Chapter 1
Quantum Cryptography:
Basic Principles and Methodology

Satish Rupraoji Billewar
Vivekanand Institute of Management Studies and Research, Mumbai University, India

Gaurav Vishnu Londhe
NMIMS Mumbai, India

Sunil Bahiru Ghane
Sardar Patel Institute of Technology, Mumbai, India

ABSTRACT

History repeats itself. Quantum cryptography has started a revolution of quantum computing and has repeated the days of Einstein's research paper on "Theory of Relativity," which changed the world's perceptions of physics completely written based on Newton's laws. Quantum cryptography is going to change the definition of computers right from scratch. The last century was witness of a space race between US and USSR. This century would be witness of quantum computing race between US and China. It has changed the dimensions of operating systems, software, hardware, databases, and applications. Quantum computers are in a phase to replace the conventional computers and they are reaching to the level called quantum supremacy. The chapter covers the details of the basic principles and work methodology of quantum cryptography, the contribution of various pioneers, advantages over classical cryptography, its applications, future scope, and limitations simultaneously. The chapter covers the contribution of leading countries and organizations in quantum revolution.

INTRODUCTION

Cryptography is the process to convert original text, conceal it in a disorganized way, and provide a protection password or a key by which the person having rights can only open it. Cryptography is the emergence of the implementation of ancient techniques to shroud the information. Quantum Cryptography brings scientific encryption to higher altitudes with the use of quantum physics principles like

DOI: 10.4018/978-1-7998-6677-0.ch001

quantum mechanisms which encode and transmit the information securely in such a way that intruders cannot hack it. Quantum mechanism prepares the set of rules for secure transmission between sender and receiver (Goyal et al., 2011). The quantum mechanism is the base of the quantum cryptography process consists of two important elements.

Heisenberg Uncertainty Principle

In 1927, a German researcher Werner Heisenberg proposed Heinsenberg's principle of uncertainty which states that it is not possible to observe and calculate two properties at a time of an object and always shows uncertainty. For an instance, consider an object with the properties like position (x) and moving with the velocity (p) cannot be calculated simultaneously because it does not make sense to exist. A person's weight is not determined by his height. This idea works when we try to observe and calculate anything. The Heisenberg uncertainty prevents the intruder when applying this principle to protons because the proportions are affected by the polarity of the photon.

Photon Polarization Principle

This principle uses non-cloning methods to ensure that the attacker does not copy unique quantum bits. This creates a quantum state which cannot be recognized and distorts other information if anyone tries to measure the bit. Quantum cryptography is a solution for cryptographic functions that cannot be performed with classical cryptography. It is the safest solution to the problem in the key exchange process (Bhatt & Sharma, 2019).

The Contribution of the Pioneers

It seems that history is about to repeat itself for computers this time. Quantum cryptography began the evolution of quantum computers and remembered the history of a research paper written by Einstein's with the title "Theory of Relativity". The paper rewrote Newton's laws basic principles of physics and changed the world's understandings of physics. Quantum computer rewrites all computer concepts right from scratch. The computer is defined based on dimensions like software, hardware, database, and applications. But the Quantum computers are in the process of switching to older computers and gaining the level called Quantum Supremacy. This happened due to the contribution of its pioneers.

Quantum computing is known as 'quantum circuit' which works like programs, specifying a set of quantum machine operations to run. In the late 1960s, two researchers Stephen Weissner and Gilles Brassrd of Columbia University tried to solve the problems of classical cryptography very first time. They wrote a research paper for IEEE Information Theory Society which was rejected but then published in SIGACT News in the early 1980s.

Stephen Weissner and Gilles Brassrd proposed the idea of the Conjugate Code. Conjugate code is a way to encode and transmit two messages with two different forms. The concept of photon polarization is used in a linear and circular form where it is possible either to receive and decode messages on the safe and two stages secured channel. They titled the protocol "Quantum Key Distribution Protocol" which is widely known as the concept QKD. As the protocol was proposed in the year 1984, the method became famous as Bennett and Bassard 1984 (BB84) method.