Chapter 3
Quantum Cryptography:
In Security Aspects

S. Venkata Lakshmi
https://orcid.org/0000-0001-7965-6552
Sri Krishna College of Engineering and Technology, India

Sujatha Krishnamoorthy
Wenzhou-Kean University, China

Mudassir Khan
https://orcid.org/0000-0002-1117-7819
King Khalid University, Saudi Arabia

Neeraj Kumar
https://orcid.org/0000-0002-6674-0584
Babasaheb Bhimrao Ambedkar University, Lucknow, India

Varsha Sahni
CT India, India

ABSTRACT

Cryptography is used for the secure communication in which two parties are involved. The most popular cryptographic issue is the transmission of confidential messages. The privacy is maintained using the cryptographic protocol. The security of quantum cryptography relies more on physics including quantum mechanics and statistics rather than on solving mathematical problems. A well-known application of quantum cryptography is quantum key distribution (QKD) that is used to establish communication by generating cryptographic keys. Moreover, it is based on the Heisenberg uncertainty principle that ensures the security and prevents from eavesdropping. Basically, quantum cryptography with faint laser pulses, polarization coding, phase coding, and frequency coding have been discussed.

DOI: 10.4018/978-1-7998-6677-0.ch003

1. INTRODUCTION

Information Technology and Communication has undergone development remarkably in the past years. To secure the communication among the parties from adversary the technique that is used is called as Cryptography. Main aim of Cryptography is to ensure Confidentiality (Third party cannot interpret the message or data that is sent between intended users), Authentication (Message is received from authentic user), Integrity (Message is not altered in between). This is achieved by sending secret message that requires the creation of the key that is sent to the other party. This key can be stolen or can be copied by the third party. Public key Cryptography can involve complex mathematical calculation that makes the process slower. To overcome these limitations and to make the communication more secure quantum Cryptography is used. Quantum cryptography was built in late 1960, when conjugate coding was written by Stephen Wiesner. Quantum Cryptography is an approach to transmit the information securely by applying the concept of quantum physics. Mathematical cryptography algorithms like RSA and elliptic curve cryptography are widely used today. There is a lack of security in these algorithms. There is a threat to sensitive information that needs high degree of security by these prevailing mathematical cryptosystems. The security of quantum cryptography relies more on physics including quantum mechanics and statistics rather than on solving mathematical problems. Well known application of quantum cryptography is quantum key distribution (QKD) that is used to establish communication by generating cryptographic keys. Moreover, it is based on Heisenberg Uncertainty principle that ensures the security and prevents from eavesdropping. Even if there is any case of eavesdropping of key that occurs by adversary, the two parties communicating with each other can come to know easily about this due to some discrepancies. QKD device comprise of photon transceiver along with electrical component. There are various limitations of QKD as well like the range is limited from 50 to 100 km as photons are easily lost during communication. Quantum Computing follows the principles of superposition, entanglement and quantum mechanics. Superposition refers to as making new moves while processing information. Quantum Superposition states that 2 particles can be at distinct locations at the same time. It is not feasible to observe it in real world as it exists in subatomic particles. Entangled particles refer to the state where the particles cannot be defined or described individually, without the consideration of other particles. In Quantum mechanics qubits are used rather than simple bits on which quantum cryptography is highly dependent on.

2. LITERATURE SURVEY

- Aditya et al. (2005) discussed on quantum cryptography and how it contribute to a defense-in-depth strategy to reduce the efforts of malicious hackers. There are various weaknesses in modern digital cryptosystems that are explained which involves complex calculations that are slow. These weaknesses are overcome by quantum cryptography that is based on the fundamental and unchanging principles of quantum mechanics. Quantum Key Distribution example is demonstrated that explain the secure distribution of keys. Desirable Characteristics of QKD are discussed that involves Confidentiality, Authentication, Rapid Key Delivery, Robustness, Location Independence and its Resistance to traffic Analysis. Different Systems have implemented Quantum Cryptography like DARPA Quantum Network, MagiQ Technologies. Quantum cryptography involves a suite of specialized protocol involving Sifting, Error Correction, Privacy amplification, Authentication.