

2026-2031年中国后量子密码行业深度调研及发展前景预测报告

报告简介

后量子密码(Post-Quantum

Cryptography, PQC)是专为抵御量子计算攻击而设计的新颖公钥密码体系,其核心在于通过数学难题的量子计算抗性构建安全基础。传统密码算法(如RSA、椭圆曲线加密)的安全性依赖于大整数分解、离散对数等在经典计算机上难以高效求解的数学问题,但量子计算机的Shor算法可在多项式时间内破解这些难题,导致现有公钥体系面临失效风险。后量子密码则基于尚未被量子算法有效解决的数学困难问题,如格理论(最短向量问题SVP、最近向量问题CVP)、多变量二次方程组求解、编码理论中的译码难题(如McEliece体制)以及哈希函数的单向性等,通过重构密码算法结构,确保在量子计算环境下仍能提供可靠的安全保障。

后量子密码行业研究报告主要分析了后量子密码行业的国内外发展概况、行业的发展环境、市场分析(市场规模、市场结构、市场特点等)、竞争分析(行业集中度、竞争格局、竞争组群、竞争因素等)、产品价格分析、用户分析、替代品和互补品分析、行业主导驱动因素、行业渠道分析、行业赢利能力、行业成长性、行业偿债能力、行业营运能力、后量子密码行业重点企业分析、子行业分析、区域市场分析、行业风险分析、行业发展前景预测及相关的经营、投资建议等。报告研究框架全面、严谨,分析内容客观、公正、系统,真实准确地反映了我国后量子密码行业的市场发展现状和未来发展趋势。

本研究咨询报告由北京中道泰和信息咨询有限公司领衔撰写,在大量周密的市场调研基础上,主要依据了国家统计局、国家商务部、国家发改委、国家经济信息中心、国务院发展研究中心、全国商业信息中心、中国经济景气监测中心、51行业报告网、全国及海外多种相关报刊杂志的基础信息以及专业研究单位等公布和提供的大量资料。对我国后量子密码行业作了详尽深入的分析,是企业进行市场研究工作时不可或缺的重要参考资料,同时也可作为金融机构进行信贷分析、证券分析、投资分析等研究工作时的参考依据。本报告也可以用于专精特新“小巨人”申请申报。

报告目录

第一章 后量子密码行业基本概念与发展背景

第一节 后量子密码的定义与技术内涵

- 一、后量子密码的基本定义及其在信息安全体系中的定位
- 二、后量子密码与传统公钥密码的根本性差异
- 三、后量子密码应对量子计算威胁的核心机制

第二节 后量子密码关键技术路线分类

- 一、基于格的密码方案
- 二、基于编码的密码方案
- 三、基于多变量多项式的密码方案
- 四、基于哈希的签名方案
- 五、基于超奇异同源的密码方案

第三节 密码敏捷性与后量子迁移基础

- 一、密码敏捷性的定义与实现架构
- 二、混合加密模式在迁移过程中的作用
- 三、密钥管理、证书生命周期与协议层适配挑战

第二章 全球后量子密码行业发展现状分析

第一节 国际标准化进程与政策推动

- 一、美国国家标准与技术研究院(nist)pqc标准化时间线
- 二、欧洲电信标准协会(etsi)与欧盟enisa后量子安全路线图
- 三、日本、韩国、加拿大等国家政府支持计划与试点项目

第二节 全球市场规模与区域分布

- 一、2023-2025年全球后量子密码市场容量(单位：亿美元)
- 二、北美、欧洲、亚太及其他地区市场份额变化
- 三、主要增长驱动因素：量子计算进展、合规要求、网络安全事件

第三节 全球技术竞争格局与生态构建

- 一、国际科技巨头布局
- 二、专业pqc初创企业崛起
- 三、开源社区与学术合作对技术扩散的影响

第三章 中国后量子密码行业发展环境分析

第一节 宏观政策与国家战略支撑

- 一、《中华人民共和国密码法》对后量子密码的引导作用
- 二、“十四五”国家信息化规划中量子安全相关内容
- 三、关键信息基础设施安全保护条例对pqc部署的潜在要求

