工程与应用

后量子密码算法在电信领域的应用研究

王靖然[1,2]，王聪丽[1,2]，宋伟[1]，陈勇量[1]，薛伟佳[1,2]，王锦华[1,2]
（1. 中国电信股份有限公司研究院，上海 201315；
2. 云网基础设施安全国家工程研究中心，上海 201315）

摘　要：密码作为国家重要的战略资源，在网络与信息安全领域发挥着核心作用。近年来，量子计算技术的快速发展，有效推动了学术界、产业界等对后量子密码（post-quantum cryptography，PQC）的研究与应用。基于此，研究了量子计算对经典密码算法的安全威胁，调研了PQC的发展现状，分析了电信领域典型场景的量子安全影响，最后开展了PQC签名算法模块化格基数字签名标准（module-lattice-based digital signature standard，ML-DSA）的迁移验证与测试分析。实验结果表明，ML-DSA算法能够满足系统的高并发、高可用要求。

关键词：后量子密码；量子安全；网络基础设施；ML-DSA
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025123

Research on the application of post-quantum cryptographic algorithms in the telecommunications field

WANG Jingran[1,2], WANG Congli[1,2], SONG Wei[1], CHEN Yongliang[1], XUE Weijia[1,2], WANG Jinhua[1,2]
1. Research Institute of China Telecom Co., Ltd., Shanghai 201315, China
2. National Engineering Research Center of Cloud and Network Infrastructure Security, Shanghai 201315, China

Abstract: As a vital strategic resource, cryptography plays a core role in the field of network and information security. In recent years, the rapid development of quantum computing has effectively promoted the research and application of post-quantum cryptography (PQC) algorithms in academia and industry. Based on this, the security threats posed by quantum computing to classical cryptographic algorithms were studied, the current development status of PQC was surveyed, the quantum security impacts on typical scenarios in the telecommunications field were analyzed, and finally, migration verification and testing analysis were conducted for the PQC signature algorithm (module-lattice-based digital signature standard) ML-DSA. The experimental results indicate that the ML-DSA algorithm can meet the requirements of high concurrency and high availability of the system.

Key words: post-quantum cryptography, quantum security, network infrastructure, ML-DSA

收稿日期：2025−01−22；**修回日期：**2025−04−29
通信作者：王靖然，wangjr7@chinatelecom.cn
基金项目：科技创新2030—“量子通信与量子计算机”重大项目（No.2021ZD0301300）
Foundation Item: The Science and Technology Innovation 2030 - Quantum Communication and Quantum Computer (No.2021ZD0301300)

0　引言

量子科技已被美国、欧盟等国家及地区纳入其发展战略规划中，各国家及地区进一步加大对量子科技的经济投入。2024 年 7 月，党的二十届三中全会中提到要因地制宜发展新质生产力，完善量子科技等战略性产业发展政策和治理体系，可见量子科技在我国的科技战略布局中占据重要地位。量子科技按照技术结构主要分为 3 个方向：量子计算、量子通信和量子测量[1]。

量子计算以量子比特为基本单元，利用量子叠加和干涉等原理实现并行计算，能为某些计算复杂的问题提供指数级加速[2]。与传统计算机相比，量子计算机具有天然的量子并行计算能力、强大的存储能力和快速的运算速度，这将为计算能力带来质的飞跃，并已成为各国争相布局的前瞻技术领域。尽管量子计算带来了巨大的算力前景，但也对经典密码算法的安全性构成了威胁，因此，亟须研究能够在量子环境下保证安全的一类密码算法，后量子密码（post-quantum cryptography，PQC）应运而生。

1　PQC 发展的必要性

经典密码算法按照功能可以分为非对称密码算法（也称公钥密码算法）、对称密码算法和密码杂凑算法[3]。其中，对称密码算法和密码杂凑算法受到 Grover 量子算法的影响，有效密钥长度减半，即安全强度减半[4]。公钥密码算法则受到 Shor 量子算法的影响，安全强度呈指数级下降，且增加密钥长度也无法保证安全[5]。经典密码算法受量子影响的分析见表 1。

