第 6 卷◆第 12 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

电子信息工程中量子加密技术的应用潜力研究

蒋开心
黑龙江工商学院　102300
DOI：10.12238/ems.v6i12.10864

［摘　要］随着信息技术的迅猛发展，电子信息工程在各个领域扮演着至关重要的角色，然而，随着网络攻击手段的不断升级，传统的加密技术已难以满足信息安全的需求，量子加密技术作为一种前沿的加密手段，凭借其独特的量子特性，为电子信息工程提供了前所未有的安全保障。本文首先概述了量子加密技术的基本原理和特性，然后探讨了其在电子信息工程中应用的意义，并详细分析了量子加密技术在量子密钥分发、量子随机数生成、量子安全通信以及量子加密拓展等方面应用潜力。
［关键词］量子加密技术；电子信息工程；应用潜力；研究

Research on the Potential Application of Quantum Encryption Technology in Electronic Information Engineering

Jiang Kaixin
Heilongjiang University of Commerce　102300

[Abstract] With the rapid development of information technology, electronic information engineering plays a crucial role in various fields. However, with the continuous upgrading of network attack methods, traditional encryption technology is no longer able to meet the needs of information security. Quantum encryption technology, as a cutting-edge encryption method, provides unprecedented security guarantees for electronic information engineering with its unique quantum characteristics. This article first outlines the basic principles and characteristics of quantum encryption technology, then explores its significance in electronic information engineering, and analyzes in detail the potential applications of quantum encryption technology in quantum key distribution, quantum random number generation, quantum secure communication, and quantum encryption expansion.
[Keywords] quantum encryption technology; electronic information engineering; Application potential; Research

引言

在数字化时代，电子信息工程已成为推动社会进步和经济发展的重要力量，然而，随着信息技术的广泛应用，信息安全问题也日益凸显，传统的加密技术，如对称加密和非对称加密，虽然在一定程度上保障了信息的安全性，但面对量子计算机等新型攻击手段，其安全性将受到严重威胁，量子加密技术作为一种新兴的加密手段，凭借其独特的量子特性，为信息安全领域带来了新的曙光。本文将深入探讨量子加密技术在电子信息工程中的应用潜力，以期为未来的信息安全提供新的解决方案。

一、量子加密技术概述

量子加密技术作为一种基于量子力学原理的信息安全解决方案，在保护数据传输过程中展现出了前所未有的安全性，它不仅利用了量子态的不可克隆性和测量扰动性来确保信息的绝对安全，还通过量子密钥分发协议如 BB84 协议等实现了双方在公开信道上安全地共享随机密钥，从而为后续的数据加密提供了坚实的基础。

这种技术的核心在于，当两个通信方通过量子信道交换量子比特时，任何第三方试图窃听或篡改这些量子比特的行为都会不可避免地引起量子状态的变化，进而被合法用户所察觉，使得量子加密技术在理论上达到了无条件的安全性标准，超越了传统加密方法所能提供的安全保障水平[1]。

二、量子加密技术在电子信息工程中应用意义

量子加密技术在电子信息工程中的应用意义深远，它不

仅为解决当前信息安全领域面临的诸多挑战提供了一条全新的路径，而且对于促进信息技术的发展、保障国家信息安全以及推动社会经济的可持续发展具有不可估量的价值，特别是在大数据时代背景下，随着云计算、物联网等新兴技术的迅猛发展，数据安全成为了制约这些技术广泛应用的关键因素之一，而量子加密技术凭借其独特的安全优势，能够有效抵御来自量子计算机的潜在威胁，为构建更加安全可靠的信息传输网络提供了可能，这不仅有助于保护个人隐私和商业秘密，同时也为政府机构和军事部门处理敏感信息提供了强有力的技术支持，进一步增强了国家的信息安全防御能力。

三、量子加密技术在电子信息工程中应用潜力

（一）量子密钥分发：筑牢安全防线，守护信息传输

量子密钥分发(QKD)作为量子加密技术的核心组成部分，通过利用量子态的不可克隆性和测量塌缩特性，为电子信息工程构建了一道坚不可摧的安全防线，其基本原理在于，QKD 允许两方通过量子信道安全地共享随机密钥，而这一过程的安全性是由量子力学的基本定律所保证的，即任何尝试对量子信号进行窃听或复制的行为都会不可避免地改变信号本身的状态，从而被合法的通信双方立即发现，这种特性确保了即使在面对拥有无限计算资源的攻击者时，QKD 也能提供理论上无条件的安全保障[2]。

在电子信息工程中，QKD 的应用潜力巨大，尤其是在需要高度保密的通信场景下，如政府机构之间的敏感信息交流、金融机构的交易数据保护、以及涉及个人隐私的数据传输等方面，QKD 技术可以提供比现有加密手段更为强大的安全保障，其不仅能够有效防止数据泄露，还能确保信息的真实性和完整性，极大地提升了信息传输过程中的安全系数。

