专题：量子通信技术

基于后量子密码的小区广播系统安全增强

王聪丽[1]，薛伟佳[1]，王靖然[1]，王锦华[1]，卢洪涛[2]
（1. 中国电信股份有限公司研究院，上海 201315；
2. 中国电信股份有限公司研究院，广东 广州 510630）

摘　要：探讨了小区广播系统在量子计算时代面临的安全挑战，并提出基于后量子密码（post-quantum cryptography，PQC）算法的安全增强方案。首先，分析小区广播系统及其安全架构，识别其在量子计算环境下的潜在脆弱性；其次，评估主流PQC数字签名算法的安全性与性能特性，设计纯后量子证书、混合证书及组合证书3类后量子数字证书结构，并提出适配现有系统的密钥管理机制、消息发送流程及消息格式扩展方案；最后，从计算开销、存储占用及消息长度适配性等方面进行实验验证。结果表明，所提方案具备部署可行性，可为小区广播系统向后量子安全体系的演进提供技术参考与实现路径。

关键词：小区广播；后量子密码；数字签名；数字证书；量子安全
中图分类号：TP393；TN918
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2025256

Security enhancement for cell broadcast systems based on post-quantum cryptography

WANG Congli[1], XUE Weijia[1], WANG Jingran[1], WANG Jinhua[1], LU Hongtao[2]
1. China Telecom Research Institute, Shanghai 201315, China
2. China Telecom Research Institute, Guangzhou 510630, China

Abstract: A security enhancement scheme based on post-quantum cryptography (PQC) was presented to address the security threats posed to cell broadcast systems in the quantum computing era. Firstly, the cell broadcast system and its security architecture were analyzed to identify potential vulnerabilities in a quantum computing environment. Subsequently, mainstream PQC digital signature algorithms were evaluated in terms of their security and performance characteristics. Three types of post-quantum digital certificate structures—pure post-quantum certificates, hybrid certificates, and composite certificates—were designed, and a key management mechanism, message transmission process, and message format extension scheme compatible with existing systems were proposed. Finally, the proposed scheme was experimentally validated from perspectives such as computational overhead, storage occupancy, and message length adaptability. The results demonstrate the deployment feasibility of the scheme, indicating that it could provide technical reference and an implementation path for the evolution of cell broadcast systems toward a post-quantum security architecture.

Key words: cell broadcast, PQC, digital signature, digital certificate, quantum-resistant

收稿日期：2025−07−02；修回日期：2025−10−31

0 引言

我国是世界上自然灾害最为严重的国家之一，灾害种类多，分布地域广，发生频率高，造成损失重。我国高度重视应急管理工作，明确要求健全应急预案体系，推动应急治理向“精准治理”转型。近年来，我国在面向应急责任人等特定群体的预警平台建设方面取得显著进展，但面向普通公众的预警信息发布机制仍存在信息传递延迟高、覆盖范围不全面等问题[1-3]。小区广播技术是发布公共预警信息的有效手段之一，其现有安全机制基于SM2、椭圆曲线数字签名算法（elliptic curve digital signature algorithm，ECDSA）等传统公钥密码算法，在量子计算环境下面临被破解的风险。

后量子密码（post-quantum cryptography，PQC）是一类能够抵御量子计算攻击的新一代密码算法，被视为应对未来量子计算威胁的关键技术方向。国际上正积极推动PQC算法的标准化进程，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）已于2024年正式发布ML-KEM、ML-DSA和SLH-DSA 3项PQC算法标准[4-6]。多个国家已陆续启动向后量子密码的迁移工作，并发布了相应的迁移计划表与路线图[7-10]。然而，在小区广播等特定应用场景中，PQC算法的实际部署处于初步探索阶段，其性能优化与场景适应性仍有待进一步研究。

本文提出一种基于后量子密码的小区广播系统安全增强方案，并通过实验验证其可行性，以期为系统的安全演进提供技术参考与实施路径。

1 小区广播系统及其安全架构

1.1 小区广播技术概述

小区广播技术是一种基于移动通信网络的信息推送方式，它利用特定的广播控制信道，在设定时间内将信息发送至指定基站覆盖范围内的所有用户。其技术原理如图1所示，小区广播实体（cell broadcast entity，CBE）负责定义消息的内容、目标区域等参数，小区广播中心（cell broadcast center，CBC）接收来自CBE的消息，将其转换为适用于移动通信网络传输的格式，并确定需覆盖的基站小区列表。最终由移动通信网络通过空中接口将消息下发至用户终端设备[11]。