目前，加密相关量子计算机（cryptographi-

表 1　经典密码算法受量子影响的分析

密码类型	算法名称		密钥长度/bit		有效密钥长度/bit	
					经典环境安全强度	量子环境安全强度
公钥密码算法	RSA-1024		私钥	1 024	80	0
	RSA-2048			2 048	112	0
	ECC-256			256	128	0
	ECC-384			384	192	0
	SM2			256	128	0
对称密码算法	AES-128		对称密钥	128	128	64
	AES-256			256	256	128
	SM4			128	128	64
密码杂凑算法	SHA-2	SHA-224	——		112	56
		SHA-256			128	64
		SHA-384			192	96
		SHA-512			256	128
	SHA-3	SHA-224			112	56
		SHA3-256			128	64
		SHA-384			192	96
		SHA3-512			256	128
		SHAKE128			min（输出长度/2，128）	min（输出长度/4，64）
		SHAKE256			min（输出长度/2，256）	min（输出长度/4，128）
	SM3				128	64

cally relevant quantum computer，CRQC）何时实现商用仍是未知数。美国兰德公司在其2020年的报告中“预测”：平均情况下密码学相关量子计算机将在2033年出现[6]。德国联邦信息安全办公室（Bundesamt für Sicherheit in der Informationstechnik，BSI）“假设”与密码学相关的量子计算机在20世纪30年代中期出现[7]。在2023年2月的第9届欧洲电信标准组织（European Telecommunications Standards Institute，ETSI）量子安全密码学会议上，加拿大滑铁卢大学Mosca教授给出了其最新“预测”：公钥密码算法RSA-2048在21世纪30年代初被攻破的乐观概率是27%，与其在2016年预测的50%的概率相比，有所下调。

在此背景下，相关研究人员仍需要提前布局PQC领域的研究，因为信息系统会面临一种名为“现在存储，以后解密”（store now，decrypt later，SNDL）的攻击。这种威胁是指攻击者会收集加密的数据，待到将来实用化量子计算机出现时再进行解密。这种攻击方式主要针对于安全性要求高、保密期限长的敏感数据。为了抵御这种攻击形式，PQC的研究迫在眉睫。

2 PQC的发展现状

目前PQC针对公钥密码算法，按照算法功能可分为公钥加密/密钥封装算法和数字签名算法两类。

2.1 国外发展现状

美国是目前推动PQC发展力度最大的国家，主要体现在PQC算法标准化和PQC迁移应用两个方面。

在PQC算法标准化方面，美国国家标准及技术协会（National Institute of Standards and Technology，NIST）于2016年启动了面向全球的PQC算法征集。截至目前，已完成3轮算法评估，并于2024年8月13日正式发布了其中3个PQC算法的标准[8-10]。NIST正式发布的3个PQC算法见表2。

在PQC迁移应用方面，美国政府与相关标准组织发布了多项迁移指导文件，其中2022年9月美国国家安全局（National Security Agency，NSA）发布了《商业国家安全算法套件2.0》，为国家安全系统（National Security System，NSS）PQC的迁移规划了明确时间节点[11]。2022年12月，美国政府签署了《量子计算网络安全准备法案》，这意味着PQC的迁移正式成为美国法律[12]。

为促进PQC项目的发展，隶属于美国NIST的美国国家网络安全卓越中心（National Cybersecurity Center of Excellence，NCCoE）正在征集产业界合作伙伴，目前已有41家企业参与到NCCoE的迁移计划中[13]，其中亚马逊、IBM、思科、微软等诸多重量级公司以及PQShield、PostQuantum等抗量子专业公司纷纷加入，足见产业界对PQC的重视程度。

欧洲并没有制定单独的PQC算法标准化计划，而是采用全力配合美国NIST算法征集的策略。目前，NIST已正式发布的3个PQC算法，均

表2 NIST正式发布的3个PQC算法

标准编号	名称及缩写	原始算法名称	算法类型	支持安全等级	算法优先级	对比经典算法
FIPS 203	模块化格基密钥封装机制标准（module-lattice-based key-encapsulation mechanism standard，ML-KEM）	CRYSTALS-KYBER	公钥加密/密钥封装	1，3，5	推荐算法	RSA、DH、ECDH、SM2
FIPS 204	模块化格基数字签名标准（module-lattice-based digital signature standard，ML-DSA）	CRYSTALS-Dilithium	数字签名	2，3，5	推荐算法	RSA、ECDSA、SM2
FIPS 205	无状态哈希数字签名标准（stateless hash-based digital signature standard，SLH-DSA）	Sphincs+	数字签名	1，3，5	备用算法	RSA、ECDSA、SM2

为欧洲参与设计的。此外，欧洲电信标准组织在技术委员会（Technical Committees，TC）网络工作组中成立了量子安全密码（quantum-safe cryptography，QSC）组，负责与PQC算法相关的标准制定和研究工作[14]。

