Chapter 16
A Quantum Key Distribution Technique Using Quantum Cryptography

Meenakshi Sharma
Galgotias University, India

Sonia Thind
Chandigarh University, India

ABSTRACT

In order to protect and secure the sensitive data over the internet, the current data security methods typically depend on the cryptographic systems. Recent achievements in quantum computing is a major challenge to such cryptography systems. In this way, the quantum key distribution (QKD) technique evolves as a very important technique which gives un-conditional data security. This technique is based on the laws of quantum physics for its security. This article gives a detailed description of the QKD technique. This technique secures the encryption key delivery between the two authenticated parties from the unauthorized access. In the next phase, quantum cryptography model is discussed. Finally, some important application areas and limitations of this technology are be discussed.

1. INTRODUCTION

Quantum cryptography is an approach that allows two parties to share encryption keys securely, even in the presence of an intruder (Payal et al., 2014). This technique is based on the laws of quantum physics for its security and detects the eavesdropping between the two communicated parties. This can be done by comparing the bits of a data subset shared between the two communicated parties.

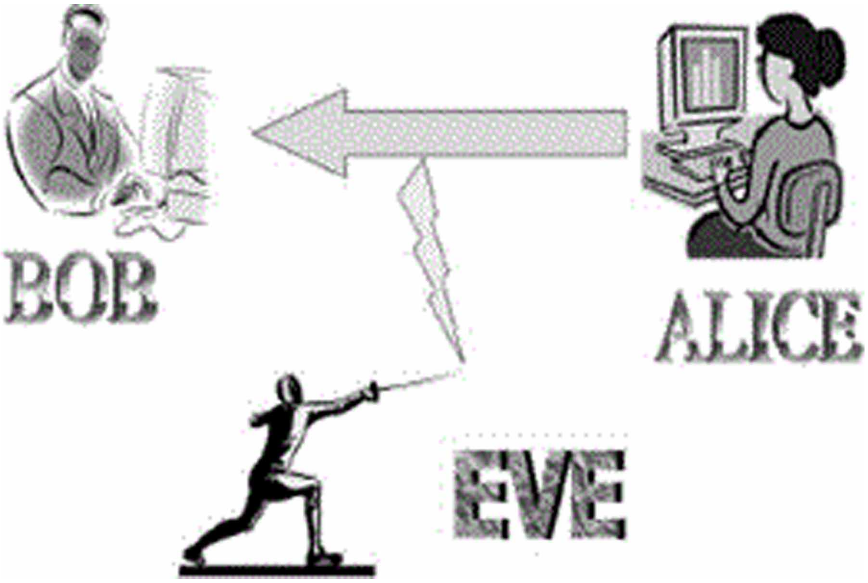
In the early 1970s, QC was introduced first by the Stephen Wiesner, when he gives the principle of quantum conjugate-coding. His research paper "Conjugate Coding", was initially rejected by the IEEE Information theory but in 1983 was eventually published in SIGACT News. Based upon this work Gilles Brassard and Bennett introduced a secure communication way based on the Wiesner's "conjugate-

DOI: 10.4018/978-1-7998-5351-0.ch016

coding". Brassard and Bennett stated that encryption keys could be developed based on the photons of light reaching a receiver and how these photons were received. The photons of light can be polarized in various directions and orientations based on the protocols developed (Pooja et al., 2016). These photon's orientations are used to show composition of bits, i.e. composition of 1s and 0s. The bits representation of polarized photons is the base of QC that gives the law of quantum key distribution (QKD).

Typically, QC depends up on the principles of quantum physics, i.e. photon polarization and Heisenberg's Uncertainty Principle (Bennett, 1999). According to the principle of Heisenberg Uncertainty, the quantum state of any system cannot be measured, without disturbing that system. Therefore, photon polarization or particles of light can only be known at the time when it is measured. In this way, activities of eavesdropper that produces an unwanted change on the state of quantum system can be ensured before the encrypted data can be transmitted to the receiver. QC basically depends on the no cloning theory of quantum mechanics. The no-cloning theory depends on the principle that no single photon can be received, and no single photon can be duplicated without informing to others (Padmavathi et al., 2016). The principle of photon polarization shows how photons of light can be polarized or oriented in a particular direction. Figure 1 shows the network communication process.

Figure 1. Network communication process



In this way, QKD technique evolves as a very important technique which gives un-conditional data security. This technique is based on the laws of quantum physics for its security. In the first phase, this paper gives detailed description of the Quantum Key Distribution technique. This technique secures the encryption key delivery between the two authenticated parties from the unauthorized access. In the next phase, quantum cryptography model can be discussed. At last, some important application areas and limitations of this technology can be discussed.