量子通信技术在保密通信中的应用前景研究

包思诚[1]　蔡　韦[2*]
1.宁波港信息通信有限公司　浙江宁波　315000
2.杭州智数科技有限公司　浙江杭州　310000

摘　要：随着信息技术的快速发展和数据传输规模的不断扩大，传统加密手段面临愈发严峻的安全挑战，量子通信技术作为新一代信息安全的重要突破，以其基于量子力学基本原理的不可克隆性和测不准性，进而实现了通信过程中的无条件安全性。尤其是量子密钥分发（QKD）技术，已在多个国家和地区实现了实验性应用和初步部署，其展现出良好的技术成熟度和广阔的发展前景。本文围绕量子通信的基本原理、关键技术和系统构成展开分析，探讨其在保密通信中的应用优势与技术挑战，并对其未来发展趋势和应用前景进行深入研究，以期为推动量子通信技术在实际保密通信中的落地提供理论支撑和参考依据。

关键词：量子通信；保密通信；数据传输

序言

在信息时代，通信安全已经成为国家安全、经济发展和社会稳定的重要保障。随着计算能力的提升，传统基于数学难题的加密方法，如RSA与椭圆曲线密码体系，面临着被量子计算破解的潜在威胁。在此背景下，具有物理层面安全保障特性的量子通信技术应运而生。量子通信以量子力学为基础，利用量子比特的叠加性和不可克隆性等特性，实现密钥分发过程中被动窃听的可检测性，从根本上提高了通信系统的安全等级。当前，多个国家纷纷加大对量子通信的研发投入，构建量子通信网络并推动其与现有通信基础设施的融合，力图在未来的全球通信格局中占据先机。本文旨在系统梳理量子通信的理论基础与关键技术，针对其面临的主要问题与发展瓶颈，深入分析其在保密通信中的应用模式和实践路径，为实现高强度、广覆盖、可规模化的量子保密通信系统提供理论指导和实践思路。

作者简介：
包思诚（1989.8-）男，汉族，浙江宁波人，学历：本科，单位：宁波港信息通信有限公司，研究方向：通讯技术；
蔡韦（1982.2-）男，汉族，浙江杭州人，学历：本科，单位：杭州智数科技有限公司，研究方向：软件开发。

一、量子通信技术基础

（一）量子力学基本原理简介

量子通信的理论基础源于量子力学，其核心原理包括叠加原理、不确定性原理、测量坍缩和不可克隆定理。叠加原理指出微观粒子可以同时处于多个状态的叠加态，直到被测量时才坍缩为某一确定状态，这意味着信息可在多个状态之间编码，提升信息处理能力[1]。不确定性原理则规定了某些物理量，如位置和动量，或不同偏振态不能同时被精确测量，从而使得外部窃听者难以获取完整信息[2]。不可克隆定理明确指出，任意一个未知量子态不能被精确复制，这使得传统窃听方式难以应用于量子通信。基于这些原理，量子通信能够在理论上实现无条件安全的密钥传输和保密通信，为传统通信安全体系提供了根本性变革的方向[3]。

（二）量子通信的关键技术

量子通信技术作为未来信息安全的重要保障，利用量子力学原理实现了信息的无条件安全传输，任何窃听行为都会导致量子态变化而被立即发现，进而确保通信过程中的密钥绝对安全[4]。同时，量子通信能够有效抵御传统通信中常见的窃听和破解攻击，且量子纠缠特性使得远距离通信的安全性大幅提升，为构建全球量子安全网络提供了技术基础[5]。其关键技术主要包括以下三个方面：

第一，量子密钥分发技术（Quantum Key Distribution，QKD）。量子密钥分发是量子通信中最重要的技术，旨

在利用量子力学的不可克隆定理和测不准原理，实现双方安全共享随机密钥。典型的QKD协议包括BB84协议、E91协议等。BB84协议通过发送不同基态的单光子，实现密钥的安全传输；E91协议则基于量子纠缠态，增强安全性。QKD技术的关键挑战在于提高密钥生成率和传输距离，同时保证抗干扰和抗窃听能力。第二，量子态制备与传输技术。量子通信的核心是对量子态的精确制备和传输。量子态制备涉及单光子源或纠缠光子的高效生成技术，要求高纯度、低噪声以及稳定的输出。量子态传输主要依赖光纤或自由空间传输通道，必须克服光子衰减、散射和环境噪声对量子态的破坏。此外，量子中继和量子存储技术的研发对于延长通信距离和实现量子网络具有重要意义。第三，量子误差校正与隐形传态技术。由于量子态极其脆弱，量子误差校正技术成为保障量子通信系统稳定性的关键。该技术通过编码冗余和纠错机制，纠正传输过程中因环境噪声引起的量子态退相干和错误。另一方面，量子隐形传态技术允许将量子态在不直接传输量子本体的情况下，实现远距离的量子态转移，极大地提升了量子通信的安全性和灵活性，是构建大规模量子通信网络的重要手段。