日韩方面对PQC的推动也较为积极，日本正积极推动NTRU（Number Theory Research Unit）算法的标准化，韩国启动了本国的PQC算法征集，目前已完成算法评估工作。2024年10月，韩国SK电讯（SKT）推出了结合量子密钥分发（quantum key distribution，QKD）与PQC的加密解决方案，采用双重加密技术来保证重要的信息安全。此外，LGU+与韩国国家情报院（National Intelligence Service，NIA）共同提出的光传输网络中的PQC应用规范已被韩国电信技术协会采纳为该国相关标准。

2.2　国内发展现状

近年来，我国对网络安全的关注度持续提升，无论对于个人信息安全还是国家信息安全，PQC都是非常重要的一环，我国已开展与PQC相关的研究工作。

2019年，国家密码管理局委托中国密码学会开展了面向国内的抗量子密码算法征集，共征集到38个算法，经过两轮的评估，遴选出一等奖3个、二等奖4个、三等奖7个。获奖算法按照功能可以分为公钥加密/密钥封装算法、密钥交换算法和签名算法。中国密码学会算法征评选情况见表3[15]。

中国科学院大学牵头的“LMS-SM3和HSS-SM3：基于SM3的带状态数字签名算法”密标申报项目，已通过密码行业标准化技术委员会（以下简称“密标委”）密码基础工作组2023年标准立项评审会的审查[16]。由我国学者提出的基于格的密钥封装算法CTRU/CNTU[17]，也已在我国密标委正式立项[18]。

表3　中国密码学会算法征评选情况

获奖情况	公钥加密/密钥封装算法	密钥交换算法	签名算法
一等奖	LAC.PKE		Aigis-sig
	Aigis-enc		
二等奖	Scloud	LAC.KEX	
	AKCN	SIAKE	
三等奖	AKCN-E8	OKCN	FatSeal
	TALE		木兰
	Piglet-1		PKP-DSS

3　电信领域量子安全影响分析

电信业务系统密码应用十分广泛，网络基础设施、物联网、云服务及管理系统等均需要公钥密码算法做安全支持[19-21]。CRQC对电信领域构成了新的威胁，因其破坏了电信网络系统中广泛使用的加密算法和协议。本节选择网络基础设施和内部管理系统两个典型应用方向，进行量子安全影响分析。

3.1　网络基础设施

在网络基础设施层面，本文选择了较为广泛应用的5G与虚拟专用网络这两类应用场景中的密码典型应用案例进行量子安全性分析。

3.1.1　5G基站与安全网关之间的安全

下一代无线接入网（NG-RAN）与5G核心网（5GC）之间的数据流量在通过不安全或第三方网络传输时容易受到攻击，3GPP标准没有强制要求在接入网和核心网的网络功能之间使用安全网关[22]，但通常由运营商部署。5GC安全网关示例如图1所示，图中缩写名称释义见表4。

安全网关与gNB之间使用IPSec隧道进行通信，每个安全网关都封装了N2和N3接口，安全网关通过这些接口将数据以明文形式转发到各自的远程端点（AMF和UPF）。gNB的身份验证是通过X.509证书进行的，以防止未经授权的实体访问5GC，IPSec隧道为N2和N3通信的完整性和机密性提供保障。

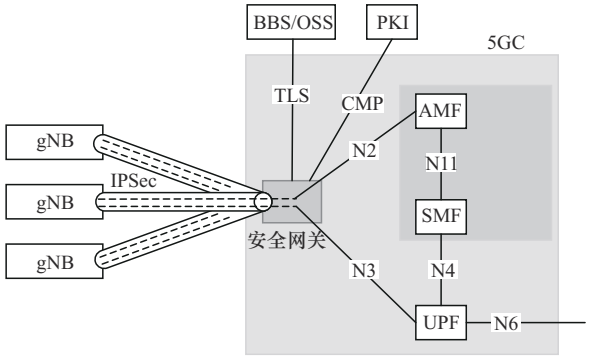

图1　5GC安全网关示例

表4　5GC安全网关示例图中缩写名称释义

英文缩写	英文全称	中文含义
gNB	the next generation node B	5G基站（下一代节点B）
BSS/OSS	business support system/operation support system	业务支撑系统/运营支撑系统
PKI	public key infrastructure	公钥基础设施
AMF	access and mobility management function	访问和移动管理功能
SMF	session management function	会话管理功能
UPF	user plane function	用户平面功能
IPSec	Internet protocol security	互联网安全协议
TLS	transport layer security	传输层安全性协议
CMP	certificate management protocol	证书管理协议
N2	—	RAN与AMF之间的控制面接口
N3	—	RAN与UPF之间的用户面接口
N4	—	SMF与UPF之间的接口
N6	—	UPF与外部数据网络之间的接口
N11	—	AMF与SMF之间的接口