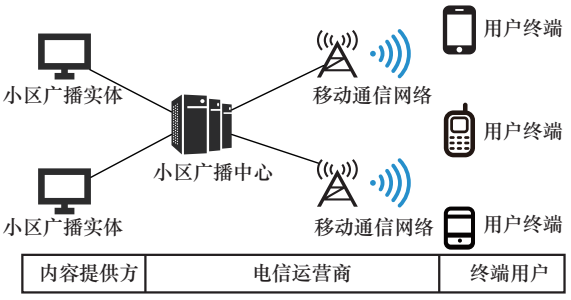


图1 小区广播技术原理

与传统信息传播渠道相比，小区广播技术具有以下优势。

（1）高速传输：可在接收到指令后的数秒内完成区域内信息覆盖，响应速度快，适用于对时效性要求高的应急场景。

（2）无容量限制：采用广播机制，可同时向区域内所有用户发送信息，且不受用户数量限制，适用于大规模人群预警。

（3）精准区域控制：可根据预设地理范围自动匹配相关基站，实现定向发布，提升预警信息的空间针对性和有效性。

（4）网络稳定性强：利用专用广播信道进行信息传输，不会增加现有通信网络的负担，也不会干扰其他通信服务的正常运行。

（5）警示效果突出：支持文字信息与特殊警示音结合，并可在用户终端强制弹窗显示，增强视觉与听觉提示效果，提高公众对紧急信息的关注度与响应效率。

小区广播技术作为一种高效、可靠且覆盖范围广的信息发布方式，能够快速向目标区域的公

众发布警报和通知，适用于自然灾害、突发事件等应急应用场景。

1.2　安全机制现状与挑战

为确保小区广播消息的真实性和完整性，我国已在该领域开展了系统性研究，并初步建立了基于数字签名的安全机制。

1.2.1　安全机制设计现状

在工业和信息化部的指导下，中国信息通信研究院协同相关单位启动了针对小区广播业务安全机制的研究工作，并于2025年4月发布了《基于数字签名的小区广播业务安全技术要求》（YD/T 6353—2025）[12]。该标准适用于4G/5G网络环境下的小区广播业务，后续商用部署方案据此进行了更新与完善。基于数字签名的小区广播系统架构如图2所示。

该系统架构主要涉及以下功能实体。

（1）小区广播信息发布平台（cell broadcast information release platform，CBIRP）：由气象局、地震局等权威机构组成，负责生成并提交预警信息。

（2）小区广播业务管理中心（cell broadcast service management center，CBSMC）：统一接收并整理来自CBIRP的消息，同时向各运营商分发。

（3）密钥管理中心（key management center，KMC）：负责密钥的生成与管理，为小区广播中心提供签名服务。

（4）小区广播中心/小区广播中心功能模块（CBC/cell broadcast center function module，CBCF）：申请签名，并发送已签名的广播消息至核心网。

（5）核心网/接入网：将消息下发至指定区域的终端设备。

（6）公钥分发平台：用于发布验证所需的公钥，供终端或厂商下载。

（7）终端设备：具备接收、验证与展示小区广播消息的能力。

小区广播消息发送步骤如下。

步骤1　CBIRP将小区广播消息发送至CBSMC。

步骤2　CBSMC将消息规整后发送至各运营

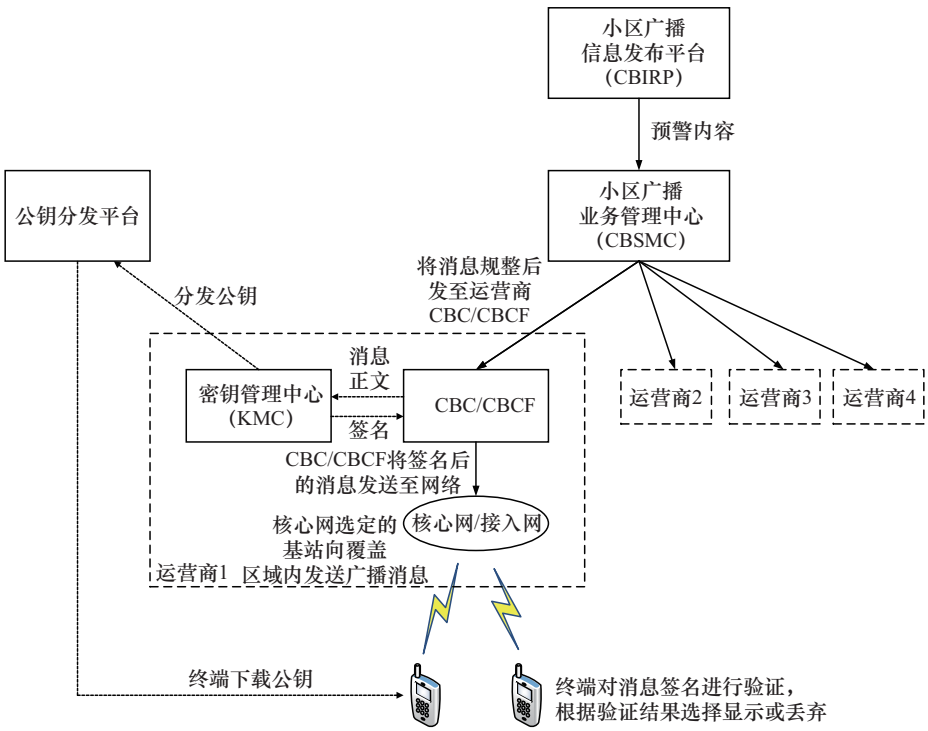


图2　基于数字签名的小区广播系统架构

商的CBC/CBCF。

步骤3 CBC/CBCF将消息发送至KMC申请签名。

步骤4 KMC对消息生成签名，并向CBC/CBCF返回安全消息体（含安全头域、消息正文及签名）。

步骤5 CBC/CBCF将安全消息体发送至核心网/接入网。

步骤6 核心网/接入网根据指示选择相应的区域发送广播消息。

步骤7 终端接收广播消息并验证签名，验证通过则显示广播消息内容，否则不显示广播消息内容。

目前，系统支持两类数字签名机制：一类采用我国商用密码标准的SM2与SM3算法组合，另一类基于NIST P-256的ECDSA与SHA-256算法组合。

1.2.2 面临的安全挑战

小区广播系统依托4G/5G网络提供服务，在量子计算环境下，面临两个关键挑战：一是4G/5G网络基础设施在量子计算攻击下的潜在脆弱性；二是当前数字签名机制在此环境下的适应性和有效性。

在网络基础设施层面，多个国际标准化组织已启动针对量子计算威胁的系统性研究。第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）自2018年起开展5G系统的后量子迁移研究，并在2022—2024年的R19阶段通过多项加密算法升级相关课题立项[13-16]。欧洲电信标准组织（European Telecommunications Standards Institute，ETSI）提出了ICT系统从非量子安全向完全量子安全迁移的框架，涵盖清单编制、计划制定与实施执行3个核心环节的迁移策略[17]。国际电信联盟电信标准化部门（International Telecommunication Union-Telecommunication Standardization Sector，ITU-T）评估了量子计算对IMT-2030系统的影响，并制定了量子安全算法应用指导原则[18]。上述标准化工作系统评估了移动通信网络中关键密码算法在量子计算环境下面临的安全威胁及相应的迁移对策，目前已逐步进入技术验证阶段。

