Quantum Computing Algorithms for Cryptographic Challenges

Περιγραφή Θέματος

This thesis delves into the implications of quantum computing on modern cryptographic systems. It reviews quantum algorithms like Shor's algorithm for factoring integers and Grover's algorithm for search, analyzing their potential to break widely used encryption protocols. Additionally, it explores quantum-resistant algorithms that ensure security in a post-quantum world. The study emphasizes the urgency of transitioning to quantum-safe encryption standards for critical applications.

Καθηγητής: Andreas Komninos

Ετος:2024