（1）脆弱性分析

非对称密码的使用威胁到依赖其构建的用户信令和管理流量的连接安全性，被认为不安全的通信过程包括：①由于使用了IPSec套件，特别是在密钥建立阶段采用互联网密钥交换（Internet key exchange，IKE）时使用的密钥交换算法（DH或ECDH），因此基站和安全网关之间的连接面临安全威胁。②基站、安全网关和OSS/BSS系统之间通过TLS协议连接，TLS协议在握手过程中使用密钥交换算法（DH或ECDH），因此也面临安全威胁。

（2）敏感数据分析

上述创建安全连接的过程存在安全威胁，进而影响到传输的敏感数据的安全，主要包括：①基站与安全网关之间传输的用户数据。②网元（基站、安全网关）与其OSS/BSS之间传输的管理数据。

3.1.2　虚拟专用网络安全

虚拟专用网络（virtual private network，VPN）通过公共网络建立安全的专用通信信道，被广泛部署在移动电信网络中，成为在多数情况下使用的安全核心组件[23]。例如，上文所述的基站和安全网关之间的连接；远程SIM配置时，安全连接基于5G服务化架构（service-based architecture，SBA）内的不同网络功能，实现固件更新和设备管理；使用云基础设施时，保护传输数据，为用户实现安全连接等。

创建虚拟专用网络有不同的安全协议，取决于安全连接是发生在网络层、传输层，还是应用层。VPN典型应用场景如图2所示。

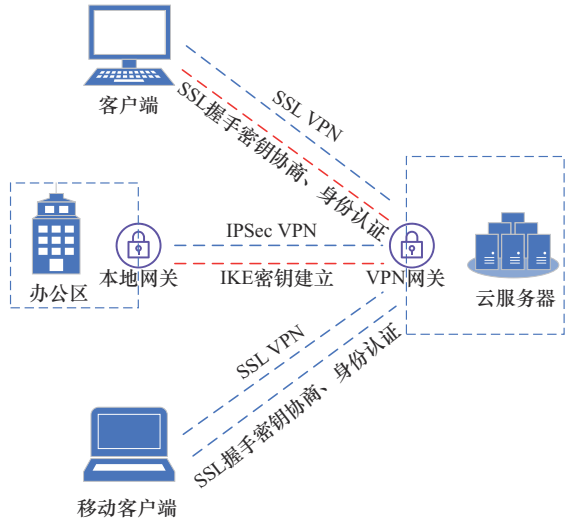

图2　VPN典型应用场景

（1）脆弱性分析

VPN 的脆弱性取决于 VPN 类型和使用环境。例如，SSL VPN 使用 SSL/TLS 协议在传输层建立 VPN 通道，只需要用户对服务器进行单向身份验证，而两个公司站点间的 VPN 通常需要通过 IPSec 协议进行双向身份认证。SSL/TLS 协议在建立安全连接时，通常使用 DH 算法实现密钥交换，使用 RSA 或 ECDSA 数字证书实现身份认证。IPSec VPN 使用 IKE 协议建立安全关联（security association，SA），与 SSL 握手过程类似，也是基于公钥密码算法实现密钥交换和身份认证功能。DH 算法和数字签名方案（如 RSA 和 ECDSA）均容易受到 Shor 算法的攻击。因此，基于该算法的 VPN 被认为是量子脆弱的。

（2）敏感数据分析

VPN 中携带的加密数据可能具有长期安全需求，这些数据正是 VPN 量子安全敏感数据的主要来源。尽管用于加密的对称密码算法对量子攻击不是特别敏感，但用于建立共享密钥的过程可能是量子脆弱的。因此，电信运营商必须确定使用 VPN 来传输具有长期安全需求的敏感数据的具体位置，并提供能够保证数据长期保密性的 VPN 产品。

3.2　内部管理系统

电信领域内部管理系统繁杂，本文以较有代表性的客户关系管理（customer relationship management，CRM）系统为例，开展安全性分析。

CRM 系统作为关键基础设施，流转海量个人用户和政企客户的重要数据。CRM 系统主要的安全防护需求为重要数据在传输、存储时的机密性和完整性保护，以及终端用户、运维人员的身份真实性校验。

（1）脆弱性分析

运维人员访问 CRM 系统时采用安全浏览器 HTTPS 协议建立加密通道。CRM 系统内的应用服务器、数据库服务器与网关、4A 统一运维平台之间的通信需要使用密码技术建立通信通道，如 SSL VPN。对于第三方业务系统，CRM 系统一般采用数字证书的方式进行身份鉴别。上述的安全手段，均有公钥算法参与，因此，被认为是量子脆弱的。

