Chapter 16
Optimal Parameter Prediction for Secure Quantum Key Distribution Using Quantum Machine Learning Models

Sathish Babu B.
RV College of Engineering, Bangalore, India

K. Bhargavi
Siddaganga Institute of Technology, India

K. N. Subramanya
RV College of Engineering, Bangalore, India

ABSTRACT

The advent of quantum computing is bringing threats to successful operations of classical cryptographic techniques. To conduct quantum key distribution (QKD) in a finite time interval, there is a need to estimate photon states and analyze the fluctuations statistically. The use of brute force and local search methods for parameter optimization are computationally intensive and becomes an infeasible solution even for smaller connections. Therefore, the use of quantum machine learning models with self-learning ability is useful in predicting the optimal parameters for quantum key distribution. This chapter discusses some of the quantum machine learning models with their architecture, advantages, and disadvantages. The performance of quantum convoluted neural network (QCNN) and Quantum Particle Swarm Optimization (QPSO) towards QKD is found to be good compared to all the other quantum machine learning models discussed.

DOI: 10.4018/978-1-7998-8593-1.ch016

INTRODUCTION

Today's e-manufacturing, digital world provides a variety of services for the benefit of mankind, which includes e-Health, e-Bank, e-Hotel, e-Government and e-Commerce. For successful operation of these services several factors, like privacy, security, confidentiality, cost, trust, compatibility, and standardization. need to be taken into account. Among all the factors security is given paramount importance as the data being exchanged need to be protected from third party attacks. Traditional cryptography is one of the methods that allow us to store and send the data via encryption and reverse decryption process and established secure communication between two parties by protecting the data from attackers using public and private key distribution strategies (Van & Thijssen, 2015).

Some of the consequences of traditional cryptography are listed below.

- The message which is strongly authenticated using cryptographic mechanism sometimes makes it difficult to take legitimate decisions at crucial time.
- The speed of execution slows down due to complex mathematical operations.
- Providing selective access to the data is difficult suing crypto system.
- The design of the crypto system is poor in terms of architecture, protocol, and procedures used for encoding and decoding.
- Cost of setup and operation of public key cryptosystem is high as it demands separate public key infrastructure.

QUANTUM COMPUTING: AN OVERVIEW

Quantum computing is a revolutionary technology which leverages the characteristics of quantum mechanics such as superposition and entanglement to perform computation extremely faster than classical computing technologies (Feynman, 1982).

Figure 1. Quantum computing process