性、事务标识一致性与对账时延要求更高;混合双轨期还要同时维护存量 RSA 链路与新增 PQC 节点,存在双重开销。这些问题可分别由载荷压缩、对账引擎幂等化、状态可观测性增强与灰度切换缓解。

7 结论

现役金融核心系统在适配 PQC 标准时频频受阻,本文即以此为研究对象,取 Project Leap 公开实测数据加以解析,厘清 RTGS 引擎在并行校验多算法签名时陷入死锁、吞吐下降的成因,并将模块化解耦与异步阻断相衔接,为国际清算网络的抗量子迁移提出一条既规避算力开销、又无需改动存量代码的路径。

落实到工程层面,该方案具备 3 方面成效:其一,嵌套组合签名把抗量子保护置于业务流之外,存量驱动无须改动一行代码即可接入;其二(更关键)在事务调度层,不执着于单一算法极限优化,而借指令预抢占与后台补偿冲正,将约 200 ms 的验签开销自主链路剥离;其三,为超时熔断划定有数学依据的量化界

限,再辅以 FPGA 流水线加速,即便高并发涌入,响应波动亦可稳定于毫秒级。

后续仍有若干工作:一是构建端到端的加密敏捷(cryptographic agility)分发网络,使网关能依据实时负载自主切换抗量子组件参数;二是深入硬件指令集,在 RISC-V 开源架构上设计专司格代数运算的单元,提升格签名在边缘节点的能效;三是跨法域协同,即如何推动双轨并行阶段有序收敛至纯后量子体系,尚待标准化握手协议与联合操作规范完善。

参考文献(References)

- [1] Mosca M. Cybersecurity in an era with quantum computers: Will we be ready?[J]. *IEEE Security & Privacy*, 2018, 16(5): 38–41.
- [2] Cybersecurity and Infrastructure Security Agency, National Security Agency, National Institute of Standards and Technology. Quantum-readiness: Migration to post-quantum cryptography[EB/OL]. [2026-06-15]. <https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography>.
- [3] Bank for International Settlements. Quantum-readiness for the financial system: A roadmap[EB/OL]. [2026-06-15]. <https://www.bis.org/publ/bppdf/bispap158.pdf>.
- [4] World Economic Forum (WEF). Transitioning to a quantum-secure economy[R]. Geneva: WEF, 2022.
- [5] Bank for International Settlements Innovation Hub, Eurosystem. Project Leap phase 2: quantum-proofing payment systems[R/OL]. 2026-06-15. <https://www.bis.org/publ/othp107.htm>.
- [6] National Institute of Standards and Technology (NIST). Module-lattice-based digital signature standard: FIPS 204[S]. Gaithersburg: NIST, 2024.
- [7] Hasan K F, Simpson L, Ali Rezazadeh Bae M, et al. A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies[J]. *IEEE Access*, 2024, 12: 23427–23450.
- [8] FS-ISAC Post-Quantum Cryptography Working Group. Building cryptographic agility in the financial sector[EB/OL]. [2026-06-15]. <https://www.fsisac.com/pqc-crypto-agility>.
- [9] European Telecommunications Standards Institute (ETSI). CYBER: Migration strategies and recommendations to quantum safe schemes: ETSI TR 103 619[R]. Sophia Antipolis: ETSI, 2020.
- [10] European Union Agency for Cybersecurity (ENISA). Post-quantum cryptography: Current state and quantum mitigation[EB/OL]. [2026-06-15]. <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>.
- [11] Giron A A. Migrating applications to post-quantum cryptography: Beyond algorithm replacement[C]//Proceedings of the 20th International Conference on Security and Cryptography. Setúbal: SCITEPRESS-Science and Technology Publications, 2023: 857–862.
- [12] National Institute of Standards and Technology (NIST). Module-lattice-based key-encapsulation mechanism standard: FIPS 203[S]. Gaithersburg: NIST, 2024.
- [13] Federal Office for Information Security (BSI). Cryptographic mechanisms: Recommendations and key lengths: BSI TR-02102-1, Version 2023-01[R]. Bonn: BSI, 2023.
- [14] Tjhai C, Tomlinson M, Bartlett G, et al. Multiple key exchanges in the Internet Key Exchange Protocol version 2 (IKEv2): RFC 9370[EB/OL]. [2026-06-15]. <https://www.rfc-editor.org/info/rfc9370>.
- [15] Schwabe P, Stebila D, Wiggers T. Post-quantum TLS without handshake signatures[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 1461–1480.
- [16] Stebila D, Fluhrer S, Gueron S. Hybrid key exchange in TLS 1.3: Draft-ietf-tls-hybrid-design[EB/OL]. [2026-06-15]. <https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/>.
- [17] Bindel N, Herath U, McKague M, et al. Transitioning to a quantum-resistant public key infrastructure[M]//Post-Quantum Cryptography. Cham: Springer International Publishing, 2017: 384–405.
- [18] Kampanakis P, Panburana P, Daw E, et al. The viability of post-quantum X. 509 certificates[EB/OL]. [2026-06-15]. <https://eprint.iacr.org/2018/063>.
- [19] International Organization for Standardization (ISO). Financial services—universal financial industry message scheme: ISO 20022[S]. Geneva: ISO, 2013.
- [20] Gray J, Lamport L. Consensus on transaction commit[J]. *ACM Transactions on Database Systems*, 2006, 31(1): 133–160.
- [21] Liu R, Zeng N. A cost-model audit of Project Leap phase 2: Latency, capacity, and migration safety in post-quantum RTGS[C]//Proceedings of WorldS4 2026. London: Springer, 2026 (in press).
- [22] 中国信息通信研究院, “密码+”应用推进计划. 后量子密码应用研究报告(2023年)[R]. 北京: 中国信息通信研究院, 2023.
- [23] 国家密码管理局. SM2椭圆曲线公钥密码算法: GM/T 0003—2012[S]. 北京: 中国标准出版社, 2012.
- [24] 国家密码管理局. SM3密码杂凑算法: GM/T 0004—2012[S]. 北京: 中国标准出版社, 2012.
- [25] 国家密码管理局. SM9标识密码算法: GM/T 0044—2016[S]. 北京: 中国标准出版社, 2016.
- [26] 中华人民共和国国务院. 商用密码管理条例(国务院令 760号)[EB/OL]. (2023-04-27) [2026-05-08]. https://www.gov.cn/gongbao/2023/issue_10506/202306/content_6885266.html.
- [27] 全国人民代表大会常务委员会. 中华人民共和国密码法[EB/OL]. (2019-10-26) [2026-05-08]. http://www.xinhua-net.com/politics/2019-10/26/c_1125156896.htm?baike=.
- [28] 中国人民银行. 金融科技发展规划(2022—2025年)[Z]. 北京: 中国人民银行, 2022.

