Quantum Computing and the Threat to Security Technology

Mitsuhiro Kitajima
Paris Lodron University of Salzburg

Martin Schider
Paris Lodron University of Salzburg

February 10, 2025

Abstract

Quantum computing represents a paradigm shift of computational technology and Information technology, leveraging the principles of quantum mechanics to solve problems that are currently not easy to solve for classical computers. This paper explores the fundamentals of quantum computing, its potential applications, and the significant threats it poses to current cryptographic systems with concrete examples like RSA encryption system.

1. What is Quantum Computing?

1.1. Overview of Quantum Computers

Quantum computing (or quantum computers) is a new model of computation that utilizes techniques and theories from quantum mechanics. One of the most significant differences is the efficiency of computation. Due to the unique characteristics of quantum computation, certain algorithms or problems that are intractable for classical computers can be solved efficiently with quantum computing.

There are many potential applications of quantum computing. One example is cryptanalysis, which relies heavily on mathematical theory and the complexity of algorithms. Another application is in machine learning, where training and optimizing large datasets require massive amounts of computation.

1.2. Difference Between Classical Computers and Quantum Computers

One of the most significant differences between classical and quantum computers is the concept of the qubit. While classical computers use binary bits (0 or 1), qubits can exist in a superposition of states. A qubit is the fundamental unit of quantum information and can be represented as:

$$a|0\rangle + b|1\rangle$$

where a and b are the probability amplitudes of the qubit being in the 0 or 1 state, respectively. These amplitudes must satisfy:

$$|a|^2 + |b|^2 = 1.$$

Another key characteristic of quantum computers is the use of quantum circuits. Quantum circuits manipulate qubits through quantum logic gates, which are analogs of classical logic gates. Unlike classical logic gates, which use Boolean algebra, quantum logic gates operate using linear algebra due to the superposition and entanglement of qubit states.

The input to a quantum circuit is generally a set of qubits initialized to the 0 state. Quantum gates, such as the Hadamard gate (H), can put qubits into superposition, and measurement collapses the qubit state to either 0 or 1.

1.3. Quantum Algorithms

Quantum algorithms are a new type of algorithm based on the principles of quantum computation. Due to the unique computational abilities of quantum computers, some quantum algorithms have polynomial time complexity, allowing them to solve problems that classical computers cannot solve efficiently.

One example is Shor's algorithm, developed by Peter Shor in 1994. Shor's algorithm is a quantum algorithm for integer factorization. It can factorize large numbers efficiently using quantum computation, posing a significant threat to cryptographic systems like RSA, which rely on the difficulty of factoring large composite numbers for security.

Another example is Grover's algorithm, developed by Lov Grover in 1996. Grover's algorithm is a quantum search algorithm that can search unsorted databases faster than classical algorithms. While classical algorithms require linear time complexity for searching unsorted data, Grover's algorithm achieves a time complexity of $\mathcal{O}(\sqrt{n})$, which is quadratically faster.

This algorithm can accelerate cyberattacks based on exhaustive search methods. For example, a brute-force attack on AES-128 encryption would require 2^{126} operations classically, but only 2^{63} operations using Grover's algorithm.

2. Threats to Security Technology

2.1. Overview of Cryptography

Cryptography is the practice of securing information or establishing secure communications through encryption. Its origins date back to ancient Egypt, around 3000 years ago. Today, cryptography is widely used in many technologies and systems, such as passwords, electronic signatures, and authentication.

2.2. Symmetric and Asymmetric Encryption

There are many types of encryption technics, but generally, they can be categorized into two groups, which is, symmetric and asymmetric Encryption.

Symmetric encryption uses shared key for both encryption and decryption. The security relies on the secrecy of the key and the strength of the encryption algolithm.

Asymmetric encryption, such as RSA-cryptosystem, uses different keys for encryption and decryption. The key for encryption is public, and the receiver uses a private key to decrypt the text.

2.3. Threats from Quantum Computing

Quantum computer and its technology pose a significant threat to current cryptographic systems.

One of the example is RSA encryption algorithm. Nowadays, RSA encryption system considered as secure encryption system, because decryption of the encrypted text without secret key takes exponential time.
But quantum algorithms for factoring such as Shor's algorithm can brake RSA encryption efficiently, because it can factorize large natural numbers.

2.4. Mitigation Measures

Today, the study of the cryptography in quantum computer era is ongoing.

Post-quantum cryptography involves developing new cryptographic algorithms that are resistant to attacks by quantum computers. Examples include lattice-based cryptography, multivariate cryptography, hash-based cryptography, code-based cryptography, and isogeny-based cryptography.

Cryptography with the theory of quantum computing is also a great interest of current cryptography. Quantum cryptography uses the principles of quantum mechanics to secure communication. For example, quantum key distribution (QKD) allows two parties to generate a shared secret key with security guaranteed by the laws of quantum physics. Another example is Quantum random number generation, which provides truly random numbers, unlike pseudo random numbers from classical computation theory.

3. Conclusions

Quantum computing holds immense potential for the new era of computing theory but also poses significant risks to current cryptographic systems. As quantum computing technology advances, it is essential for the cybersecurity community to find potential threats and ensure the security of digital communications.

References

[1] J. D. Hidary. *Quantum Computing: An Applied Approach*. Springer, 2021.

[2] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *IEEE Computer Society Press*, 10:20–22, November 1994.