关于网络安全技术中的量子密码通信分析

段凤娟

（武警包头支队，内蒙古 包头 014060）

摘 要 信息技术飞速发展，全球互联和数据爆炸带来了前所未有的安全和隐私挑战。传统密码学基于数学难题的加密方法，在量子计算崛起的背景下，其安全性受到了严重威胁。量子密码学作为一种新兴的安全通信技术，凭借其基于量子力学的不可逆性和不可克隆性，为信息安全提供了全新的保障。本文对量子密码通信的原理、关键技术、应用前景以及面临的挑战进行了全面分析，以期为相关领域的研究和应用提供借鉴。

关键词 量子密码学；量子密钥分发；量子态；量子测量；网络安全

中图分类号：TN918.1 **文献标志码**：A **DOI**：10.3969/j.issn.2097-3365.2025.03.006

0 引言

在数字化时代，网络安全成为一个备受关注的议题。传统密码学在过去的几十年中发挥了重要作用，但随着量子计算的快速发展，其安全性受到了前所未有的挑战。量子密码学利用量子力学中的特殊性质，为信息安全提供了一种全新的解决方案。本文将深入探讨量子密码通信的原理、关键技术、应用前景以及面临的挑战，以期为相关领域的研究和应用提供有价值的参考。

1 量子密码的通信工作原理分析

量子通信技术将量子状态视为信息传递的核心元素，巧妙地利用了量子物理学的规则，实现了信息传输的高效性和安全性。这项创新不仅具有划时代的学术意义，在实际应用中也展现出巨大的扩展潜力[1]。它标志着量子物理保密技术从理论概念阶段走向现实的应用领域，为通信科技的发展带来了一个重要的转折点。量子通信技术之所以备受推崇，是因为它借助量子力学的本质属性带来的独特优势[2]。在量子通信领域，信息以量子状态的形式出现，表现出叠加性和纠缠性等特征，这使得量子信息在传输过程中具有无与伦比的安全性。当量子状态被用作信息编码时，任何企图复制或窃取信息的行为都会不可避免地干扰量子状态，导致状态的崩溃或变化。这种变化是即时且不可逆转的，因此为通信两端提供了明显的警示信号，确保了信息的安全性。量子通信技术的应用领域非常广泛，根据传输内容的不同，大致可以分为两大类：经典信息传输和量子信息传输。在经典信息传输领域，量子通信技术主要应用于量子密码学。量子身份证、量子密码和量子比特承诺等应用充分利用了量子状态的不可复制性和不可预测性，实现了信息的安全传输。例如，量子密码技术通过量子密钥分发（QKD）协议，能够在公共信道上安全地交换密钥。即使存在无限计算资源的攻击者，也无法获取量子密钥所保护的通信内容。

在量子信息传输方面，量子通信技术致力于实现量子遥传和量子通信网络的构建。量子遥传是一种利用量子纠缠状态实现远距离信息传送的技术，它能够在不直接传输物质粒子的情况下，将量子状态的信息从一个地点传送到另一个地点。这种技术不仅传输效率高，而且能够实现信息的完整复制和传递，为量子通信网络的构建提供了基石。量子通信网络的建设是量子通信技术走向实际应用的必经之路[3]。将量子通信设备与光纤通信网络相结合，可以构建出既安全又高效的量子通信网络。该网络不仅能实现信息的快速传输，还能确保信息传输的绝对安全，进一步保障了军事、金融等领域的信息安全。量子密码学作为量子物理学与量子密码学的结晶，为信息加密提供了全新的策略和途径。传统加密方法主要依赖于数学问题解决的复杂性来确保信息安全，但随着量子计算机的崛起，这些传统方法面临挑战。而量子密码技术则借助量子状态的特性，如不确定性原理和测不准原理等，实现了信息的绝对安全加密。这种加密方式不仅安全等级高，还能适应量子计算机发展的需求，为信息安全领域带来新的生机。

2 量子通信原理

量子信息处理与通信技术的深入探究，不仅深化了我们对量子物理基本法则的认知，同时也为信息安全、计算效率和通信效果的提升提供了创新路径。量

子体系是一个由多个依据量子力学规律运作的基本粒子组成的复杂结构。这些粒子，如电子和光子，在量子领域内表现出与经典物理截然不同的行为特性。量子信息处理研究的核心目标是利用这些独特的行为特性，将量子态作为信息传递的媒介，并结合信息理论，开创出一种新的信息处理模式[4]。

