量子通信技术对信息保密性能的影响及展望

吴萨日娜
内蒙古电信股份有限公司通辽分公司　内蒙古　通辽　028000

摘　要：数字时代信息保密面临量子计算带来的传统加密技术破解风险，量子通信依托“量子不可克隆”“测不准原理”，为信息保密提供全新方案。分析其对信息保密性能的影响，可揭示其在提升保密强度、抵御破解风险上的核心优势，也能明确技术落地的现实挑战。这项研究能丰富信息安全技术理论体系，为金融、政务等行业选择保密技术提供参考，助力构建更可靠的信息安全屏障，推动信息保密技术向量子化升级。

关键词：量子通信技术；信息保密性能；加密机制；技术挑战；发展展望

引言

信息时代下，金融交易、政务数据、个人隐私等信息的保密直接关系社会稳定与个人权益，然而传统加密技术如 RSA 加密，在量子计算超强算力面前面临被破解的潜在风险，信息保密技术升级迫在眉睫。量子通信技术基于量子力学原理，具备独特的抗破解特性，在信息保密领域展现出巨大应用潜力，但当前其实际应用还存在技术瓶颈与场景适配问题。因此，系统梳理量子通信对信息保密性能的影响、分析挑战并展望未来，对推动技术发展具有重要意义。

1 量子通信技术对信息保密性能的核心影响机制

1.1 基于量子密钥分发（QKD）的加密强度提升机制

量子密钥分发（QKD）借助量子态传输生成密钥，从根源上增强了信息加密强度。传统加密密钥依靠数学算法生成，存在被量子计算破解的隐患，而 QKD 以光子的量子态（如偏振态、相位态）作为密钥载体，密钥生成过程与量子力学规律紧密绑定。通信双方通过传输量子态粒子，历经基矢比对、误码校验等步骤生成共享密钥，且密钥长度可依据需求动态调整。由于量子态无法被精准复制，任何窃取密钥的行为都会改变量子态，导致窃听被即时察觉，使生成的密钥具备 “绝对安全” 属性，大幅增强信息加密的抗破解能力。

在QKD过程中，单光子源发射单个光子，每个光子携带一个量子比特的信息，以特定的量子态进行编码。接收方使用合适的探测器对光子进行测量，根据测量结果与发送方进行信息比对和协商，从而确定最终的密钥。这种基于量子物理特性的密钥生成方式，摆脱了传统数学加密算法对计算复杂度的依赖，从根本上避免了因算法被破解而导致的密钥泄露风险。同时，QKD系统还可以结合量子纠错编码技术，进一步提高密钥生成的准确性和可靠性，即使在存在噪声和干扰的通信环境下，也能保证生成高质量的密钥，为信息加密提供坚实的保障。

1.2 借助 “量子不可克隆原理” 抵御信息窃取的防护机制

“量子不可克隆原理” 是量子力学的核心原理之一，其内涵为无法精准复制未知量子态，这一特性为防范信息窃取提供了天然防护。在传统通信中，攻击者可通过复制信息副本实现窃取且不被发现，而量子通信中，信息以量子态形式传输，若攻击者试图窃取信息，需先复制量子态，但 “量子不可克隆原理” 使其无法完成精准复制，且窃取行为会干扰量子态，导致传输的量子态发生改变。通信双方通过检测量子态的完整性，可立即发现窃听行为，及时终止通信或重新传输，从机制上杜绝了信息被窃取而不被察觉的可能。

这种基于 “量子不可克隆原理” 的防护机制，不仅在理论上具有绝对安全性，在实际应用中也展现出强大的优势。一方面，它不依赖于复杂的加密算法和密钥管理，减少了因算法漏洞或密钥泄露带来的安全风险。另一方面，由于量子态的改变是即时且不可逆的，攻击者无法通过多次尝试或改进技术手段来突破这种防护，使得信息在传输过程中的保密性得到了极大提升。此外，随着量子技术的不断发展，基于 “量子不可克隆原理” 的防护机制还将不断优化和完善，为信息保密提供更加可靠和高效的解决方案。

1.3 利用“量子纠缠”特性实现的跨域保密通信保障机制

“量子纠缠”指两个或多个量子粒子形成的关联状态，无论粒子间距离多远，一个粒子状态改变都会即时影响另一个粒子，这一特性为跨域保密通信提供了保障。在跨域通信场景中，可将纠缠量子对分别传输至通信双方所在区域，双方通过对本地量子粒子进行测量，

