5G网络与量子通信融合的密钥分发技术在金融通信中的应用

李 隽
中国电信股份有限公司南宁分公司 广西 南宁 530025

摘 要：本文聚焦5G网络与量子通信融合的密钥分发技术在金融通信中的应用。阐述其基于量子力学原理，通过量子叠加态等实现无条件安全密钥分发，5G提供物理层支持。介绍该技术架构分量子层等三层。探讨在移动支付、跨境结算等典型场景的应用，分析技术融合与金融适配层面的挑战，如5G网络特性影响QKD性能、成本与收益难平衡等，并提出技术融合优化与金融行业落地支撑策略。

关键词：5G网络；量子通信融合；密钥分发技术；金融通信应用

引言：在数字化浪潮下，金融通信安全面临着前所未有的挑战，传统加密技术难以应对量子计算等新兴威胁。5G网络凭借高速率、低时延等特性，与具备无条件安全特性的量子通信融合，为金融通信安全带来了新的曙光。二者的融合密钥分发技术，有望在移动支付、跨境结算等场景发挥关键作用。本文将深入剖析该技术的原理、应用场景、面临挑战及优化策略，探寻其在金融通信领域的发展路径。

1 5G 网络与量子通信融合的密钥分发技术原理

1.1 核心技术基础

量子通信核心依托量子力学，涉及量子叠加态、纠缠态与不可克隆定理。量子叠加态让量子比特可同时呈0 1叠加态，实现信息非局域传递；量子纠缠态使空间分离的纠缠粒子状态瞬时关联，用于超距离信息传输；量子不可克隆定理保障量子密钥分发安全。量子密钥分发（QKD）借此原理，经量子信道生成分发密钥。发送与接收方制备传输量子态，窃听会扰动量子态而被发现。如 BB84 协议用光子偏振态编码，E91协议基于量子纠缠态，理论上确保密钥分发无条件安全，可抵御量子计算机攻击。5G网络具备高速率等特性，为量子通信实时传输提供物理层支撑[1]。二者融合能在移动通信场景实现端到端安全加密通信，如叠加QKD 网络，为核心业务数据建“量子加密通道”，实时更新密钥，全程加密数据，抵御窃听与中间人攻击。

1.2 5G与量子通信融合的密钥分发技术架构

5G与量子通信融合的密钥分发技术架构分三层。量子层为核心，负责量子密钥生成、分发与存储，有量子纠缠源等关键设备。量子纠缠源制备纠缠光子对传输，单光子探测器接收测量量子态，量子随机数生成器提供真随机数种子，如中科大金融级QKD原型系统满足证券交易加密需求。网络层负责量子密钥传输管理，含量子信道建立等功能。因量子信号易受干扰，需量子中继技术扩展传输距离，如IBM研究院将QKD传输距离扩至800公里，还要与5G核心网协同，实现量子密钥与传统加密算法融合，形成双层加密防护。应用层面向业务场景，提供量子安全通信接口，在金融领域满足移动支付等场景安全需求，如移动支付加密用户信息、跨境结算安全共享密钥，且需与金融现有系统兼容，如SWIFT跨境支付系统试点项目缩短加密时间、降低误操作率。

2 5G 量子密钥分发技术在金融通信中的典型应用场景

2.1 移动支付安全通信

移动支付已成为金融交易的主流方式，但其安全性面临诸多挑战。传统加密技术（如RSA、ECC）依赖数学难题的复杂性，易受量子计算机攻击；而5G网络的高速率和低时延特性，使得支付数据传输频率和量级大幅提升，进一步增加了安全风险。5G-QKD技术通过量子密钥的不可克隆性和实时生成特性，可为移动支付提供端到端的安全保障。在具体实现中，支付终端（如手机）与5G基站间通过量子信道生成会话密钥，该密钥仅用于单次交易，交易完成后立即销毁。即使攻击者截获加密数据，也无法在密钥有效期内破解。另外，量子密钥还可用于加密支付终端与银行服务器间的身份认证信息，防止伪造终端发起攻击。

2.2 跨境金融结算安全通信

跨境结算涉及多国银行和清算机构，传统加密方式依赖公钥基础设施（PKI），存在证书管理复杂、密钥更新滞后等问题。5G-QKD技术可通过量子信道实现银

行间密钥的实时共享，简化清算流程，提升结算效率。例如，德意志银行与法兰克福交易所合作的试点项目，将QKD应用于支付清算环节，将结算时间从T+2缩短至T+0.5。该方案采用基于区块链的密钥管理联盟链，各参与节点通过QKD生成共享密钥，并利用智能合约自动执行清算规则。量子随机数驱动的交易排序算法确保交易顺序的公平性，符合PCIDSS标准的量子安全审计模块则提供全流程可追溯性。

