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, February 2024

Quantum Cryptography: Future-proofing Digital Security

Ms. Aparna Panigrahy
Assistant Professor, Department of Information Technology
Nirmala Memorial Foundation College of Commerce and Science

The field of cryptography underpins the security of our digital world, ensuring the confidentiality, integrity, and authenticity of sensitive information. However, the landscape is shifting with the rise of quantum computers. These machines harness the principles of quantum mechanics to perform computations infeasible for classical computers. One of the most concerning implications is their ability to break widely used public-key encryption algorithms, such as RSA and Elliptic Curve Cryptography (ECC). These algorithms rely on the mathematical difficulty of factoring large numbers or solving discrete logarithm problems. While computationally expensive for classical computers, Shor's algorithm, a quantum algorithm, can solve these problems efficiently, rendering current encryption methods vulnerable.