在小区广播业务层面，如前所述，数字签名机制采用SM2/SM3与ECDSA/SHA-256两类密码算法组合。在量子计算环境下，SM2和ECDSA等基于离散对数问题的公钥密码算法可被Shor算法在多项式时间内破解，导致签名机制失效；而SM3和SHA-256等杂凑算法在Grover算法攻击下，实际安全强度将降至原有强度的约2/3，抗量子能力显著下降。

在经典计算和量子计算环境下，当前小区广播系统中使用的公钥密码算法与杂凑算法的参数及安全性分别见表1、表2[19-21]。

表1 小区广播系统所采用的公钥密码算法参数及安全性

公钥密码算法	公钥长度/bit	私钥长度/bit	签名长度/bit	安全强度/bit		受到量子计算的影响
				经典环境	量子环境	
SM2	512	256	512	128	0	不再安全
ECDSA-P 256	512	256	512	128	0	

表2 小区广播消息所采用的杂凑算法参数及安全性

杂凑算法	构造方式	输出长度/bit	分组长度/bit	安全强度/bit		受到量子计算的影响
				经典环境	量子环境	
SM3	M-D结构	256	512	128	80	安全性降低约2/3
SHA-256	M-D结构	256	512	128	80	

综上所述，尽管当前数字签名机制在经典计算环境下可提供有效的安全保障，但其依赖的公钥密码算法在量子计算威胁下存在明显安全缺陷。因此，有必要在系统大规模部署前，开展基于后量子密码的安全架构设计，提前定义兼容性接口与扩展机制，以支持向后量子安全体系的渐进式迁移。

2　后量子密码在小区广播系统中的应用

本节将围绕PQC算法在小区广播系统中的应用展开研究，重点探讨其选型依据、数字证书设计及与现有业务流程的集成方案。首先，介绍主流PQC数字签名算法及其标准化进展；接着，分析3种适配小区广播系统的后量子证书模式；最后，结合现行标准，提出支持PQC算法的广播消息发送流程、密钥管理机制与消息格式扩展方案，为后续性能评估与部署策略提供技术支撑。

2.1　后量子算法选型

根据功能需求，PQC算法可分为公钥加密算法（或密钥封装算法）和数字签名算法。在小区广播的应用场景中，主要采用数字签名算法。目前常见的PQC数字签名算法主要包括以下几类[4-6, 22]。

（1）基于格的数字签名算法：安全性依赖于求解格中特定数学问题的困难性。此类算法通常具有较短的密钥与签名长度，同时具备较高的计算效率。代表算法包括ML-DSA与Falcon，二者均已被纳入NIST标准体系。

（2）基于哈希的数字签名算法：安全性直接依赖于哈希函数的抗碰撞性，提供了较高的理论安全性，但签名长度较长。代表性算法SLH-DSA已被纳入NIST标准体系。

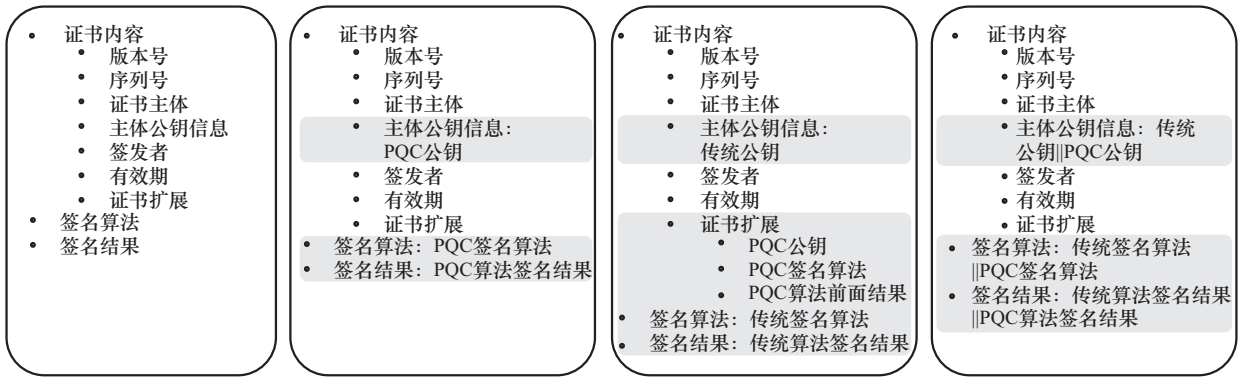
（3）基于编码的数字签名算法：安全性依赖于某些编码方案的译码困难性。尽管该类算法存在密钥尺寸较大、密钥生成速度较慢等问题，但其密文较小。代表算法为CROSS，目前正处于NIST附加轮的评估阶段，尚未被标准化。

（4）基于多变量的数字签名算法：安全性依赖于求解有限域上非线性多变量多项式方程组的困难性。该类算法的优势在于签名生成速度快，但密钥尺寸较大。代表算法为Mayo，目前正处于NIST附加轮的评估阶段，尚未被标准化。

上述4类算法各具特点，本文针对每种类别选取代表性算法进行研究。优先选用已标准化的算法，而对于尚未形成标准的类别，则选取当前处于NIST标准化评估阶段的候选算法。

2.2　后量子数字证书设计

数字证书是小区广播安全机制中实现身份认证与信任链构建的核心。随着PQC算法的部署，证书的结构与签发机制亟须重构。当前主流方案包括纯后量子、混合与组合数字证书3类[23-27]，其基本结构如图3所示。



