Advantage of Quantum Computing in Breaking RSA Encryption

Your Name

March 20, 2025

Abstract

Quantum computing has emerged as a revolutionary paradigm in computational science, offering significant advantages over classical computing in solving certain types of problems. One of the most notable implications of quantum computing is its potential to break widely used cryptographic systems, such as RSA encryption. This report explores the principles of RSA encryption, the role of Shor's algorithm in quantum computing, and the implications of quantum advancements on cryptographic security.

1 Introduction

RSA encryption is one of the most widely used public-key cryptographic systems, relying on the computational difficulty of factoring large integers. The security of RSA is based on the assumption that classical computers cannot efficiently factorize large numbers. However, the advent of quantum computing challenges this assumption, posing a significant threat to the security of RSA and similar cryptographic systems.

2 Overview of RSA Encryption

RSA encryption is based on the mathematical properties of prime numbers and modular arithmetic. The key generation process involves:

- Selecting two large prime numbers, p and q.
- Computing $n = p \cdot q$, where n is the modulus.
- Calculating the totient $\phi(n) = (p-1)(q-1)$.
- Choosing a public exponent e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
- Determining the private key d such that $e \cdot d \equiv 1 \pmod{\phi(n)}$.

The encryption and decryption processes rely on modular exponentiation, which is computationally efficient for large numbers.

3 Quantum Computing and Shor's Algorithm

Quantum computing leverages the principles of quantum mechanics, such as superposition and entanglement, to perform computations. Shor's algorithm, developed by Peter Shor in 1994, is a quantum algorithm that can efficiently factorize large integers. The algorithm operates in polynomial time, making it exponentially faster than the best-known classical algorithms for integer factorization.

The key steps of Shor's algorithm include:

1. Quantum phase estimation to find the period of a function related to the integer to be factorized.

2. Classical post-processing to determine the factors of the integer.

This capability directly undermines the security of RSA encryption, as the private key can be derived from the public key by factorizing n.

4 Implications for Cryptographic Security

The ability of quantum computers to break RSA encryption has profound implications for cybersecurity. Sensitive data encrypted using RSA could be decrypted by adversaries with access to sufficiently powerful quantum computers. This has led to the development of post-quantum cryptography, which aims to create cryptographic systems resistant to quantum attacks.

5 Conclusion

Quantum computing represents a paradigm shift in computational capabilities, with significant implications for cryptography. Shor's algorithm demonstrates the potential of quantum computers to break RSA encryption, highlighting the need for robust post-quantum cryptographic solutions. As quantum technology continues to advance, it is imperative to transition to cryptographic systems that can withstand quantum attacks.

References

1. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*.

2. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*.

3. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`.