A modular decoupling architecture for the post-quantum migration of financial market infrastructures

LIU Rui^{1,2}, ZHANG Bin³, ZENG Neng¹

1. Post-Quantum Migration Interdisciplinary Laboratory (PQC-X), Xi'an Jiaotong-Liverpool University, Suzhou 215123, China

2. Suzhou LangKong Post-Quantum Technology Co., Ltd., Suzhou 215021, China

3. Yunchao Financial Services (Beijing) Co., Ltd., Beijing 102300, China

Abstract Quantum computing erodes the security foundation of classical public-key systems, prompting global financial market infrastructures (FMIs) to accelerate their migration to post-quantum cryptography (PQC). The Phase 2 empirical tests of the Bank for International Settlements (BIS) Project Leap reveal the engineering constraints of shifting real-time gross settlement (RTGS) systems to hybrid cryptography: native schemes do not support parallel processing of heterogeneous algorithms, and end-to-end PQC signature verification takes about 209.9 ms, which is 7.5 times the 28.1 ms of classical cryptography. Our analysis shows that this overhead stems mainly from system-level stages such as message parsing and verification-software orchestration rather than from the lattice operations themselves; placing it on the synchronous critical path of high-concurrency settlement would depress throughput. This study therefore decouples the processing chain so that the upgrade can proceed in stages: a nested signature with an inner PQC layer and an outer RSA layer is constructed in the Business Application Header (BAH), allowing legacy gateways to accept messages without parsing PQC extension blocks (zero-intrusion access); the verification latency is offset by the asynchronous rollback of a distributed transaction, in which a pre-settlement hold removes synchronous blocking and a compensating transaction restores global consistency, overlaid with a quantified monitoring model featuring anomaly-triggered circuit breaking. Simulations show that, once verification is moved off the critical path, the settlement-decision latency drops to the millisecond level and the software-only path already meets the conventional 500 ms monitoring ceiling; with an optional FPGA pipeline accelerator to suppress jitter, the threshold can converge to within 50 ms. The analysis of a three-stage evolution path further supports this conclusion: with proper decoupling and sound asynchronous orchestration, real-time throughput need not be sacrificed, and financial core systems can steadily complete their quantum-resistant security upgrade.

Keywords post-quantum cryptography; financial market infrastructure; Project Leap; transaction decoupling; FPGA acceleration; hybrid signature ●



(责任编辑 王志敏)