（a）X.509v3数字证书　（b）纯后量子数字证书　（c）混合数字证书　（d）组合数字证书

图3　后量子数字证书基本结构

2.2.1 纯后量子数字证书

纯后量子数字证书完全基于PQC算法构建，涉及密钥生成、签名签发与验证等关键环节。通过定义新的对象标识符（object identifier，OID）明确标识所采用的PQC算法实例，确保协议交互中的可识别性与操作一致性。其结构遵循标准X.509v3格式，设计简洁、逻辑清晰，便于系统管理与信任链构建。然而，由于主流操作系统与应用平台尚未原生支持PQC算法，部署此类证书通常需对应用系统、密码模块及信任根进行整体升级，因而更适用于PQC生态成熟后的长期部署阶段。

2.2.2 混合数字证书

混合数字证书在单张X.509v3证书中并行集成传统公钥算法与PQC算法，支持从传统密码体制向后量子安全架构的渐进迁移。传统公钥、算法标识及签名值保留在标准字段中，PQC算法组件则封装于可标记为“非关键”的扩展字段，使不支持PQC的验证方可安全忽略该部分，避免解析错误或验证中断，从而实现向后兼容。然而，该设计面临降级攻击风险：攻击者可通过屏蔽或篡改PQC扩展，诱导验证方仅依赖传统算法完成认证，规避PQC算法提供的安全性。为缓解此威胁，可在协议层强制执行双算法联合验证，或优先启用PQC算法，确保其保护机制不被绕过，提升迁移阶段的安全强度。

2.2.3 组合数字证书

组合证书与混合证书类似，均在单张X.509v3证书中集成多个密码算法，但其结构设计更为紧耦合。它不依赖X.509v3扩展机制，而是将多个算法的公钥、算法标识符与签名值按预定义顺序编码为结构化复合体，直接替换证书中的相应标准字段。该设计要求参与方具备多算法解析能力，并通过联合验证机制确保所有组件签名同时通过验证，从而在单个算法失效时仍能维持整体安全性，显著提升系统的容错性与鲁棒性。然而，该方案面临剥离攻击风险，攻击者可能诱导验证方仅接受某一组件算法的有效性。为实现有效防御，所有公钥必须被视为不可分割的整体密钥，任何子签名的独立信任均应被拒绝。同时，所选算法组件本身应处于安全状态，以避免引入结构性安全漏洞。

3类后量子数字证书均具备抵御经典计算与量子计算攻击的能力，但在结构设计、实现鲁棒性与系统兼容性方面存在显著差异。纯后量子证书结构简洁，是长期演进的理想形态；混合证书通过扩展字段实现算法共存，具备良好的向后兼容性，适合过渡阶段部署；组合证书采用多算法联合验证，提升了对单一算法被破解的安全鲁棒性，但对终端与基础设施的兼容性要求更高。因此，实际选型应综合考虑系统支持能力、运维复杂度与密码迁移阶段，进行场景化评估与部署规划。

2.3 后量子安全机制集成路径

由于PQC算法的多样性，以及不同运营商和终端设备在部署能力上存在差异，本节提出的方案并非唯一可行路径，而是构建了一种以“最小化影响、最大化兼容”为核心理念的集成设计思路。该设计围绕纯后量子证书、混合证书与组合证书3类数字证书结构，从密钥管理机制、广播消息传输流程及消息格式设计与扩展机制等方面，系统阐述后量子安全机制的集成路径。

2.3.1 密钥管理机制

本方案采用标准化的二级证书链结构，包含根证书和公钥证书，由各运营商独立管理。终端可通过预置方式或从运营商平台下载安装根证书，作为验证公钥证书的信任锚点。公钥证书由根证书签发后统一上传至公钥分发平台，供终端按需下载使用。相应的私钥由KMC集中管理，用于对CBC/CBCF发起的相关请求进行数字签名。

为保证证书体系的一致性，根证书与公钥证

书应采用相同的证书类型，可选择纯后量子数字证书、混合数字证书或组合数字证书等形式。证书更新机制遵循原有标准流程，确保系统的持续可用性与安全性。

2.3.2　广播消息传输流程

本方案在整体流程设计上与第1.2.1节所述标准流程保持一致。根据所采用数字证书类型的差异，本方案可分为3种实现方式：基于纯后量子数字证书的方案、基于混合数字证书的方案和基于组合数字证书的方案。3类方案的主要区别在于密钥配置、签名生成方法、消息格式设计及终端验证策略，其余操作步骤则保持一致，形成统一的流程基础。广播消息传输流程如图4所示。

（1）基于纯后量子数字证书的方案。

在该方案中，KMC通过密钥管理机制配置PQC私钥，终端则配置相应的纯后量子数字证书。当CBC/CBCF提交消息正文请求签名时，KMC使用PQC私钥对消息正文进行签名，并将生成的签名结果封装于安全消息体中，随后下发至核心网/接入网。核心网/接入网根据区域配置广播该消息。终端接收广播后，提取公钥证书中的PQC公钥对签名进行验证。若验证通过，则显示消息内容；否则，丢弃该消息。该方案适用于对安全性要求较高，且终端设备全面支持PQC算法的部署场景。

