

PRISMA Systematic Literature Review

Topic: Quntum Cryptography

Requirements: Quntum Cryptography

Summary

Quantum cryptography is a method of secure communication that uses quantum mechanics to encode and decode messages. It relies on the principles of quantum entanglement and superposition to create an unbreakable code. The current state of research in this field has shown significant advancements, with several protocols and systems being developed for practical applications.

Findings and Gaps

The review found that quantum cryptography has made significant progress in recent years, with the development of various protocols and systems. Key findings include: (1) Quantum key distribution (QKD) is a widely used protocol for secure key exchange; (2) The BB84 protocol is a popular choice for QKD due to its simplicity and high efficiency; (3) The implementation of quantum cryptography in real-world scenarios has shown promising results, with several organizations and companies actively developing and testing the technology. However, research gaps remain, including: (1) The need for further development of practical and scalable systems; (2) The requirement for more efficient key distribution protocols; and (3) The necessity for increased understanding of quantum errors and their impact on cryptographic applications.

Related Papers

- Quantum cryptography based on entangled photons
- -9224.1
- 1999