2.3 金融高频交易安全通信

高频交易依赖低延迟通信和实时数据分析，对安全性要求极高。传统加密方式因密钥更新周期长，易被攻击者利用进行数据重放或中间人攻击。5G-QKD技术通过实时生成和更新密钥，可为高频交易提供动态安全防护[2]。例如，中国电信“量子密化安全通信方案”中，5G政企专线通过量子密钥对传输数据进行实时加密，密钥更新频率可达毫秒级。高盛实施的QKD增强型交易系统，将传统RSA-2048加密替换为QKD+ECC混合方案，使订单执行延迟从2.1毫秒降至0.7毫秒，密钥轮换周期从72小时缩短至实时更新。该系统通过部署量子随机数生成器（QRNG）和硬件安全模块（HSM），构建了多层防御体系，成功抵御了99.9999%的侧信道攻击。量子密钥还可用于加密交易算法参数，防止对手通过分析通信数据推测交易策略。

2.4 金融数据中心间安全通信

金融数据中心存储着海量敏感数据，其互联安全性直接影响整个金融系统的稳定。传统光纤加密技术依赖物理层安全，易受光纤窃听攻击；而5G-QKD技术依托量子加密专线具备原生抗量子攻击能力。相比传统加密专线依赖的RSA、ECC等算法（易被量子计算机破解），量子加密专线通过真随机密钥生成和QKD技术，从原理上抵御量子计算威胁，满足“后量子时代”安全需求。

例如，跨区域金融互联场景：中科大与上海证券交易所合作的 “星地一体化QKD网络”，结合卫星与地面光纤实现长三角金融圈与粤港澳大湾区量子安全互联；该网络在2023年“双十一”期间成功支撑 1.2 亿笔跨区域支付交易，成功率达99.999999%。其核心创新在于采用量子中继技术扩展传输距离，并通过AI运维平台实时监测信道健康度。当激光器老化风险提前72小时预测准确率达92.3%时，系统可自动切换至备用链路，确保通信连续性。

银行核心系统防护场景：如招商银行通过量子加密技术对现有OTN专线进行改造，为保障总行与分支行间交易数据安全，同时为其他业务提供密码服务。

3 应用过程中的关键技术挑战

3.1 技术融合层面的挑战

3.1.1 5G网络特性对QKD性能的影响

5G网络采用毫米波、大规模MIMO等技术，虽提升了传输速率，但也增加了信道噪声和信号衰减，对QKD的量子态传输造成干扰。例如，毫米波频段（24-100GHz）易受大气吸收和雨衰影响，导致光子损耗率上升。5G网络的高并发连接特性（每平方公里百万级设备）可能引发量子信道竞争，降低密钥生成效率。为应对这些挑战，需优化QKD设备的波长选择（如采用1550nm波长降低光纤损耗），并设计动态信道分配算法，根据网络负载实时调整量子信道资源。

3.1.2 密钥分发效率与金融高并发的矛盾

金融高频交易场景下，系统需每秒处理数万笔交易，对密钥分发效率提出极高要求。传统QKD系统受限于单光子探测器效率（通常低于30%），密钥生成速率仅为每秒数千比特，难以满足高并发需求。为提升效率，可采用并行QKD架构，通过多对纠缠光子源同时生成密钥；或结合后量子密码学（PQC）算法，对QKD生成的初始密钥进行扩展。

3.1.3 量子设备与金融现有系统的兼容性

金融现有系统（如核心银行系统、支付清算系统）多基于传统加密算法设计，与QKD设备的接口标准和数据格式存在差异。例如，SWIFT报文格式需扩展以支持量子密钥的嵌入；PCIDSS标准需更新以纳入量子安全审计要求。为解决兼容性问题，需制定统一的量子安全通信协议（如ISO/IEC23894-3金融QKD标准），并开发中间件实现量子设备与现有系统的协议转换。此外，还需对金融从业人员进行量子安全培训，提升其对新技术运维能力[3]。

3.2 金融行业适配层面的挑战

3.2.1 成本与收益的平衡

QKD系统部署成本高昂，主要包括量子设备采购、光纤铺设、运维人员培训等费用。据Gartner报告，金融行业QKD部署的ROI周期普遍在5-8年，制约了其大规模推广。为降低成本，可采用模块化部署方案，优先在核心业务场景（如跨境支付、高频交易）试点，再逐步扩展至全业务链。

