Chapter 7
Quantum Cryptography:
Algorithms and Applications

R. Thenmozhi
SRM Institute of Science and Technology, India

D. Vetriselvi
https://orcid.org/0009-0001-3870-9061
SRM Institute of Science and Technology, India

A. Arokiaraj Jovith
SRM Institute of Science and Technology, India

ABSTRACT

Cryptography is the process of encrypting data or transforming plain text to ciphertext so that it can be deciphered only by appropriate key. Quantum cryptography employs quantum physics principles to encrypt and transport data in an unpackable manner. Quantum key distribution (QKD) is a technique for creating and exchanging private keys over quantum channels between two parties. Then, using standard cryptography, the keys can be used to encrypt and decrypt messages. Unbreakable encryption is something we really must have. The integrity of encrypted data is now in danger due to the impending development of quantum computers. Fortunately, quantum cryptography, via QKD, provides the answer we require to protect our information for a very long time to come. This is all based on the intricate principles of quantum mechanics. This chapter is discussing the various algorithms used and the applications of quantum cryptography.

INTRODUCTION

Quantum Computing

Quantum computing is a multidisciplinary field that integrates computer science, mathematics, and physics. We can solve complex problems far faster with quantum physics than we can with conventional

DOI: 10.4018/979-8-3693-1642-9.ch007

computers. Quantum computing includes both hardware and software development and research. Two examples of quantum mechanical characteristics that quantum computers employ to surpass classical computers in particular problem types are superposition and quantum interference. This is so that quantum computers may make use of these phenomena. Machine learning (ML), optimisation, and simulation of physical systems could all profit from the faster processing rates provided by quantum computers. Potential applications in the future include enhancing financial portfolios and modelling chemical reactions, two tasks that require resolving issues that are beyond the capabilities of even the most potent supercomputers available today.

Quantum bits, or qubits, are represented by symbols called quantum particles. The control devices play a major role in the success of the attempt to maximise the processing capabilities of a quantum computer by manipulating qubits. The bits found in traditional computer types are comparable to the qubits seen in quantum computers. A traditional machine's CPU is primarily in charge of manipulating bits to accomplish its tasks. Parallel to this, the manipulation of qubits is the only way the quantum processor can perform its duties (Raymer, 2017).

An electronic signal that can exist in one of two states—on or off—is referred to as a "bit" in the context of classical computing. Depending on the circumstance, the classical bit's value can be either one (on) or zero (off). Owing to its foundation in the concepts of quantum physics, the qubit can exist in a superposition of states.

BACKGROUND

Quantum Mechanics

In the study of very small-scale particle behaviour, physics offers a field known as quantum mechanics. The equations governing particle behaviour at the subatomic scale are not the same as those describing the macroscopic environment. The utilisation of these phenomena by quantum computers results in computational processes that are radically novel (Sasaki, 2012).

Basic Concepts Behind Quantum Computing

The application of quantum ideas forms the foundation of quantum computing. A new lexicon of terms is required to fully comprehend quantum principles. These include concepts like decoherence, entanglement, and superposition. Let us get a deeper comprehension of these principles (Banafa, 2023).

- **Superposition**
  Superposition is the idea that two or more quantum states can be combined in a way that is like how waves are combined in conventional physics, and the outcome will be another valid quantum state. Conversely, any given quantum state can also be defined as the sum of two or more other unique states. The inherent parallelism of quantum computers, which allows them to perform millions of tasks simultaneously, comes from this superposition of qubits.

Related Content