（2）敏感数据分析

CRM 系统的敏感数据包括：普通用户/管理员用户的信息（姓名、证件号、手机号等）、CRM 系统的订单信息，以及运维管理员的访问控制信息等。

综上分析可知，多数场景的共性量子安全威胁与 TLS、IPSec 等安全协议有关。因此，安全协议的 PQC 迁移是保障电信网络安全的重中之重。目前，国际互联网工程任务组（Internet Engineering Task Force，IETF）的安全领域工作组，如 TLS、IPsecME、LAMPS 等正在开展 PQC 的协议适配方案研究，已有初步草案发布[24-26]，预测未来主流安全协议向 PQC 的扩展将加快推进。

4　PQC 的应用验证

PQC 的算法标准化工作仍在进行中，算法构建方式、特性等均存在差异，需要根据场景需求进行选择，本文选择了 NIST 已标准化且优先推荐的签名算法 ML-DSA，并在电信某业务系统中开展 PQC 的迁移应用验证。

4.1　实验方案设计

业务系统现有认证过程如图 3 所示。图 3 为当前能力提供方（业务系统）与能力使用方第三方客户端进行认证的过程。

（1）通信双方基于离线的方式预先约定相同密钥 secretkey，双方保密。

（2）客户端使用省份编码 ProvinceCode、服务请求 ServiceReq、时间戳 Tonce 和密钥 secretkey 生成消息验证码 Hmac，并将其添加到 HTTP 请求

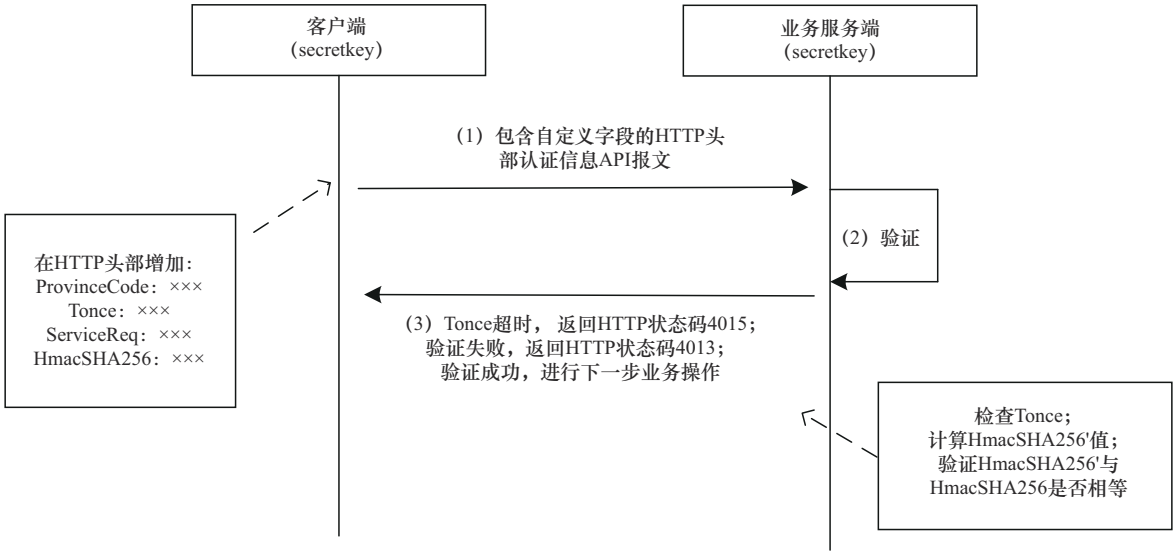

图3 业务系统现有认证过程

头中。

（3）业务服务端基于接收到的请求，检查时间戳Tonce，并验证Hamc值。若时间戳Tonce超时，则返回HTTP状态码4015；若验证失败，则返回HTTP状态码4013；若验证成功，则进行下一步业务操作。

