Chapter 44
A Proposed Architecture for Key Management Schema in Centralized Quantum Network

Ahmed Farouk
Zewail City of Science and Technology, Egypt & Mansoura University, Egypt

Josep Batle
Universitat de les Illes Balears, Spain

Mohamed Elhoseny
Mansoura University, Egypt & Scientific Research Group in Egypt (SRGE), Egypt

Mosayeb Naseri
Islamic Azad University, Kermanshah, Iran

Aboul Ella Hassanien
Cairo University, Egypt & Scientific Research Group in Egypt (SRGE), Egypt

ABSTRACT

Most existing realizations of quantum key distribution (QKD) are point-to-point systems with one source transferring to only one destination. Growth of these single-receiver systems has now achieved a reasonably sophisticated point. However, many communication systems operate in a point-to-multi-point (Multicast) configuration rather than in point-to-point mode, so it is crucial to demonstrate compatibility with this type of network in order to maximize the application range for QKD. Therefore, this chapter proposed architecture for implementing a multicast quantum key distribution Schema. The proposed architecture is designed as a Multicast Centralized Key Management Scheme Using Quantum Key Distribution and Classical Symmetric Encryption. In this architecture, a secured key generation and distribution solution has been proposed for a single host sending to two or more (N) receivers using centralized Quantum Multicast Key Distribution Centre and classical symmetric encryption.

DOI: 10.4018/978-1-5225-2229-4.ch044

INTRODUCTION

The quantum computers are dissimilar from classical computers depending on transistors. While a classical computer involves data to be converted into bits (0 or 1), the quantum computer involves quantum bits (qubits) can be in superposition state. The superposition state means that the quantum state can be 0, 1 or in both states at the same time. Quantum computers share hypothetical relationships with non-deterministic and probabilistic computers (Nielsen& Chuang, 2000). By way of 2015, the improvement and growth of a real quantum computer is still in early stages but many poetical and theoretical experimentations were implemented by many research groups (Metwaly et al., 2014).

Quantum bit can take the properties of 0 and 1 simultaneously at any one moment (Barenco et al., 1995). A quantum bit, or qubit for short, is a 2wir dimensional Hilbert space H_2. An orthonormal basis of H_2 is specified by { $\left|0\right\rangle, \left|1\right\rangle$ }. The state of the qubit is an associated unit length vector in H_2. If a state is equal to a basis vector then we say it is a pure state. If a state is any other linear combination of the basis vectors, we say it is a mixed state, or that the state is a superposition of $\left|0\right\rangle$ and $\left|1\right\rangle$ (Barenco et al., 1995).

The quantum bit can be measured in the traditional basis where it is equal to the probability of effect for α^2 in $\left|0\right\rangle$ direction and the probability of effect for β^2 in $\left|1\right\rangle$ direction where α and β must be constrained by Eq. (1) and Figure 1 (Zeng, 2006; Zeng, 2010).

$$\alpha^2 + \beta^2 = 1 \tag{1}$$

Quantum computers can manipulate quantum information where the quantum state can be transformed from a pure or mixed state to another pure or mixed state correspondingly. The transformation can be achieved by applying a unitary linear operation $\breve{U}$, where $\breve{U}\breve{U}^{\dagger} = \breve{U}^{\dagger}\breve{U} = I$ if the quantum state is a single qubit. If we have a pure quantum state $\left|\psi\right\rangle$ can be transformed into another pure state $\breve{U}\left|\psi\right\rangle$, as well if we have a mixed quantum state ρ can be transformed into another mixed state $\breve{U}\rho\breve{U}^{\dagger}$ (Sharbaf, 2009; Stinson, 1995). The unitary transformation operations are defined by (Eq. (2)). X, Y, Z can be

Figure 1. Classical and quantum bits