（三）量子通信系统构成

一个完整的量子通信系统通常由量子信号源、量子信道、探测系统和经典控制系统组成。量子信号源负责产生特定的量子态，如单光子源或纠缠光源，是系统的核心部分。量子信道通常是光纤或自由空间通道，用于量子态的传输，其稳定性和损耗控制直接影响通信质量。探测系统则包括光子探测器，用于接收和测量量子信号，要求高灵敏度和低误码率。经典控制系统包括密钥协商、误码纠正与隐私放大模块，用于保障通信过程中密钥生成与传输的正确性与保密性。各子系统之间需高度协同，以实现稳定、实时、高保密性的通信过程。随着光子器件和通信协议的不断优化，量子通信系统的集成度和实用性持续提升，推动其向更大规模和更复杂应用场景迈进。

二、量子通信在保密通信中的优势与挑战

（一）主要优势分析

量子通信技术作为新一代信息安全手段，在保密通信领域展现出独特而显著的优势。首先，量子通信基于量子力学的基本原理，尤其是量子纠缠和量子不可克隆定理，实现了信息传输过程中的物理层安全。以量子密钥分发（QKD）为代表的应用可在不依赖第三方信任机制的前提下，实现通信双方之间的密钥共享，一旦存在窃听行为，将不可避免地扰动量子态，从而被通信双方立即察觉，确保密钥的绝对安全。其次，量子通信不依赖计算复杂性保障安全性，不受计算能力提升（包括未来可能的量子计算）所带来的破解威胁，这种“无条件安全”是传统加密技术无法实现的。随着光子通信技术的发展，量子通信具备较高的传输效率和良好的扩展性，进而在城域网、骨干网等场景中实现示范应用。

（二）当前面临的技术瓶颈

尽管量子通信技术具有显著优势，但其在实际应用中仍面临多项技术瓶颈。首先，量子信道的传输距离和稳定性仍受限于光子在光纤中传输过程中的衰减与噪声干扰，限制了其在大规模跨区域通信中的应用能力。虽然通过中继节点或量子中继理论可以延伸通信距离，但实际中量子中继器的工程化尚未成熟。其次，量子器件的性能和成本也是制约因素。目前，高质量单光子源、探测器等核心器件成本高昂，制造难度大，难以实现产业化批量应用。同时，系统复杂度高、环境适应性差也对其在复杂环境下的稳定运行构成挑战。此外，量子通信网络的组网架构、协议标准尚未完全统一，缺乏与现有传统通信网络的高效融合机制，限制了其在现有信息基础设施中的部署效率。

（三）与传统加密技术对比

量子通信与传统加密技术在安全原理与实现方式上存在本质差异。传统加密方法主要依赖数学算法和计算复杂度，如RSA、AES等加密标准，其安全性建立在大数分解或对称密钥破解所需的巨大计算量上。然而，随着计算能力的增强，尤其是量子计算的逐步发展，传统加密算法面临被攻破的风险。例如，Shor算法已被理论证明可在量子计算机上高效分解大数，从而威胁RSA等公钥体系的安全性。相比之下，量子通信利用量子力学中的测不准原理和不可克隆性，确保密钥传输的不可窃听性，具备物理层面的“无条件安全”。在遭受攻击时，量子通信系统能够即时识别攻击行为并终止通信，从而避免信息泄露。同时，传统加密依赖后期的密钥更新机制，而量子密钥分发可以持续生成新密钥，提升通信灵活性和抗疲劳性。但需要指出，当前量子通信尚无法完全取代传统加密，更多的是作为其补充或协同手段，尤其适用于对保密性要求极高的场景，如国防、金融、政府等领域。