基于上述原认证方式，实验设计了基于PQC签名算法ML-DSA（Dilithium）的认证方法。业务系统基于PQC算法的认证过程如图4所示。

（1）客户端与业务服务端分别基于ML-DSA算法的KenGen函数生成抗量子签名算法的公私密钥对。

（2）通信双方将各自的公钥通过数字证书或离线的方式下发。

（3）客户端使用省份编码ProvinceCode、服

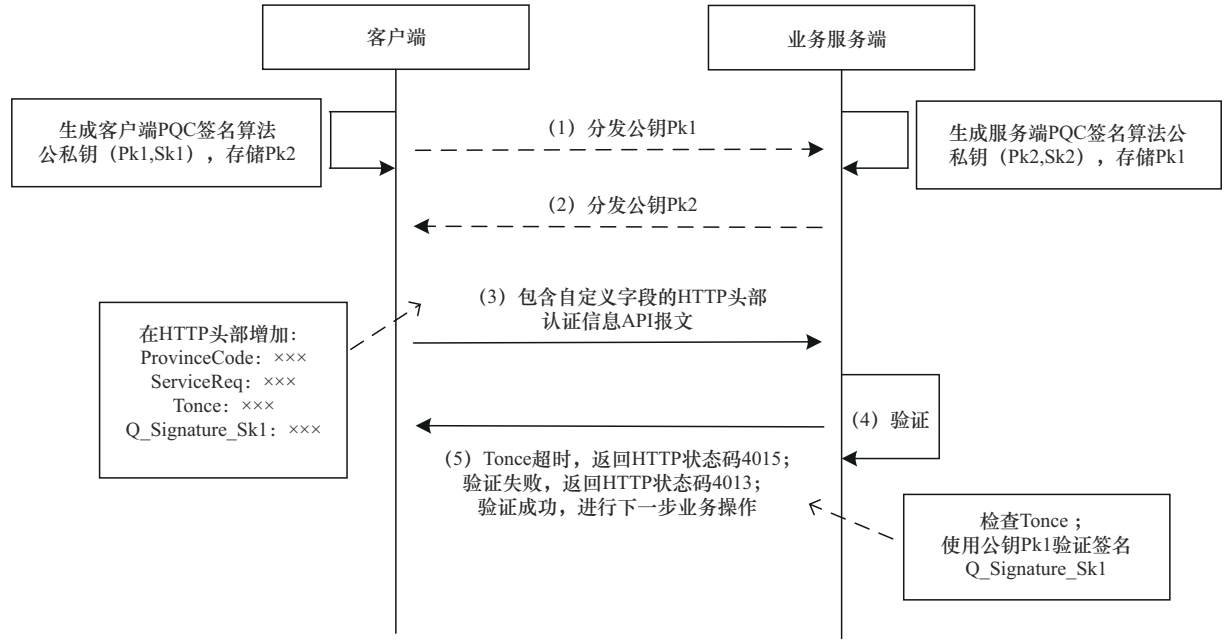

图4 业务系统基于PQC算法的认证过程

务请求 ServiceReq、时间戳 Tonce 和平台的私钥 Sk1 生成签名数据 Q_Signature_Sk1，并将其添加到 HTTP 请求头中。

（4）业务服务端基于接收到的请求，检查时间戳 Tonce，使用平台公钥 Pk1 验证签名。若时间戳 Tonce 超时，则返回 HTTP 状态码 4015；若验证失败，则返回 HTTP 状态码 4013；若验证成功，则进行下一步业务操作。

4.2　测试数据分析

本文设计的业务系统 PQC 认证方案，支持 PQC 签名算法 ML-DSA 的 3 个安全等级，开展了该方案的开发验证与实验测试。实验在配备 32 GB 内存和第 8 代 Intel(R) Core(TM) i7-8565U 处理器 (1.99 GHz)的 Windows 11 环境中进行，测试使用的签名字符串长度设置为 11 598 byte，分别对 PQC 签名算法 ML-DSA 的 L2、L3、L5 安全等级进行压力测试与时延测试，并与我国 SM2 签名算法进行对比分析。

为了评估 PQC 迁移后业务系统的性能，实验开展了系统压力测试，测试的内容包括 10 并发压测 1 000 次、20 并发压测 1 000 次以及 100 并发压测 100 次。PQC 迁移后业务系统压力测试结果见表 6。由表 6 可知，迁移后 ML-DSA 算法 3 个安全等级的每秒请求数均在 60～70。随着安全等级的升高，每秒请求数有所降低，这与高安全等级算法的复杂度增加有关，但整体差距较小，仍处于系统可接受的范围内。此外，传统的 SM2 签名算法的每秒请求数低于 ML-DSA 算法，这说明基于格的抗量子签名算法 ML-DSA 迁移后在系统高并发、高可用方面表现良好，能够满足系统性能要求。

PQC 迁移后业务系统时延测试结果见表 7。由表 7 可知，ML-DSA 的签名/验签的时延要明显优于 SM2，L2 安全等级的 ML-DSA 的每秒签名次数是 SM2 的 2.37 倍，验证签名次数是 SM2 的 5.08 倍，优势明显。此外，ML-DSA 算法本身验签的速度要明显优于签名速度。