依据测量结果生成密钥或直接传输信息。由于纠缠量子的关联特性不依赖传统通信信道，信息传输无需经过中间节点，避免了传统跨域通信中中间节点可能存在的信息泄露风险。

在实际应用中，利用量子纠缠实现的跨域保密通信具有显著优势。一方面，由于量子纠缠的瞬时性和非局域性，通信双方可以在几乎零延迟的情况下完成信息的加密和解密过程，大大提高了通信效率。例如，在金融交易领域，这种高效的跨域保密通信可以确保交易指令的实时、安全传输，避免因信息延迟或泄露导致的交易风险。另一方面，量子纠缠通信不受地理距离的限制，无论通信双方相隔多远，只要能够建立量子纠缠通道，就可以实现安全的保密通信。这对于跨国企业、国际组织等需要频繁进行跨域信息交流的场景具有重要意义，能够有效保障其信息传输的安全性和保密性。

此外，量子纠缠通信还具有强大的抗干扰能力。在传统通信中，信号可能会受到各种电磁干扰、噪声等因素的影响，导致信息传输错误或丢失。而量子纠缠通信基于量子力学原理，其信息传输过程不受这些传统干扰因素的影响。即使存在一定程度的噪声和干扰，只要量子纠缠状态不被完全破坏，通信双方仍然可以通过纠错和恢复机制，准确获取传输的信息，从而确保跨域保密通信的可靠性和稳定性。

2 量子通信技术应用于信息保密的现存挑战

2.1 量子通信设备的技术成熟度与成本控制问题

当前量子通信设备的技术成熟度仍需提升，核心组件如量子光源、单光子探测器、量子存储器等，在稳定性与可靠性方面还无法满足大规模商用需求。例如，量子光源输出的光子纯度不足，易混入杂散光影响密钥生成精度；单光子探测器在高温环境下探测效率下降，限制了设备的适用场景。同时，设备成本居高不下，单光子探测器、量子加密终端等核心设备单价昂贵，且设备运维需要专业技术人员，进一步推高了应用成本，导致量子通信技术目前主要应用于政务、军事等高端领域，难以快速向民用领域普及。

技术成熟度不足不仅体现在核心组件性能上，还反映在设备集成度与工程化水平方面。现有量子通信设备多采用分立式架构，各模块间协同效率较低，导致系统整体功耗偏高且体积庞大，难以满足金融、医疗等民用场景对设备便携性的要求。此外，量子通信设备的制造工艺仍依赖高精度光学加工与低温真空环境，量产良品率不足30%，直接推高了单机生产成本。运维成本方面，由于量子系统对环境参数极度敏感，需配备恒温恒湿机房与专业校准设备，使得单站点年度维护费用超过传统通信设备的5倍，进一步制约了技术下沉速度。

2.2 量子通信网络的覆盖范围与多场景适配难题

量子通信网络的覆盖范围目前存在明显局限，受量子态传输特性制约，光子在光纤中传输会因损耗导致量子态衰减，当前单模光纤中量子通信的无中继传输距离通常在百公里级别，跨城市、跨国家的长距离传输需依赖量子中继器，但量子中继器技术尚未完全成熟，难以实现大规模部署。此外，多场景适配能力不足，不同应用场景（如城市光纤通信、卫星通信、移动终端通信）对量子通信的传输速率、延迟、抗干扰能力要求不同，现有量子通信网络多针对单一场景设计，缺乏能灵活适配多场景的统一技术架构，制约了技术的广泛应用。

在覆盖范围方面，量子通信网络的长距离传输难题尤为突出。以跨省际通信为例，即使采用最优品质的单模光纤，量子信号在传输500公里后信噪比会下降至初始值的1/10以下，导致密钥分发成功率不足40%。目前仅能在相邻城市间构建点对点量子链路，要实现全国性网络覆盖，需建设数千个量子中继节点，按当前每个中继站2000万元的造价计算，整体投资将超过千亿元规模。

多场景适配层面，现有技术方案存在显著短板。城市光纤场景要求传输延迟低于1ms，而移动终端场景需支持50km/h运动状态下的稳定连接，卫星通信场景则要承受-100℃至+120℃的极端温差。当前量子通信设备在温度适应性方面，仅能在-20℃至+50℃环境稳定工作，导致在高原、极地等特殊区域无法部署。更严峻的是，不同场景间的技术标准尚未统一，某军工项目曾因卫星端与地面站的量子编码协议不兼容，导致长达8个月的系统调试延误。