目前，量子密钥分发（QKD）技术已经在理论研究和实际应用两方面取得了显著进展。在理论研究上，QKD 技术不仅深化了对量子力学的理解，还形成了包括 BB84 协议、B92 协议在内的多种成熟的密钥分发方案，这些方案为实现安全的量子通信提供了坚实的理论基础；在实际应用方面，QKD 技术已经通过光纤网络实现了城市间的量子密钥分发系统，例如，中国在 2016 年成功建立了世界首条千公里级别的量子保密通信“京沪干线”，并且利用“墨子号”量子科学实验卫星完成了跨越数千公里的星地量子密钥分发实验，这些成就不仅验证了 QKD 技术在长距离通信中的可行性，也为构建全球性的量子通信网络奠定了基础。

随着 QKD 技术的不断发展和完善，其应用前景愈发广阔，未来，QKD 技术有望在多个领域发挥重要作用，比如，在智能电网中，QKD 可以提供高度安全的通信通道，确保电力系统监控信息的安全传输；在车联网领域，QKD 技术能够保护车辆间信息交换的安全，防止黑客攻击，保障交通安全；对于普通消费者而言，QKD 技术的应用将使得个人隐私和数据安全得到前所未有的保护，无论是银行交易还是社交媒体通讯，都将变得更加安全可靠。此外，QKD 技术的发展还将推动相关产业链的升级与转型，催生新的商业模式和服务形态，为社会经济发展注入新的活力。

（二）量子随机数生成：确保随机性真，强化密码安全

量子随机数生成（QRNG）利用量子态的固有随机性，为电子信息工程中的密码系统提供了真正意义上的随机数，与传统的伪随机数生成器相比，QRNG 能够产生无法预测且不可重现的随机序列，这对于提高密码系统的安全性和可靠性至关重要，因为许多加密算法的有效性依赖于高质量的随机数作为密钥或初始化向量，而伪随机数生成器由于存在一定的可预测性和周期性，可能会成为攻击者的突破口[3]。

QRNG 的基本原理是利用量子态的不可预测性和测量结果的不确定性来生成随机数，常见的实现方法包括基于光子到达时间的单光子检测、基于量子隧穿效应的电子噪声检测等，这些方法能够直接从量子物理过程中提取随机性，确保了生成的随机数具有真正的随机性和不可预测性。

在电子信息工程中，QRNG 的应用潜力同样巨大，首先，它能够显著增强各种加密算法的安全性，无论是对称加密还是非对称加密，高质量的随机数都是确保密钥强度和加密效果的基础，通过使用 QRNG 生成的密钥，可以有效避免由于密钥生成过程中的随机性不足而导致的安全漏洞；其次，在身份认证和数字签名等安全协议中，QRNG 提供的随机性可以用于生成一次性口令、随机挑战等，增强协议的防篡改能力和抗重放攻击能力；再者，对于需要大量随机数的应用场景，如随机化算法、蒙特卡洛模拟等，QRNG 能够提供高质量的随机数源，提高算法的准确性和效率；最后，在区块链技术中，QRNG 可以用于生成区块的哈希值、智能合约的随机参数等，增加系统的不确定性和安全性，防止恶意节点的操纵。

目前，QRNG 技术不仅在理论上得到了充分的研究，形成了多种高效的实现方案，而且在实际应用中也展现了良好的性能和稳定性。例如，一些科研机构和企业已经开发出商用化的 QRNG 设备，这些设备不仅能够提供高速率的随机数输出，还具备高集成度和易用性，适用于数据中心、云服务、网络安全等多个领域。此外，随着量子信息技术的快速发展，QRNG 技术正逐渐与其他量子技术相结合，如与量子密钥分发（QKD）系统集成，共同构建更加安全的量子通信网络，或与量子计算平台结合，为量子算法提供必要的随机性支持。展望未来，随着 QRNG 技术的不断成熟和成本的降低，其应用范围将进一步扩大，不仅限于高端安全领域，还将渗透到日常生活的方方面面，为构建一个更加安全可信的信息社会做出重要贡献。

（三）量子安全通信：实现信息畅通，保障通信安全

量子安全通信利用量子态的不可克隆性和测量塌缩等特

性，实现了信息的安全传输，其核心在于发送方利用特定的量子态来编码信息，并通过预先建立的量子信道将这些量子态发送给接收方，接收方通过精确的量子测量技术解码这些量子态，还原出原始信息，由于量子态的不可克隆性，任何试图在传输过程中窃取信息的第三方都会不可避免地改变量子态，进而产生可检测的异常，使得发送方和接收方能够及时发现并采取相应的安全措施，这一过程确保了信息在传输过程中的绝对安全性和完整性[4]。