虽然 ML-DSA 算法在计算性能上表现优秀，但其公私钥以及密文长度要远大于传统签名算法，公私钥与签名长度对比见表 7。L2 安全等级的 ML-DSA 算法的公钥与私钥已达到 1 KB 以上，与 SM2 算法的 64 byte 和 32 byte 非同一数量级。签名长度为 2 420 byte，远大于 SM2 的签名长度 64 byte。此外，ML-DSA 随着安全等级的升高，

表 5　PQC 迁移后业务系统压力测试结果

压力测试内容		每秒请求数			
		ML-DSA-44（L2）	ML-DSA-65（L3）	ML-DSA-87（L5）	SM2
签名内容字符串长度 11 598 byte	并发 10，压测 1 000 次	69.23	62.16	63.39	60.43
	并发 20，压测 1 000 次	70.18	62.11	61.73	62.14
	并发 100，压测 100 次	68.35	66.62	66.38	63.45

表 6　PQC 迁移后业务系统时延测试结果

时延测试	每秒操作次数			
	ML-DSA-44（L2）	ML-DSA-65（L3）	ML-DSA-87（L5）	SM2
签名	1 349	965	899	569
验签	3 274	2 923	2 557	644

表7 公私钥与签名长度对比

对比项	数据长度/byte			
	ML-DSA-44（L2）	ML-DSA-65（L3）	ML-DSA-87（L5）	SM2
公钥	1 312	1 952	2 592	64
私钥	2 560	4 032	4 896	32
签名	2 420	3 309	4 627	64

公私钥与签名的长度也在增加，L5安全等级的签名长度已达到4 627 byte，是SM2签名长度的72.3倍。签名长度的增加，增加了网络带宽需求，不利于数据传输。

4.3 电信领域PQC发展建议

PQC作为未来保障网络与信息安全的下一代密码技术，受到全球各行各业的关注，如何有序稳步推动PQC迁移是未来发展的关键。对此，本文提出针对电信领域的PQC发展建议，旨在促进电信领域PQC产业化应用，保障量子时代网络信息安全。

（1）推动我国PQC通信相关行业标准体系建设

电信领域相关企业可参与中国通信标准化协会（China Communications Standards Association，CCSA）等相关通信标准组织，为电信行业PQC算法的应用制定相应的技术指南、标准规范，为后续后量子迁移工作的有序高效开展提供指引。

（2）研究针对性密码脆弱性分析工具，设置迁移优先级

电信系统量子安全的脆弱性发现是电信领域PQC迁移面临的重要问题。电信现有业务与支撑系统错综复杂，内部量子脆弱，位置很难检测。研究快速准确的电信领域密码脆弱性评估工具，将有利于电信业务系统PQC迁移工作的推进。企业可根据系统脆弱性分析结果，设置系统迁移优先级，参考美国迁移时间节点，逐步开展PQC的迁移工作。

（3）加强产业协同探索，重点关注PQC芯片、性能优化等领域

PQC应用目前仍处于初期起步阶段，仍存在许多需要深入研究的方向，应联合产学研各方力量，推动PQC在电信领域的应用研究探索，重点关注PQC芯片、算法性能优化等领域，推动相应密码产品研发，提升工程化能力与性能，助力PQC迁移的原型验证及未来迁移的落地。

5 结束语

PQC算法作为抵御量子计算威胁的一条主流技术路线，已成为密码和网络安全领域的重点关注方向。本文分析了量子计算对经典密码算法以及电信领域相关业务系统的安全影响，总结了量子脆弱点和敏感数据，并开展了基于电信现有业务系统的PQC迁移实验与测试分析。实验结果表明，PQC算法ML-DSA迁移后系统在高并发、高可用、时延等方面均满足系统现网应用需求，但由于传输数据量的大幅增加，对网络带宽的要求有所提高。本文还给出了电信领域PQC算法未来的发展建议，为未来PQC算法大规模应用奠定坚实基础，赋能未来网络安全。

参考文献：

[1] COCCIA M, ROSHANI S. Evolutionary phases in emerging quantum technologies: general theoretical and managerial im-

plications for driving technological evolution[J]. IEEE Transactions on Engineering Management, 2024, 71: 8323-8338.

[2] YANG Z B, ZOLANVARI M, JAIN R. A survey of important issues in quantum computing and communications[J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 1059-1094.

[3] 杨波. 现代密码学[M]. 5版. 北京: 清华大学出版社, 2022.
YANG B. Modern cryptography[M]. 5th Edition. Beijing: Tsinghua University Press, 2022.