第二节 技术创新与科研基础

- 一、国家重点研发计划“网络空间安全”专项支持情况
- 二、清华大学、中国科学技术大学、中科院信息工程研究所等机构成果
- 三、国家密码管理局推动的pqc算法征集与评估机制

第三节 产业生态与资本支持

- 一、2023-2025年国内pqc相关融资事件统计
- 二、科创板对密码安全类企业的上市通道优势
- 三、地方政府产业园区对pqc企业的落地扶持政策

第四章 中国后量子密码市场运行分析

第一节 市场规模与结构特征

一、2023-2025年中国后量子密码行业市场规模(亿元人民币)

二、软件、硬件、服务三大细分市场占比变化

三、政府采购、金融自建、互联网平台采购比例分析

第二节 产品形态与技术成熟度

一、pqc算法库、sdk、api接口产品化程度

二、支持pqc的密码机、智能密钥、安全网关等硬件出货量

三、云原生pqc服务(pqcaas)初步商业化探索

第三节 区域发展格局与产业集群

一、北京、上海、深圳、杭州等地pqc企业聚集效应

二、成渝、武汉、西安等中西部城市试点应用进展

三、地方专项政策对比：补贴、测试平台、人才引进

第五章 后量子密码产品分类与技术体系详解

第一节 软件类产品

一、通用pqc算法库(c/c++、java、python等语言支持)

二、tls 1.3扩展模块与pqc兼容中间件

三、密钥管理系统(kms)对pqc的支持能力

第二节 硬件类产品

一、服务器密码机、金融数据密码机集成pqc能力

二、usb key、智能ic卡等终端设备轻量化pqc实现

三、专用pqc加速芯片与fpga原型验证

第三节 服务与解决方案

一、pqc迁移咨询与风险评估服务

二、混合加密系统设计与部署服务

三、密码敏捷架构改造整体解决方案

第六章 密码敏捷性与后量子迁移路径分析

第一节 密码敏捷架构设计原则

一、协议层、应用层、密钥管理层的解耦机制

二、动态算法切换与回滚能力实现

三、与现有pki/ca体系的兼容策略

第二节 迁移阶段划分与实施路线

一、评估阶段(2023-2025年)：资产盘点、风险识别、poc验证

二、试点阶段(2026-2027年)：重点行业小范围部署

三、规模化阶段(2028-2030年)：强制替换与全面商用

第三节 迁移成本与性能影响实测

一、2023-2025年典型场景pqc性能开销测试数据(密钥生成、签名、验证时间)

二、带宽、存储、计算资源增量分析

三、不同行业可接受性能阈值调研结果

第七章 下游应用领域需求分析

第一节 金融行业

一、央行数字货币(dc/ep)对长期密钥安全的需求

二、银行核心交易系统、跨境支付平台pqc改造计划

三、证券登记结算、保险保单存证等场景适配性

第二节 政务与关键信息基础设施

一、国家电子政务外网pqc试点工程进展

二、电力调度、轨道交通、水利监控系统安全加固需求

三、密评(密码应用安全性评估)纳入pqc指标预期

第三节 通信与互联网

一、5g核心网信令面pqc可行性研究

二、大型云服务商内部安全演进

三、物联网设备固件签名与远程更新pqc方案

第四节 国防与航天

一、军用通信抗量子攻击能力建设要求

二、卫星遥测遥控指令长期保密需求

三、国产化替代背景下pqc自主可控优先级

第八章 中国后量子密码行业领先企业分析

第一节 中电科网络安全科技股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第二节 启明星辰信息技术集团股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第三节 天融信科技集团股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第四节 三未信安科技股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第五节 飞天诚信科技股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第六节 数盾信息科技股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第七节 北京格尔软件股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第八节 中孚信息股份有限公司