量子通信技术不仅拓展了经典信息论的边界，更融入了量子纠缠这一奇特的物理特性，催生了量子隐形传态这种震撼人心的传输手段。回溯至1993年，六位来自不同国家的科学家——以Bennett为首的团队，提出了一项创新的理论构想：将不明的量子状态信息拆分成两个部分，通过量子信道和经典信道将其发送给接收方。在此过程中，经典信息基于发送者对原始量子状态进行测量后的结果，而量子信息则包含了未被解析的其余信息。借助这些分割的信息，接收者能够准确地重建出最初的量子状态。此项发现打破了传统通信的壁垒，为量子通信技术的演变提供了坚实的理论基石。然而，在量子计算机的迅猛发展浪潮中，依赖于传统渠道安全及数学难题的密码系统面临着前所未有的威胁。现有的密码体系主要依赖于传统信道的安全属性和数学问题的性质来确保密码的安全性。但这种安全感是基于相对性的，尤其在量子计算机面前显得较为薄弱。1994年，Shor揭示了一个能在量子计算机上运作的算法，成功将大素数分解问题从NP问题简化为P问题，对传统密码系统构成了巨大挑战。为了对抗这种挑战，人们开始探索一种更加安全的加密通信系统——量子加密通信系统。量子加密通信的关键在于密钥分配过程，其安全性主要建立在量子力学的不确定性原理、量子不可克隆定理以及量子状态不可分割的特性之上。这些特性使得任何企图破坏量子状态的行为都将不可避免地触发量子状态的破坏，进而被通信双方所察觉。此外，量子加密通信中使用的密钥是一种一次性便笺密钥，这种加密技术在当代数学理论中已被证明是目前不可破解的密码。量子加密通信的实现，离不开量子密钥分配（QKD）技术的支持。QKD技术利用量子状态的叠加与纠缠特性，在通信双方之间安全地交换密钥。在QKD过程中，对量子状态的任何测量都会导致状态的坍缩，从而揭示任何破坏者的存在。量子隐形传态利用量子纠缠实现信息的超长距离传输，而量子网络则通过建立量子信道和量子节点，实现信息的快速、有效传输[5]。这些技术的发展，不仅加速了量子信息技术的跃进，也为未来量子互联网的构建提供了坚实的基础。

3 量子密码通信的关键技术

3.1 量子密钥分发（QKD）

量子密码术的中流砥柱——量子密钥分配技术，借助量子特性的精妙，使得两位通信者能够在高度安全的环境下交换不易被复制的秘密密钥。在QKD协议中，发送者（Alice）运用量子位元将随意的量子状态送到接收者（Bob）手中，Bob接受后进行量子检测，并与Alice共享检测成果，确立起一道安全的密钥防线。QKD面临的关键挑战在于确保传输的量子状态不被“捕获”。目前，备受瞩目的QKD技术路径分为两类：基于单个光量子的QKD和基于连续变量的QKD。基于单个光量子的QKD技术依托于光量子的离散特性，将秘密信息隐藏在单独光量子的量子状态中进行传输。BB84协议和B92协议便是基于单个光量子的QKD技术的典型代表。而基于连续变量的QKD技术则利用光的连续变量（例如相位或振幅）编码信息，通过检测这些连续变量来恢复信息。该方法利用量子状态的连续性，实现了更快速的信息传输。在基于连续变量的QKD技术中，Gaussian模态的QKD和差分相位调制的QKD成为常见的技术选择。

在深挖基于单个光量子和连续变量的QKD技术后，必须把视野扩大到QKD技术的另一个关键领域——量子中继器与长途传输问题。尽管QKD在理论上拥有无可争议的安全性，但在实际运用中，量子状态在长距离传输过程中遭遇衰减和噪声的双重打击，这限制了QKD系统的传输距离和实用性。为了应对这一挑战，科研工作者提出了量子中继器的概念，它通过在传输路径上布设一系列中继点，应用量子纠缠交换和净化技术，有效延伸了量子状态的传输路程。量子中继器的核心任务是保持量子纠缠在远距离传输中的稳定性，并进行净化。在传输过程中，每个中继点都会接受上一个中继点发出的量子状态，并利用量子纠缠交换技术，将接收到的量子状态与本地生成的量子状态进行纠缠，实现量子状态的长途传输。同时，为了消除量子状态在传输过程中可能遭受噪声的污染，科研工作者还研发了量子状态净化技术，通过多次重复检测和筛选，提升传输量子状态的纯度，保证最终收到的量子状态具有高保真度[6]。除量子中继器外，量子卫星和量子网络的发展也为QKD技术的广泛应用开辟了新天地。量子卫星能够利用太空无障碍传输的有利条件，实现地球表面任意两点间量子状态的传输，极大地拓宽了QKD系统的覆盖范围。量子网络则通过将众多QKD系统互联，构建一个庞大的量子通信网络，实现了量

