IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, April 2024

Quantum Cryptography: Advancements, Challenges, and Applications in Modern Communication

Vimmi Malhotra[1], Sahil Yadav[2], Vishal[3]
Assistant Professor, Department of Computer Science Engineering[1]
UG Students, Department of Computer Science Engineering[2,3]
Dronacharya College of Engineering, Gurgaon, India

Abstract: *This research paper explores the fascinating field of Quantum Cryptography, a cutting-edge technology that leverages principles of quantum mechanics to secure information transfer. The objective of this study is to delve into the underlying principles of Quantum Cryptography, specifically Quantum Key Distribution (QKD), and discuss its potential applications and challenges. The methodology involves a comprehensive review of existing literature and recent advancements in the field. The key findings reveal that Quantum Cryptography presents a promising solution for secure communication, offering robust defence against potential eavesdroppers. However, practical implementation faces several challenges, including technological limitations and the need for standardization. The implications of this study underscore the transformative potential of Quantum Cryptography in shaping the future of secure communication and highlight the need for further research and development in overcoming existing challenges.*

Keywords: Quantum Cryptography

REFERENCES

[1]. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.
[2]. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.
[3]. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661-663.
[4]. Scarani, V., Acín, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters, 92(5), 057901.
[5]. NIST Post-Quantum Cryptography Standardization Project. (2020). Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization
[6]. Mosca, M., & Stebila, D. (2019). PQCRYPTO: The NIST Post-Quantum Cryptography Standardization Process. PQCrypto 2019: 10th International Conference on Post-Quantum Cryptography, 57-67.
[7]. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography (1st ed.). Springer.
[8]. van de Graaf, J., & Bos, J. W. (2020). Quantum-Resistant Cryptography. Springer.
[9]. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 212-219.
[10]. National Academies of Sciences, Engineering, and Medicine. (2019). Quantum Computing: Progress and Prospects. The National Academies Press.