[4] 马彰超. 量子时代的网络安全挑战及其应对研究[J]. 信息通信技术与政策, 2019(10): 37-42.
MA Z C. The cyber security challenge in the quantum era and its countermeasures[J]. Information and Communications Technology and Policy, 2019(10): 37-42.

[5] HASAN K F, SIMPSON L, ALI REZAZADEH BAEE M, et al. A framework for migrating to post-quantum cryptography: security dependency analysis and case studies[J]. IEEE Access, 2024, 12: 23427-23450.

[6] RAND Corporation. Securing communications in the quantum computing age[R]. 2020.

[7] BSI. Securing tomorrow, today: transitioning to post-quantum cryptography[R]. 2024.

[8] NIST. FIPS 203 module-lattice-based key-encapsulation mechanism standard[S]. 2024.

[9] NIST. FIPS 204 module-lattice-based digital signature standard[S]. 2024.

[10] NIST. FIPS 205 stateless hash-based digital signature standard[S]. 2024.

[11] NSA. Commercial national security algorithm suite 2.0[R]. 2022.

[12] MACE N, KHANNA R. H.R.7535: Quantum Computing Cybersecurity Preparedness Act[EB]. 2022.

[13] NIST. Migration to post-quantum cryptography[EB]. 2025.

[14] ETSI. Quantum-safe cryptography (QSC)[EB]. 2025.

[15] 中国密码学会. 关于全国密码算法设计竞赛算法评选结果的公示[EB]. 2020.
China Cryptography Society. Public notice on the results of the National Cryptographic Algorithm Design Competition algorithm evaluation[EB]. 2020.

[16] 孙思维, 刘田雨, 关志, 等. SPHINCS$^+$-SM3: 基于SM3的无状态数字签名算法[J]. 密码学报, 2023, 10(6): 1266-1278.
SUN S W, LIU T Y, GUAN Z, et al. SPHINCS$^+$-SM3: SM3-based stateless digital signature scheme[J]. Journal of Cryptologic Research, 2023, 10(6): 1266-1278.

[17] LIANG Z C, FANG B Y, ZHENG J Y, et al. Compact and efficient KEMs over NTRU lattices[J]. Computer Standards & Interfaces, 2024, 89: 103828.

[18] 密码行业标准化技术委员会. 2023年度密码行业标准制修订任务(商用密码领域)[EB]. 2023.
Cryptography Standardization Technical Committee (CSTC). 2023 annual encryption industry standard formulation and revision tasks (commercial encryption field)[EB]. 2023.

[19] CHATTOPADHYAY A, BHASIN S, GÜNEYSU T, et al. Quantum-safe Internet of Things[J]. IEEE Design & Test, 2024, 41(5): 36-45.

[20] FERNÁNDEZ-CARAMÉS T M. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of Things[J]. IEEE Internet of Things Journal, 2020, 7(7): 6457-6480.

[21] GSMA. Post-quantum telco-network impact assessment white-paper (Version1.0)[R]. 2023.

[22] 3GPP TS 33.501. Security architecture and procedures for 5G system V18.6.0 (Release 18)[S]. 2024.

[23] BUDIYANTO S, GUNAWAN D. Comparative analysis of VPN protocols at layer 2 focusing on voice over Internet protocol[J]. IEEE Access, 2023, 11: 60853-60865.

[24] IETF. Draft-IETF-TLS-Hybrid-design-09: hybrid key exchange in TLS 1.3[S]. 2023.

[25] IETF. RFC 9370: multiple key exchanges in the Internet key exchange protocol version 2 (IKEv2)[S]. 2023.

[26] IETF. Draft-IETF-Lamps-Kyber-certificates-06: Internet X.509 public key infrastructure-algorithm identifiers for the module-lattice-based key-encapsulation mechanism (ML-KEM)[S]. 2024.

[作者简介]

王靖然（1995− ），女，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为网络安全技术、密码协议、后量子密码等。

王聪丽（1994− ），女，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为公钥密码基础设施、密码应用、商用密码应用安全性评估、5G安全、量子安全等。

宋伟（1994– ），男，中国电信股份有限公司研究院工程师，主要研究方向为网络安全运营。

薛伟佳（1990– ），女，博士，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为密码应用、商用密码及密评、量子保密通信与密码融合应用等。

陈勇量（1991– ），男，中国电信股份有限公司研究院工程师，主要研究方向为网络安全运营。

王锦华（1982– ），男，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为云计算、大数据安全、终端安全、密码应用、量子安全等。