网络架构的灵活性同样制约发展。现有量子网络采用固定拓扑结构，新增节点需重新配置整个网络的量子态制备参数。某金融行业试点项目中，当接入第15个银行网点时，系统重构导致密钥分发中断达12小时。这种刚性架构使得网络扩容成本呈指数级增长，每增加一个节点，平均需追加35%的运维投入，严重阻碍了商业化推广进程。

2.3 量子通信与传统通信系统的兼容协同问题

量子通信与传统通信系统之间存在明显的兼容协同障碍，二者在技术架构、协议标准上差异显著，传统通信系统无法直接接入量子通信网络，需额外部署量子加密网关、协议转换设备等，增加了系统复杂度与成本。同时，协同工作机制不完善，在实际通信中，部分信息无需超高保密级别，可通过传统通信传输，部分敏感信

息需量子通信保障，但目前缺乏高效的信息分类传输与切换机制，易出现量子通信资源浪费或传统通信泄密风险。

3 量子通信技术在信息保密领域的未来发展展望

3.1 量子通信技术与 5G/6G 网络融合的保密应用方向

未来量子通信技术将与 5G/6G 网络深度融合，为移动通信提供更高安全级别的保密保障。5G/6G 网络支持海量设备连接与高速数据传输，但其传统加密技术面临量子计算威胁，量子通信可作为核心保密手段，与 5G/6G 网络的网络切片技术结合，为不同安全需求的业务（如车联网、远程医疗、工业控制）提供专属量子保密切片，实现数据传输的端到端量子加密。

为实现这一目标，需研发量子通信与5G/6G网络融合的适配层协议，解决量子密钥分发速率与5G/6G高速传输不匹配的问题。同时，构建智能化的业务安全分级系统，通过机器学习算法动态识别数据敏感等级，自动切换量子加密或传统加密通道。例如在车联网场景中，车辆控制指令采用量子保密切片传输，而娱乐信息则通过传统通道传输，既能保障核心安全又可控制成本。此外，还需制定量子-5G/6G融合设备的互操作标准，确保不同厂商设备间的量子密钥安全同步与业务连续性。

3.2 面向行业特殊需求的定制化量子保密方案

针对不同行业的特殊保密需求，将开发定制化量子保密方案，推动量子通信技术向垂直领域渗透。在政务领域，针对政务数据传输、电子政务签名等需求，设计基于量子密钥的政务保密通信系统，确保政策文件、公民信息等敏感数据不被泄露或篡改；在军事领域，针对战场通信、指挥控制等场景，开发抗干扰、抗截获的量子保密通信设备，保障军事信息的绝对安全。

3.3 量子通信标准化体系构建与国际合作发展方向

量子通信标准化体系的构建将成为未来发展的重要方向，需联合各国科研机构、企业制定统一的技术标准，包括量子密钥生成与管理标准、量子通信协议标准、设备接口标准等，解决技术碎片化问题，推动量子通信设备与网络的互联互通。同时，国际合作将进一步深化，量子通信技术的发展与应用具有全球性，单一国家难以独立应对量子计算带来的全球信息安全挑战，需通过国际合作共建全球量子保密通信网络，共享量子中继器、量子卫星等基础设施，联合开展量子通信技术研发，制定全球统一的量子信息安全规则，共同抵御全球性信息保密威胁。

4 结论

量子通信技术通过量子密钥分发、量子不可克隆原理、量子纠缠特性，从加密强度、抗窃取能力、跨域保障三方面革新了信息保密性能，其在信息保密领域的不可替代性显著，但当前面临设备成熟度低、网络覆盖有限、与传统系统兼容难等挑战。推动量子通信技术发展，需遵循 “技术突破、成本优化、场景适配” 原则，既要加强核心技术研发提升设备稳定性、降低成本，又要完善网络架构扩大覆盖范围，还要构建兼容协同机制实现与传统系统融合。

参考文献

[1]周德旺,皇安伟.量子通信助力信息安全保密[J].保密工作,2018,(08):6-8+1.

[2]项俊栋,方赟朋,姚海燕,等.量子通信技术在电力信息系统保密传输中的应用研究[J].数字通信世界,2024,(06):149-151.

[3]许德斌,裴友泉.运用量子通信技术实现档案（保密）信息传递的构想[J].档案学研究,2019,(05):127-132