子状态在多个节点间的高效传输和共享。尽管QKD技术在理论上实现了无条件的安全性，但在实际应用中仍需克服诸多挑战。例如，量子设备的稳定性、量子状态的传输效率以及量子检测结果的准确性等，都是影响QKD系统效能的重要因素。因此，科研工作者需要持续探寻新的量子材料和量子器件，优化量子状态的传输和检测技术，提升QKD系统的实用性和可靠性。同时，随着量子计算技术的迅速发展，QKD技术也必须不断地升级和完善，以应对未来可能出现的量子攻击。例如，科研工作者正在研发基于后量子密码术的QKD协议，确保在量子计算机普及后，QKD系统仍能保持无条件的安全性。此外，量子密钥分配技术与其他量子信息技术的深度融合，如量子随机数生成、量子身份认证等，也将为量子密码通信领域带来新的发展机会和挑战。

3.2 量子认证

量子验证技术作为一种先进的科技手段，其目的在于保障信息交换双方的身份得以精准无误地确认。这项技术的原理在于量子力学的基本法则[7]。相较于那些依赖于密码学或数字签名的传统身份认证方式，尽管这些方法在传统的计算架构下运作良好，但在面对先进的量子计算机时，它们的防御能力显得较为薄弱。相比之下，量子验证利用了量子物理学中一些独特的现象，比如量子态的独一无二且无法复制的特性，以及其不可观测性，为个体识别提供了一种革新的方法。更进一步地说，量子态的这种不可复制性意味着任何尝试去拷贝一个量子状态的行为都会导致该状态发生改变，并且这种改变能够被通信的双方所感知，从而揭露出可能的安全威胁。基于这样的机制，量子验证技术能够提供更为严格的身份验证过程，确保了通信双方的真实性与安全性。此外，通过将量子验证与量子密钥分配技术相结合，可以在生成和确认密钥的过程中加强安全性。在这个过程中，参与者会交换量子状态并测量反馈结果来共同建立一把安全的密钥。鉴于量子状态的本质特性——不可克隆性，任何试图拦截或者篡改密钥的行为都将无所遁形。因此，整合了量子密钥分发技术的量子验证方法能够提供更加可靠的身份核实及密钥传输服务。

3.3 量子随机数生成

在密码学领域，产生随机数是构建安全通信的基石。这种随机数的生成通常依赖于伪随机数生成器，它们通过复杂的计算过程生成看似随机的数字序列。然而，面对量子计算机的攻击，这些伪随机数序列的可预测性提高，从而对加密系统的安全性构成威胁。相反，量子随机数生成器利用量子系统的不可预测性和测量时的不确定性，产生真正的随机序列。在经典系统中缺乏的随机性，是由于量子态的测量和坍缩过程造成的。通过对量子态特征（如位置、动量或自旋）的测量，我们能够获得一系列不可预测的随机数，它们展现出不可预测性和不可操纵性，为密码学提供了更为可靠的随机数生成工具[8]。设计和实施量子随机数生成器需要考虑量子态的制备、测量以及数据的处理等多个方面。为了保持生成的随机数的纯度和安全性，科研人员需要利用精确的量子测量技术和先进的数据处理算法。此外，量子随机数生成器也必须经过严格的测试与验证，以确保在实际使用中的可靠性和稳定性。

4 结束语

量子密码通信凭借其基于量子力学的独特优势，为网络安全提供了革命性的保障。然而，我们也应清醒地认识到，量子密码通信仍面临诸多挑战，如量子设备的稳定性、量子状态的传输效率以及量子检测结果的准确性等。因此，科研人员需要持续投入，不断探索新的量子材料和量子器件，优化量子状态的传输和检测技术，以提升量子密码通信系统的实用性和可靠性。

参考文献：

[1] 康婕.多方量子密码协议的设计与分析[D].西安:西安电子科技大学,2021.
[2] 张盛,王搏稀.基于Matlab的量子密码攻击性能分析[J].电子技术与软件工程,2020(19):238-240.
[3] 孙刚.关于网络安全技术中的量子密码通信分析[J].数字通信世界,2020(09):97-98.
[4] 高鹏,周华旭,于国际,等.量子通信技术与当前应用分析[J].电子设计工程,2020,28(16):115-118,123.
[5] 祝孔妮.半量子通信协议的设计与安全性分析[D].南昌:南昌大学,2020.
[6] 李志娟.量子密码安全服务平台在视频监控联网应用中的建设思路[J].数字技术与应用,2024,42(01):239-242.
[7] 何重阳,刘晓浩,陈刘忠,等.量子密码技术现状及云安全应用展望[J].网络安全技术与应用,2023(09):27-28.
[8] 王爱兵.基于量子密码的网络信息安全动态防护方法[J].信息与电脑:理论版,2023,35(10):212-214.