一、企业概况与发展历程

二、核心业务与产品结构

三、技术优势与创新能力

四、市场份额与竞争地位

五、未来发展战略与规划

第九章 全球与中国后量子密码技术对比分析

第一节 算法路线选择差异

一、nist选定算法 vs 中国自主算法(如sm-pqc系列)

二、专利自由实施(fto)风险对比

三、性能、安全性、实现复杂度综合评估

第二节 工程化与生态成熟度

一、国际pqc开源库(open quantum safe)成熟度

二、中国pqc参考实现与测试工具链短板

三、开发者社区活跃度与文档完善度

第三节 标准互认与出口合规

一、中国pqc产品进入欧美市场的认证障碍

二、gdpr、ccra等法规对pqc部署的影响

三、一带一路国家技术标准跟随可能性

第十章 中国后量子密码行业竞争格局分析

第一节 市场集中度与竞争梯队

一、cr5、hhi指数测算结果

二、国家队(央企背景)、民营安全厂商、初创企业三分天下

三、新进入者主要来自密码芯片与云安全领域

第二节 商业模式创新

一、按调用量计费的pqc api服务

二、pqc即服务(pqcaas)订阅模式

三、与操作系统、浏览器厂商预装合作

第三节 并购与联盟动态

一、2023-2025年行业并购事件梳理

二、中国密码学会pqc工作组成员合作机制

三、产学研联合实验室建设案例

第十一章 2026-2031年中国后量子密码市场需求预测

第一节 总体市场规模预测

一、2026-2031年市场规模(亿元)及复合增长率

二、分年度驱动因素：政策强制、事件催化、技术成熟

三、潜在市场天花板与渗透率极限测算

第二节 分产品需求预测

一、pqc软件库与sdk市场占比提升趋势

二、硬件安全模块(hsm、密码卡)需求爆发期(2028年起)

