Chapter 3
Quantum Key Distribution Protocols

Shyam Sihare
https://orcid.org/0000-0003-2096-8273
Dr. A.P.J. Abdul Kalam Government College, India

ABSTRACT

The author will discuss different quantum protocols in this chapter for guided media and open space communication. The author examines already developed quantum protocols for photons and electrons. Earlier developed quantum protocols are the basis of recently developed quantum protocols. The author makes a study on quantum protocols with the help of quantum mechanics features such as entanglement, superposition, uncertainty principle, and no cloning.

1. INTRODUCTION

Quantum protocols act as a guide to transfer a message from one party to more than one parties. Quantum protocols are completely different than classical protocols as functionally and operationally. There are different types of quantum protocols (Colbeck R.; 2009). Among different types of protocols, the BB84 protocol plays a significant role and guide the development of the subsequent protocol e.g. decoy, SARG04, E91, KMB09 (Malathy et al.; 2022).

Photons or electrons can practice for message encryption and apply on them different orientation. Furthermore, the encrypted message has been transferred from Alice to Bob in the presence of Eve (intruder) (Williams C P & Williams C P; 2011). The quantum protocols give the guarantee of absolute security due to quantum mechanics features (Van De Graaf J; 1997). Particle orientation has been performed by the PBS, Filter, Polarizer, Merger, and Amplifier (Tsekeri et al.; 2021).

DOI: 10.4018/978-1-7998-9522-0.ch003

Oriented particles send through guided media, or open space, or both medias. Before sending oriented particles, Bob and Eve share her key either private or public way (Chun W H K; 2008).

A classical network protocol contains a set of rules enabling the exchange messages from one computer to another (Bonaventure; 2011). A well-known classical protocol is the TCP-IP protocol. Other classical protocols include FTP, SMTP, Telnet, POP, IMAP, Bitcoin, and VoIP. Currently, few protocols are used (Yildirim; 2010).

Different quantum protocols exist for quantum communication and quantum information. The operation of quantum protocols is entirely different from classical network protocols (Cacciapuoti et al.; 2019). The quantum protocol operation depends on quantum mechanics features, whereas the classical network protocol operation depends on classical physics features (Perseguers et al.; 2010).

Quantum protocols are used for exchanging quantum keys between Alice and Bob in the presence of Eve by using a public channel (Parakh A; 2013). The protocols are used to establish a link between Alice and Bob (Mödersheim S; 2009, March). This method is known as private key cryptosystem because the communication is conducted privately with high security. After a connection is established, message exchange is performed through a public channel without worrying about the presence of an unauthorised person. For communication, a control channel is required throughout the communication process (Dzung et al.; 2005).

The possibility of errors during quantum communication is more than the possibility during classical communication (Buhrman H, Cleve R, & Wigderson A; 1998, May). During classical communication, errors are detected and corrected by classical algorithms such as CRC, Hash function $H(x)$, Hamming code, and parity bits (Babar et al.; 2018). These algorithms are applied for error detection and correction while using IPv4, IPv6, user datagram protocol (UDP), and TCP-IP and during deep-space communications, satellite broadcasting, and data storage. The sender and receiver are not involved in the error correction and detection (De Cola et al.; 2011). A sender sends messages over a classical channel without the knowledge of a receiver's operational pattern. Approximately, 10% reverse communication occurs between a sender and receiver for error correction. During the communication between Alice and Bob, error correction and detection algorithms are used to detect bit-, stream-, message-, and block-level errors (Chiueh T D & Tsai P Y; 2008).

Quantum errors are detected and corrected with the assistance of Alice, Bob, or both by sharing of private key. Without mutual understanding, quantum errors cannot be controlled (El Ashmawy M S; 2021). Alice sends qubits and Bob receives the qubits without the knowledge of Eve presence. Every qubit measurement is conducted at the receiver end. After the qubits are transferred, the polarised qubits are checked by Bob with the help of Alice (Valivarthi V R R; 2017). If the error in the checked qubits is below a threshold value, then the qubits are accepted otherwise

A Generalized Parallel Quantum Inspired Evolutionary Algorithm Framework for Hard Subset Selection Problems: A GPQIEA for Subset Selection

Sulabh Bansaland C. Patvardhan (2021). *Research Anthology on Advancements in Quantum Technology (pp. 51-92).*

www.irma-international.org/chapter/a-generalized-parallel-quantum-inspired-evolutionary-algorithm-framework-for-hard-subset-selection-problems/277769