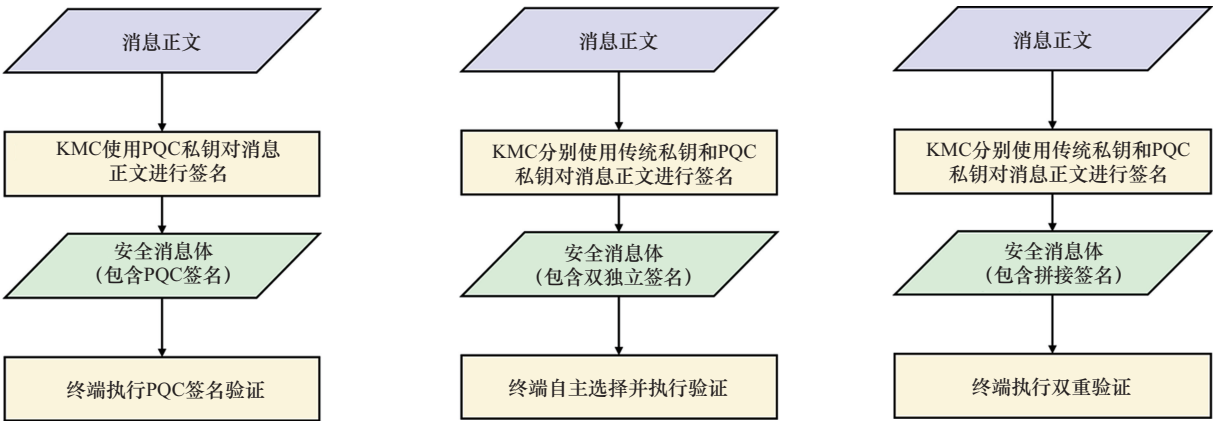
（2）基于混合数字证书的方案。

在该方案中，KMC通过密钥管理机制同时配置传统私钥与PQC私钥，终端则配置相应的混合数字证书。当CBC/CBCF提交消息正文请求签名时，KMC分别使用传统私钥和PQC私钥对消息正文进行双重签名，并将两个独立的签名结果封装于同一安全消息体中，随后下发至核心网/接入网。核心网/接入网根据区域配置广播该消息。终端接收广播后，根据自身处理能力与安全策略选择验证路径：若终端支持PQC算法，则优先验证PQC签名；若不支持，则忽略PQC部分，仅验证传统签名。

该方案适用于处于从传统密码体系向后量子密码体系过渡阶段的运营商网络环境，在保障新终端抗量子安全能力的同时，兼顾旧终端的兼容性，具备良好的实用性与部署灵活性。

（3）基于组合数字证书的方案。

在该方案中，KMC通过密钥管理机制同时配置传统私钥与PQC私钥，终端则配置相应的组合数字证书。当CBC/CBCF提交消息正文签名请求时，KMC分别使用传统私钥和PQC私钥对消息正文进行双重签名，并将两个签名结果合并为一个联合签名信息，封装于安全消息体中，随后下发至核心网/接入网。核心网/接入网根据区域配置广播该消息。终端接收广播后，分别验证其



（a）基于纯后量子数字证书　（b）基于混合数字证书　（c）基于组合数字证书

图4　广播消息传输流程

中的传统签名与后量子签名，从而实现对消息完整性的双重确认。

该方案不以兼容传统系统为目标，而是侧重于整体安全性的提升，确保即使某一类算法在未来被破解，系统仍具备足够的抗风险能力。因此，该方案适用于对安全性要求较高，且各参与方均具备多算法协同处理能力的部署环境。

2.3.3　消息格式设计与扩展机制

根据现有标准定义，小区广播消息以“安全消息体”形式进行传输，由安全头域、安全消息正文和签名3部分组成。其中，安全头域包含“算法标识”字段，用于指示消息所采用的签名算法及相关参数。签名部分支持配置2个独立字段，均可对完整的安全头域与安全消息正文进行签名。小区广播消息中的安全消息体结构如图5所示。

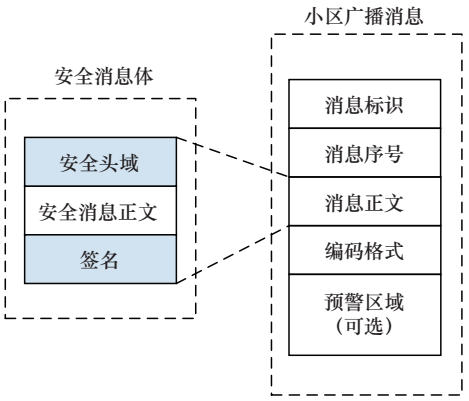


图5　小区广播消息中的安全消息体结构

为适配后量子密码机制，本文对算法标识字段进行扩展，新增3个取值，并相应调整签名字段的配置方式，以支持多种后量子证书方案，并为终端提供明确的验证指引。具体定义如下。

（1）0x04：用于表示纯后量子证书方案，消息中仅包含一个基于PQC算法的签名字段，不启用第二个签名字段。

（2）0x05：用于表示混合数字证书方案，消息中包含2个独立的签名字段，分别使用传统算法和PQC算法进行签名。

（3）0x06：用于表示组合数字证书方案，消息中包含一个联合签名字段，其内容由传统算法签名与PQC算法签名拼接组成，不启用第二个独立签名字段。

上述取值可根据实际部署需求灵活定义，本文仅提出逻辑分类建议，不对具体编码值做强制规定。标准中现有方案与本文扩展方案中的算法标识值与签名字段映射关系见表3。

表3　算法标识值与签名字段映射关系

算法标识		签名1	签名2
现有方案取值	0x01	SM2与SM3签名	ECDSA与SHA256签名
	0x02	SM2与SM3签名	无
	0x03	ECDSA与SHA256签名	无
扩展方案取值	0x04	PQC算法签名	无
	0x05	传统算法签名	PQC算法签名
	0x06	传统算法签名与PQC算法签名	无

3　可行性分析

为验证本文提出的后量子密码集成方案在小区广播系统中的适用性与可实施性，本节从计算资源开销、存储资源占用和消息长度适配性3个方面开展系统性分析。实验部署于中国电信研究院上海资源池的虚拟化平台，虚拟化环境为QEMU；硬件平台基于国产化鲲鹏处理器（2×Kunpeng 920@2.6 GHz），采用aarch64架构，配置为2核CPU及8 GB内存；软件环境使用国产服务器操作系统CTyunOS 22.06；密码算法支持基于OpenSSL 3.4.1、liboqs 0.13.0及oqs-provider 0.9.0构建。