三、迁移咨询与测试验证服务蓝海市场

第三节 分行业需求预测

一、金融行业2027年后进入强制迁移窗口

二、政务系统2028年完成省级平台改造

三、通信、能源、交通等行业2029-2030年跟进部署

第十二章 供给能力与产业链安全分析

第一节 研发投入与人才储备

一、2023-2025年高校密码专业招生与就业数据

二、企业研发人员占比与薪酬竞争力

三、国家级重点实验室建设进展

第二节 供应链安全与国产化

一、pqc芯片依赖进口fpga风险分析

二、国产risc-v cpu支持pqc指令集进展

三、安全操作系统(如麒麟、统信)pqc适配计划

第三节 产能与测试验证瓶颈

一、头部企业2026-2031年扩产计划

二、国家级pqc测试平台建设滞后问题

三、算法实现一致性与互操作性认证缺失

第十三章 2026-2031年政策监管与合规环境展望

第一节 国家密码管理局政策动向

- 一、pqc产品纳入商用密码认证目录时间预测
- 二、密评2.0版本强制要求pqc评估条款
- 三、关键信息基础设施pqc部署时间表

第二节 国际合规挑战

- 一、美国出口管制条例(ear)对pqc技术限制可能性
- 二、欧盟网络安全认证框架(eucc)对pqc要求
- 三、中国企业出海面临的本地化合规成本

第三节 行业自律与标准体系

- 一、团体标准向行业/国家标准转化路径
- 二、中国自主pqc算法标准体系构建
- 三、开源pqc项目知识产权治理机制

第十四章 投资机会与风险预警

第一节 高潜力细分赛道

- 一、pqc专用芯片设计企业
- 二、垂直行业迁移解决方案提供商
- 三、pqc测试工具与渗透测试服务商

第二节 主要风险因素

- 一、nist标准变更导致技术路线重选
- 二、量子计算机实用化时间不确定引发需求延迟

三、中小企业因性能开销放弃pqc部署

第三节 投资策略建议

- 一、优先布局具备政府/军工订单能力的企业
- 二、关注拥有核心算法专利与fto分析能力的标的
- 三、规避无实际产品仅靠概念融资的初创公司

第十五章 国际合作与“走出去”战略

第一节 技术标准国际合作

- 一、参与iso/iec jtc1 sc27、ietf等国际组织
- 二、推动中国pqc算法纳入国际标准可能性
- 三、中美欧三方技术对话机制建立前景

第二节 一带一路市场拓展

- 一、东南亚、中东、非洲对pqc认知与需求萌芽
- 二、中国pqc产品性价比与本地化服务优势
- 三、联合当地运营商提供整体安全解决方案

第三节 应对技术脱钩策略

- 一、构建自主可控pqc生态闭环
- 二、加强与非美系芯片、云厂商合作
- 三、发展多边技术联盟降低地缘政治风险

第十六章 可持续发展与社会影响评估

第一节 绿色计算与能效挑战

- 一、pqc算法碳足迹测算(vs rsa-2048/ecc-256)
- 二、数据中心pqc部署对pue影响评估

三、低功耗pqc算法优化研究方向

第二节 人才教育与公众认知

一、中小学网络安全课程纳入pqc科普内容

二、高校设立pqc微专业与实训基地

三、cisp-pqc等职业认证体系完善

第三节 伦理与全球治理

一、pqc是否加剧发展中国家数字鸿沟

二、政府大规模监控能力与公民隐私平衡

三、全球密码治理话语权争夺与中国角色

图表目录

图表：2023年全球后量子密码市场规模(亿美元)

图表：2024年全球后量子密码区域市场份额

图表：2025年全球后量子密码技术路线占比

图表：2023-2025年nist pqc标准化关键节点

图表：2023年中国后量子密码行业市场规模(亿元)

图表：2024年中国后量子密码市场增长率

图表：2025年中国后量子密码下游应用结构

图表：2023-2025年基于格密码方案市场渗透率

图表：2024年长三角后量子密码企业数量分布

图表：2025年京津冀pqc政府采购金额

图表：2023年全球后量子密码专利申请量top10机构

图表：2024年中国高校pqc相关论文发表数量

图表：2026-2031年中国后量子密码市场规模预测(亿元)

图表：2027年金融行业pqc采购预算预测

图表：2028年政务云pqc改造完成率预测

图表：2029年通信行业pqc模块渗透率

图表：2030年能源行业pqc安全投入占比

图表：2026年pqc软件库市场占比预测

图表：2027年pqc硬件安全模块出货量预测

图表：2028年云pqc服务订阅用户数预测

图表：2023-2025年pqc算法性能对比

图表：2024年pqc在iot设备中的能耗测试数据

图表：2025年pqc与ecc加解密速度对比

图表：2026年pqc芯片国产化率预测

图表：2027年密码测评机构pqc检测能力覆盖率

图表：2028年“密评”强制包含pqc条款概率

图表：2023年全球pqc初创企业融资总额

图表：2024年中国pqc领域风险投资轮次分布

图表：2025年科创板密码安全类企业平均市盈率

图表：2026年东南亚国家pqc需求指数预测

图表：2027年中东政府pqc采购意向调查结果

图表：2023年pqc算法碳排放强度测算

图表：2024年高校密码专业毕业生就业去向

图表：2025年cisp-pqc认证持证人数

图表：2026年pqc开源项目活跃度排名

图表：2027年risc-v支持pqc指令集芯片出货量

图表：2028年零信任架构中pqc集成率

图表：2029年混合加密模式市场占比

图表：2030年全球pqc市场cr5集中度预测

把握投资 决策经营！

咨询订购 请拨打 400-886-7071 (免长途费) Email : kf@51baogao.cn

报告编号：4065951

本文地址：<https://www.51baogao.cn/baogao/20260328/4065951.shtml>

在线订购：[点击这里](#)