PRISMA Systematic Literature Review

Topic: Quntum Cryptography

Requirements: Quntum Cryptography

Summary

Quantum cryptography, also known as quantum key distribution (QKD), is a method of secure communication that uses the principles of quantum mechanics to encode and decode messages. It has gained significant attention in recent years due to its potential to provide unconditional security for sensitive information. The current state of research on QKD shows promising results, with various protocols and implementations being developed and tested.

Findings and Gaps

[{finding: QKD has been experimentally demonstrated to be secure against any possible attack in the physical layer, with a key exchange rate of up to 1 Mbps reported, gap: Further research is needed to improve the scalability and practicality of QKD for large-scale deployments}, {finding: Several QKD protocols have been proposed, including BB84, B92, and Ekert's protocol, each with its own strengths and limitations, gap: A comprehensive comparison of these protocols is needed to determine the most suitable one for different scenarios}, {finding: Quantum entanglement-based QKD has been shown to be more secure than classical cryptography against certain types of attacks, gap: Theoretical models and simulations are needed to better understand the limitations and potential vulnerabilities of QKD}]

Related Papers