三、量子通信在保密通信中的应用场景分析

（一）军事与国防保密通信

在军事与国防领域，信息的高度保密性直接关系到国家安全与战略部署的成败。传统通信方式在面对不断升级的网络攻击与窃听手段时，存在较大的安全隐患，而量子通信以其不可克隆性和量子不可测性的技术特性，为军事通信系统提供了新的安全保障。量子密钥分发（QKD）是当前最成熟的量子通信应用之一，其核心优势在于能够实时发现窃听行为，一旦通信链路被监听，系统即可中断密钥传输，保障信息安全不被泄露。在实战应用中，量子通信可以被用于战场信息传输、指挥系统联络以及军事卫星与地面站之间的加密通信。部分国家如中国和美国，已在高层次军事通信网络中部署量子通信试验系统。例如，中国“墨子号”量子科学实验卫星已实现地面与卫星之间的量子密钥交换，为全球范围的军事安全通信网络奠定了基础。

（二）政府与外交通信

政府部门与外交机构在日常工作中涉及大量的国家政策制定、国际谈判、情报交换等敏感信息，传统的加密通信手段已难以完全抵御日益复杂的网络攻击与信息泄露风险。在这一背景下，量子通信为政府与外交通信提供了前所未有的安全保障。通过量子密钥分发实现点对点的密钥安全传输，即使面对超级计算能力的攻击，也无法破解其加密机制。政府可以利用量子通信构建高安全级别的信息网络，用于国家政策的内部传递、机密文件的传输和高层领导人的通信保障。同时，量子通信在外交领域同样具有重要意义，能够有效防止国际间电文的窃取与篡改，保障谈判过程的私密性与真实性。近年来，多个国家纷纷启动量子通信在政府与外交系统的试点工程，例如，中国已在北京与上海之间建立了“京沪干线”量子通信主干网，并逐步接入党政机关的通信系统。

（三）金融与商业领域

金融行业对数据的安全性和保密性有着极高的要求，涉及账户信息、交易记录、资金流动等核心内容，一旦遭遇信息泄露，将导致严重的经济损失和信任危机。量子通信技术的引入，为金融机构提供了一种全新的安全通信手段，尤其是在金融数据传输和远程办公中具有极大的应用潜力。量子密钥分发可用于构建高度安全的专用通信通道，保障金融交易中的数据不被截获或篡改。银行、证券交易所、支付平台等关键节点可以通过量子网络实现内部数据传输的加密升级。同时，商业企业尤其是涉及高价值数据的科技公司和跨国集团，也可借助量子通信技术提升其商业机密的防护能力。例如，某些大型银行已经开始尝试部署量子加密链路，用于总部与分支机构之间的数据交换。在未来，随着量子通信设备的成本下降和技术标准的统一，金融行业和商业领域将迎来量子通信在大规模、实用化层面的快速发展，进一步推动全球数据安全格局的革新与重构

结语

综上所述，量子通信作为新一代信息安全技术的核心代表，凭借其基于量子物理的无条件安全优势，在保密通信领域展现出广阔的应用前景。无论是在军事、政府、金融等对信息安全要求极高的关键领域，还是在未来智慧社会的建设过程中，量子通信都将发挥至关重要的作用。尽管目前仍存在诸如传输距离受限、器件成本高、网络架构不成熟等技术瓶颈，但随着科学研究的深入和产业投入的持续，量子通信正逐步从实验验证走向实际应用。通过构建一个覆盖全球、标准统一、安全高效的量子通信网络，将成为国家信息战略竞争的重要高地。

参考文献

[1]吴忠平，王路杰，许佳诺，等.基于量子保密通信及5G硬切片专网的配网应用研究[J].电信科学，2022，38（1）：159-169.

[2]李宏伟，潘志远，黄继杰.一种基于双勾函数的数据加密算法研究[J].计算机技术与发展，2022，32（6）：120-125.

[3]李文清，刘津濂，齐晓曼，等.量子技术在电力领域的应用分析与展望[J].电力与能源，2022，43（1）：1-6.

[4]瞿迪庆，张万生，余侃，等.量子安全增强的电力5G配网终端技术测试与研究[J].网络空间安全，2022，13（1）：55-61.

[5]周晓东，王晟，张天兵，等.基于级联Polar码和多级译码方法的连续变量QKD数据协商协议[J].量子电子学报，2022，39（3）：411-417.