Quantum Computing and its Potential Applications in Cryptography

December 15, 2024

Abstract

Quantum computing promises to revolutionize the field of cryptography by introducing new algorithms capable of solving problems that are intractable for classical computers. This paper explores the theoretical foundations of quantum computing and its implications for current cryptographic systems. We review quantum algorithms such as Shor's algorithm and Grover's algorithm, discussing their potential to break widely-used encryption methods like RSA and AES. The paper also examines ongoing research in post-quantum cryptography, which aims to develop encryption schemes resilient to quantum attacks.

References