ID 104

Quantum Cryptography: Enhanced Security for Better Communication

KBMH Kariyawasam[1#] and DVDS Abeysinghe[1]

[1]Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

[#]38-bce-0020@kdu.ac.lk

Abstract

This review extensively explores and compares classical cryptographic methods with a specialized emphasis on Quantum Key Distribution (QKD) techniques in quantum cryptography. It thoroughly examines their security foundations, key distribution mechanisms, vulnerabilities, and implications in modern computing. While revealing vulnerabilities within classical methods, notably in key distribution and susceptibility to evolving quantum threats, this review places a significant focus on the intricate nuances and diverse techniques within Quantum Key Distribution. It highlights QKD's theoretical invulnerability, its diverse methods for secure key exchange, and its resistance against quantum attacks, underscoring its pivotal role in quantum cryptographic frameworks. This assessment points up classical cryptography's vulnerabilities amidst advancing computing power and interception during key exchange. Conversely, it underscores the resilience of Quantum Key Distribution against quantum-based threats, presenting diverse methods for intrusion detection. By delving deeply into Quantum Key Distribution techniques, this review underlines their potential to revolutionize secure communication paradigms. Rooted in quantum principles, these techniques pave the way for enhanced security, delineating a transformative path in securing future communications.

Keywords: *Cyber security, Networking, Quantum computing, Quantum key distribution, Secure communication, Secure networks*