3.1　计算资源开销评估

为评估PQC算法在签名生成与验证阶段的性能表现，本节基于第2.2节提出的PQC算法选型原则，选取ML-DSA、Falcon、SLH-DSA（SPHINCS+）、CROSS和MAYO 5类主流PQC数字签名算法

（每类算法包含多种安全等级的子算法），并与传统公钥算法SM2和ECDSA进行对比。实验基于OpenSSL 3.4.1框架，采用liboqs作为PQC算法源，并通过oqs-provider开源库实现相关算法在OpenSSL中的集成与调用。首先，利用随机数生成器构造一个长度为1 230 byte的数据包，用以模拟小区广播系统中安全消息体的最大长度[12,28]；随后，针对每种算法分别生成对应的公私钥对，并使用该密钥对数据包进行签名与验签操作。每个算法均重复运行1 000次，记录总耗时并计算平均执行时间。后量子密码算法与传统密码算法在签名生成与验证过程中的性能对比如图6所示。

实验结果显示，传统SM2和ECDSA-p256算法在签名与签名验证效率方面优于ML-DSA、Falcon等PQC算法。其中，ML-DSA和Falcon的签名时间较SM2增加0.6～0.7 ms，签名验证时间增加0.3～0.4 ms；而SPHINCS+、MAYO和CROSS等算法性能更接近传统算法，其签名时间增加0.4～0.5 ms，签名验证时间增加0.2～0.3 ms。尽管PQC算法引入了一定的性能开销，但所有算法的单次签名与签名验证操作均控制在8～9 ms，显著低于国家标准《公共预警短消息业务技术要求》（GB/T 32634—2016）规定的广播消息端到端时延上限（10 s），具备工程应用可行性。通过软件优化或硬件加速手段有望进一步缩小PQC算法与传统算法之间的性能差距。

3.2　存储资源占用分析

为评估后量子数字证书的存储开销，本节基于第2.3节提出的后量子数字证书设计方案，选取纯后量子证书、混合证书及组合证书，并与传统SM2和ECDSA证书的大小进行对比。实验基于OpenSSL框架，采用liboqs作为PQC算法实现库，并通过oqs-provider开源模块完成相关算法在OpenSSL中的集成与调用。PQC算法采用oqs-provider中定义的OID进行标识，所有证书的CN字段统一设置为“China Telecom Cell Broadcast Service”，有效期均为365天，并以PEM格式进行存储。为避免操作系统文件存储机制对结果的影响，实验中记录的是证书的实际大小，而非磁盘占用空间。PQC数字证书与传统数字证书尺寸对比如图7所示。

实验结果显示，不同算法生成的数字证书大小存在显著差异，传统SM2和ECDSA-p256算法的证书大小约为0.63 KB，而后量子算法及其组合方案的证书大小增加了数倍至数十倍。其中，Falcon系列证书平均为2.5～2.7 KB，MAYO系列为2.9～9.4 KB，ML-DSA系列为5.4～10.4 KB，

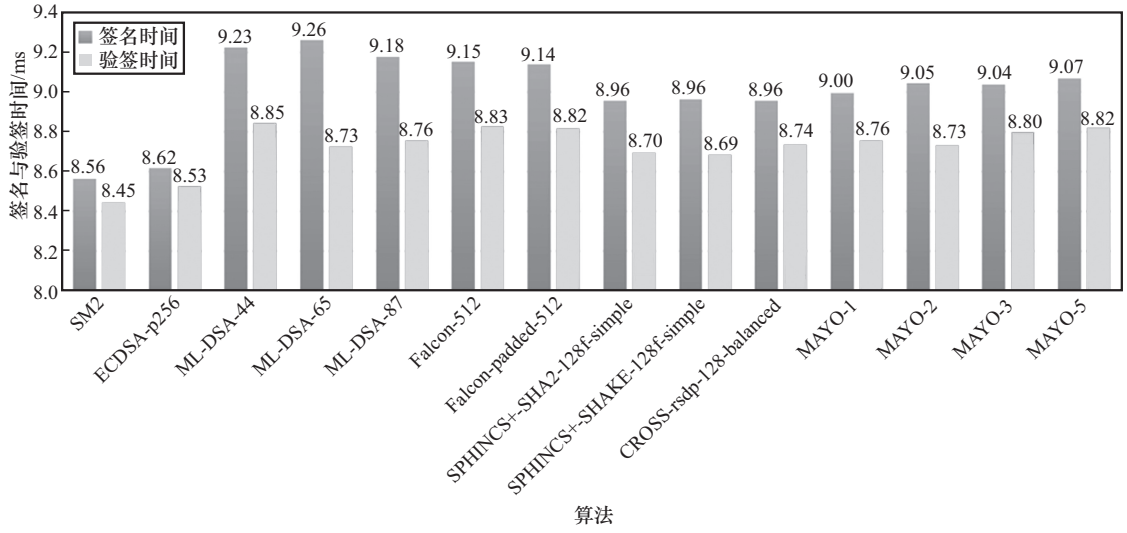
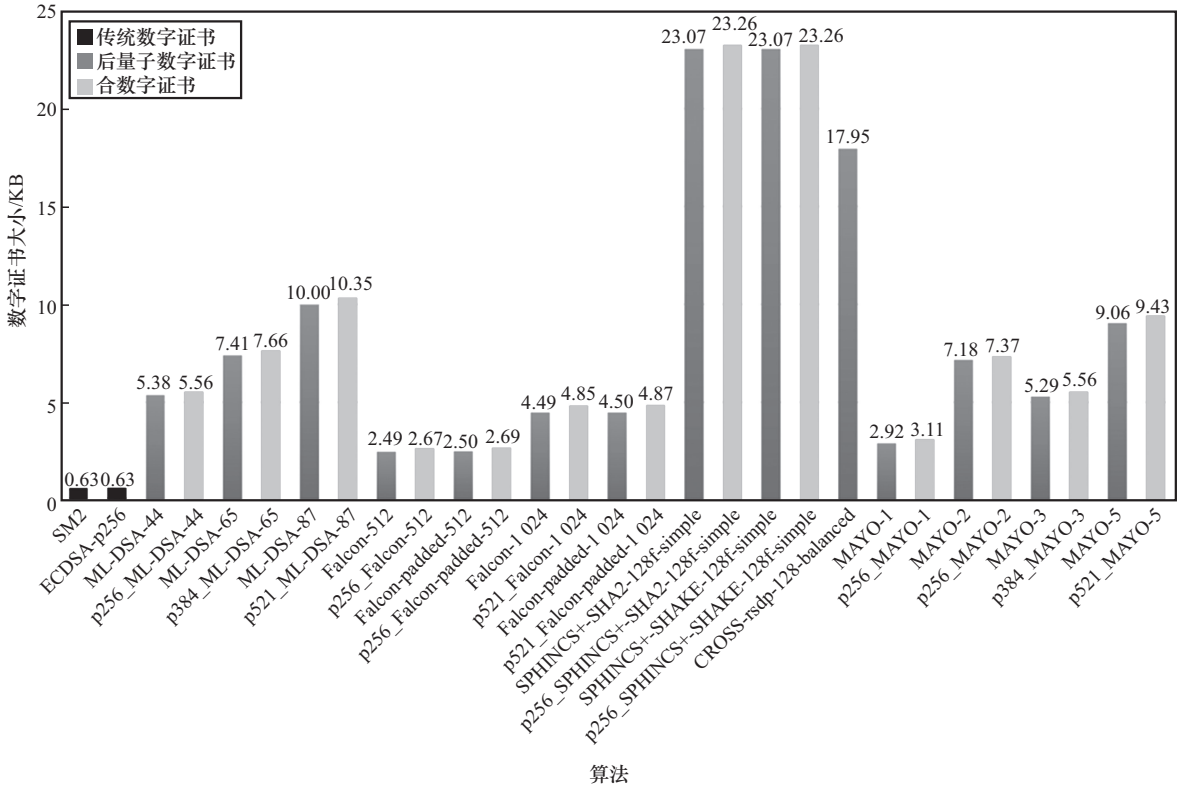