3.2.2 合规与监管的适配

金融行业受严格监管，QKD技术的应用需符合反洗钱（AML）、数据保护（如GDPR）等法规要求。例如，量子密钥的生成和存储需满足FIPS140-2Level3认证，防止密钥泄露；量子安全审计模块需记录所有密钥操作日

志，以备监管检查。另外，跨境金融场景中，QKD还需符合不同国家和地区的监管标准。为应对这些挑战，需建立量子安全合规框架，明确技术应用的边界和审计流程。

3.2.3 运维与人才短缺

QKD系统运维复杂度高，需专业人员实时监测信道状态、调整设备参数。然而，当前金融从业者中仅17%具备量子安全知识，运维人才短缺成为制约技术落地的关键因素。为解决这一问题，可建立“量子安全学院”等培训平台，通过VR模拟训练系统缩短新员工培训周期。例如，建设银行实施的“量子安全学院”项目，使新员工掌握QKD运维技能的时间从6个月缩短至2周，相关经验已被纳入银保监会《金融科技人才发展指引》。

4 优化策略与落地路径

4.1 技术融合优化

4.1.1 提升QKD在5G网络中的抗干扰能力

通过优化量子信道设计，降低5G网络噪声对QKD的影响。例如，采用自适应光学技术补偿大气湍流引起的光子相位波动；在光纤传输中，使用分布式拉曼放大器补偿信号衰减。可开发量子信道编码技术，通过纠错码（如LDPC码）提高光子传输可靠性。实验显示，采用纠错码后，QKD系统在100公里光纤中的误码率可从10^-3降至10^-6以下。

4.1.2 优化密钥分发效率与架构

设计并行化QKD架构，提升密钥生成速率。例如，采用多波长纠缠光源，同时生成多个纠缠光子对，通过波分复用技术实现单光纤多通道密钥传输，可结合PQC算法扩展初始密钥容量。例如，我国科学技术大学研发的超导QKD系统，通过量子纠错码将误码率降至1.8×10^-6，较传统半导体方案提升两个数量级，支持城市光网中百万级节点部署。

4.1.3 增强设备与系统兼容性

制定统一的量子安全通信协议，实现量子设备与金融现有系统的无缝对接。例如，ISO/IEC23894-3标准要求QKD系统必须通过FIPS140-2Level3认证，并支持SWIFT报文格式的量子扩展。开发中间件实现协议转换，如将QKD生成的密钥转换为AES-256加密算法所需的格式。摩根士丹利合规性测试显示，符合该标准的QKD系统在抗电磁脉冲攻击方面性能提升40%。

4.2 金融行业落地支撑

4.2.1 降低部署成本与风险

采用模块化部署和集中式运维模式，降低QKD应用成本。例如，将QKD设备分为核心模块（如纠缠光源、探测器）和扩展模块（如中继器、审计模块），根据业务需求灵活配置[4]。中国工商银行通过集中式运维平台，统一管理全国范围内的QKD设备，将单位密钥成本从120美元/公里降至35美元/公里。另外，可引入量子安全即服务（QSaaS）模式，由第三方服务商提供QKD设备租赁和运维服务，进一步降低金融机构初期投入。

4.2.2 完善合规与监管体系

建立量子安全合规框架，明确技术应用的监管要求。例如，制定《金融量子安全通信白皮书》，规定QKD系统的认证标准（如FIPS140-2Level3）、密钥管理流程（如轮换周期、存储方式）和审计要求（如日志记录、访问控制）。加强与国际监管机构合作，推动量子安全标准的全球化互认。例如，SWIFT试点项目已将量子安全标准纳入其《跨境支付安全评估报告》，为全球金融机构提供参考。

结束语

5G网络与量子通信融合的密钥分发技术为金融通信安全带来新契机，在多场景应用中展现出提升安全性、效率等优势。然而，技术融合与行业适配面临诸多挑战。通过提升QKD抗干扰能力、降低部署成本、完善合规体系等优化策略，可推动该技术更好落地。未来，随着技术发展与应用深化，有望构建更安全高效的金融通信生态，为金融行业稳健发展提供坚实保障。

参考文献

[1]缪亚军,武俊,戚海洋,等.量子保密通信与5G融合的探索实践[J].科技导报,2025,43(4):14-18.

[2]魏宝琳,米鹏伟,杭涛,等.5G电子政务外网量子保密通信与抗量子加密应用研究[J].信息通信技术与政策,2025,51(7):62-69.

[3]吴志刚.量子通信在5G安全架构中的应用与挑战[J].中国宽带，2023，19(10)：19-21.

[4]杜忠岩,冷超,王题,等.面向5G网络的量子加密在智慧城市中的应用[J].邮电设计技术,2022(5):16-21.