量子安全通信的应用潜力同样巨大，它不仅能够满足现代社会对信息安全日益增长的需求，还能够在多个关键领域发挥重要作用,从而为社会的稳定和发展提供强有力的支撑。首先，量子安全通信可以用于保护重要信息的传输安全，特别是在军事通信、政府通信、金融交易、医疗数据传输等对安全要求极高的领域，通过采用量子安全通信技术，可以确保这些敏感信息在传输过程中不被非法窃取或篡改，有效防止了信息泄露造成的严重后果，从而保障了国家的安全和利益，促进了社会稳定和谐；其次，量子安全通信还可以用于构建安全的通信网络，传统的通信网络由于存在诸多安全隐患，容易遭受黑客攻击和窃听等威胁，而采用量子安全通信技术的通信网络则能够从根本上抵御这些威胁，实现信息的安全传输，为用户提供更加可靠和值得信赖的通信服务；最后，量子安全通信还可以用于提升网络安全防护能力，通过将量子安全通信与现有的网络安全技术相结合，可以构建起更加安全、可靠的网络安全防护体系，不仅能够有效防范外部攻击，还能增强内部管理，提升网络的整体安全性，为数字经济时代的到来打下坚实的基础。

目前，量子安全通信技术尽管已经取得了一系列重要的研究成果，如量子密钥分发（QKD）、量子随机数生成（QRNG）等，但要实现大规模的商业化应用仍面临不少挑战，包括提高量子通信的距离、降低成本、简化操作流程等。未来随着量子技术的不断进步和成熟，量子安全通信技术有望克服现有障碍，在更多领域得到应用和推广，特别是在智慧城市、物联网、大数据中心等新兴领域，量子安全通信技术将发挥不可替代的作用，成为保障信息安全的重要力量。可以预见的是，随着量子技术的普及和应用，量子安全通信技术有望成为未来信息安全领域的主流技术之一，为构建一个更加安全、高效、智能的信息社会贡献力量。

（四）量子加密拓展：拓展应用领域，守护信息安全

除了上述核心应用外，量子加密技术还在身份认证、数字签名、物联网等领域展现了广泛的应用前景，这些领域的拓展不仅体现了量子加密技术的多功能性和适应性，也进一步丰富了其在保障信息安全方面的实践价值。

在身份认证领域,量子加密技术可以用于实现更加安全、可靠的身份认证机制，传统的身份认证方法由于依赖于静态密码或者生物特征识别，容易受到伪造和攻击等威胁，而采用量子加密技术的身份认证机制则能够有效抵御这些威胁，确保身份认证的真实性和安全性，例如，可以利用量子密钥分发（QKD）技术来生成和分发身份认证所需的密钥，这种方式不仅能够确保密钥的绝对安全，还能实时监测是否有第三方尝试窃听或篡改密钥，一旦发现异常，系统将自动终止认证过程，从而大大提高了身份认证的安全性[5]。

在数字签名领域,量子加密技术可以用于实现更加安全、可靠的数字签名机制，传统的数字签名方法虽然能够验证文件的完整性和来源，但由于依赖于数学难题的复杂性，仍然存在被破解的风险，而采用量子加密技术的数字签名机制则能够从根本上解决这个问题，确保数字签名的真实性和安全性，例如，可以利用量子随机数生成（QRNG）技术来生成数字签名所需的随机数,由于 QRNG 产生的随机数具有真正的随机性和不可预测性,这使得基于 QRNG 的数字签名几乎不可能被伪造，即使是最先进的量子计算机也难以破解，从而为数字文档、软件分发等场景提供了更为强大的安全保证。

在物联网领域，量子加密技术则可以用于保护物联网设备之间的通信安全，物联网设备数量庞大、种类繁多，且往往部署在开放的环境中，这使得它们成为黑客攻击和窃听的主要目标，通过采用量子加密技术，可以确保物联网设备之间的通信安全，防止信息被窃取或篡改，例如，可以利用量子安全通信技术来保护物联网设备之间的通信链路，不仅能够实现端到端的加密通信，还能通过量子密钥定期更新的方式，确保即使某个设备被攻破，也不会影响整个网络的安全性。

四、结论

综上所述，量子加密技术在电子信息工程中的应用潜力巨大，通过充分利用量子加密技术的独特优势，不仅可以推动电子信息工程的创新发展，还能显著提升信息安全防护能力，为未来的信息安全领域提供新的思路和方法。随着量子技术的不断进步和成熟，相信量子加密技术将在多个方面发挥更为重要的作用，成为保障信息社会安全的重要支柱。

[参考文献]

[1]杨圣亚.大数据背景下的电子信息加密集中管控技术分析[J].微型计算机，2024（6）：49-51.

[2]石润华，邓佳鹏，于辉，柯唯阳.基于量子行走公钥加密的电子投票方案[J].信息网络安全，2024（5）：732-744.

[3]曾建光，谯连，古沛，黄海.加快量子信息安全托管中心建设,推动能源革命向纵深发展[J].中国发展,2024(4)：42-47.

[4]黄钊龙，韩召颖.量子信息技术发展与国家安全[J].武汉大学学报（哲学社会科学版），2024，77（2）：51-60.

[5]彭飞，田增垚，张晓华，安天瑜，孟庆东，陈志奎.基于量子安全的电力信息系统安全增强方法研究[J].重庆大学学报，2024，47（2）：62-74.