图6　后量子密码算法与传统密码算法在签名生成与验证过程中的性能对比



注：组合证书与混合证书大小基本一致，故以组合证书为代表参与存储开销对比分析。

图7　PQC数字证书与传统数字证书大小对比

CROSS系列约18 KB，SPHINCS+系列为23 KB。尽管现代智能手机通常具备GB级的存储容量，但实际分配给该功能模块的可用存储空间可能较为有限。因此，在算法选型时应优先考虑证书大小较小的方案。对于SPHINCS+或CROSS类证书大小较大的算法，建议结合证书格式精简与存储优化策略降低对终端存储资源的依赖。

3.3　消息长度适配性评估

根据行业标准[13,32]要求，小区广播安全消息体的最大长度限定为1 230 byte，因此需评估签名长度对消息结构的影响。PQC算法与传统算法签名长度对比如图8所示。

数据显示，传统签名算法SM2和ECDSA的签名长度均为64 byte，显著小于各类PQC算法。Mayo系列具有较明显的轻量化特征，其中Mayo-2的签名长度为186 byte，符合标准要求；Falcon-Padded-512的签名长度为666 byte，在合理预留其他字段空间后可满足标准要求。ML-DSA系列签名长度随安全参数提升呈阶梯式增长，分别为2 420 byte（ML-DSA-44）、3 309 byte（ML-DSA-65）和4 627 byte（ML-DSA-87），均超出标准限制。SPHINCS+和CROSS-rsdp-128-balanced的签名长度分别高达17 088 byte和13 152 byte，远超标准要求。

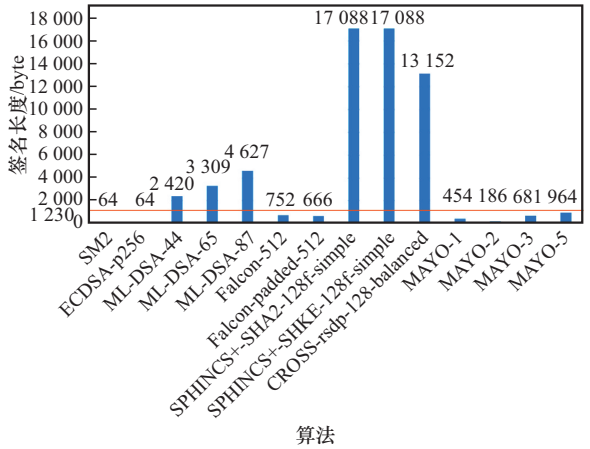


图8　PQC算法与传统算法签名长度对比

综合分析表明，Mayo 和 Falcon 系列签名长度较小，具备良好的部署可行性，而 ML-DSA 需配合协议优化才能实用化，SPHINCS+ 和 CROSS 系列在当前架构下适用性有限。建议在系统部署与升级过程中，优先选用适配性强的签名方案，以兼顾消息安全性、运行效率与结构稳定性。

4　结束语

目前，基于数字签名的小区广播系统已进入试点阶段，具备广泛部署的应用前景。本文在系统设计初期前瞻性地引入 PQC 算法，提出一种安全增强架构，并通过实验验证了其可行性，为应对量子计算威胁下的系统安全演进提供了可行的技术路径与实证支持。

值得一提的是，PQC 算法的安全性仍在持续评估中，其实用性与部署成熟度尚处于早期阶段。本文聚焦于 NIST 标准化算法在小区广播场景中的工程适配性，旨在为 PQC 迁移提供技术支撑。然而，系统的安全性本质上依赖于底层算法的长期抗破解能力。一旦算法被攻破，历史签名的真实性将无法保障，且尚无有效的密码学手段予以补救。因此，数字签名的长期真实性保障仍是一个开放性挑战，最终商用部署需遵循届时权威的 PQC 标准。

未来研究可聚焦于以下方向：（1）高并发场景下的系统响应效率与稳定性验证，建立可量化的性能基准；（2）5G 网络中域内 TLS 与域间 IPSec 协议的 PQC 安全增强，实现小区广播网元与核心网的安全联动；（3）面向算法破解风险的弹性信任机制，探索多算法冗余、敏捷更新等策略，提升系统的长期安全韧性。

参考文献：

[1] 王景丽, 赵宇 . 预警信息传播需求与通信网传播渠道匹配研究[J]. 电信科学, 2022, 38(5): 104-113.
WANG J L, ZHAO Y. Study on the matching scheme between early warning information dissemination demands and communication network dissemination channels[J]. Telecommunications Science, 2022, 38(5): 104-113.

[2] 王柯, 刘颖杰, 宋瑛瑛, 等 . 全民早期预警行动计划: 预警技术发展和监管政策研究[J]. 信息通信技术与政策, 2024, 50(11): 63-70.
WANG K, LIU Y J, SONG Y Y, et al. Early warnings for all action plan, early warning technology development and regulatory policies research[J]. Information and Communications Technology and Policy, 2024, 50(11): 63-70.

[3] 李晓华, 郄卫军, 姚平 . 应急预警下的小区广播技术综述[J]. 信息通信技术与政策, 2019(11): 31-35.
LI X H, QIE W J, YAO P. A survey on cell broadcast in emergency situation[J]. Telecommunications Network Technology, 2019(11): 31-35.

[4] NIST. Module-lattice-based key-encapsulation mechanism standard: FIPS 203[S]. 2023.

[5] NIST. Module-lattice-based digital signature standard: FIPS 204[S]. 2023.

[6] NIST. Stateless hash-based digital signature standard: FIPS 205[S]. 2023.

[7] NIST. Transition to post-quantum cryptography standards: NIST IR 8547[R]. 2024.

[8] NCSC. Timelines for migration to post-quantum cryptography[EB]. 2025.

[9] European Commission. A coordinated implementation roadmap for the transition to post-quantum cryptography[EB].2025.

[10] CCCS. Roadmap for the migration to post-quantum cryptography for the Government of Canada: ITSM.40.001[EB].2025.

[11] 3GPP. Technical realization of cell broadcast service (CBS): TS 23.041.v18.6.0[S]. 2024.

[12] 中国通信标准化协会 . 基于数字签名的小区广播业务安全技术要求: YD/T 6353—2025[S].2025.
CCSA. Security technique requirements of cell broadcast service based on digital signature: YD/T 6353—2025[S].2025.

[13] 3GPP. Study on the support of 256-bit algorithms for 5G: TR 33.841.v16.1.0[R]. 2019.

[14] 3GPP. New WID on addition of 256-bit security algorithms: SP-231159[S]. 2023.

[15] 3GPP. New SID on study on enabling a cryptographic algorithm transition to 256-bits: SP-231788[S]. 2023.

[16] 3GPP. New WID on addition of milenage-256 algorithm: SP-

231792[S]. 2023.

[17] ETSI. Cyber; Migration strategies and recommendations to quantum safe schemes: TR 103 619[R]. 2020.

[18] ITU-T. Security guidelines for applying quantum-safe algorithms in IMT-2020 systems: X.1811[S]. 2021.

[19] 后量子密码应用研究报告[R]. 2023.
Research report on post-quantum cryptography applications[R]. 2023.

[20] NIST. Recommendation for key management: Part 1 - General: SP 800-57 Part 1 Rev. 5[R]. 2020.

[21] NIST. Status report on the third round of the NIST post-quantum cryptography standardization process: IR 8413[R]. 2022.

[22] NIST. Post-quantum cryptography: additional digital signature schemes[EB]. 2025.

[23] Information technology – open systems interconnection-Part 8: The Directory: Public-key and attribute certificate frameworks: ISO/IEC 9594-8: 2020[S]. 2020.

[24] 荆继武, 林璟锵, 冯登国 . PKI 技术[M]. 北京: 科学出版社, 2008.
JING J W, LIN J Q, FENG D G. Technologies on public key infrastructure[M]. Beijing: Science Press, 2008.

[25] WANG C L, XUE W J, WANG J R. Integration of quantum-safe algorithms into X509v3 certificates[C]//Proceedings of the 2023 IEEE 3rd International Conference on Electronic Technology, Communication and Information (ICETCI). Piscataway: IEEE Press, 2023: 384-388.

[26] IETF. Composite ML-DSA for use in X.509 public key infrastructure: draft-ietf-lamps-pq-composite-sigs-12[S]. 2025.

[27] IETF. Convertible forms with multiple keys and signatures for use in Internet X509 certificates: draft-sun-lamps-hybrid-scheme-01[S]. 2025.

[28] 工业和信息化部(通信). 公共预警短消息业务技术要求: GB/T 32634—2016[S].2016.
MIIT. Technical requirements of short message service for public early warning: GB/T 32634—2016[S]. 2016.

[作者简介]

王聪丽（1994– ），女，中国电信股份有限公司研究院工程师，主要研究方向为公钥基础设施、后量子密码、商用密码应用安全性评估等。

薛伟佳（1990– ），女，博士，中国电信股份有限公司研究院工程师，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。

王靖然（1995– ），女，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、后量子密码等。

王锦华（1982– ），男，中国电信股份有限公司研究院工程师，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。

卢洪涛（1977– ），男，中国电信股份有限公司研究院高级工程师，主要研究方向为应急通信、移动通信、低空经济等。