Chapter 41
Quantum Cryptography

Ahmed Mahmoud Abbas
The American University in Cairo, Egypt

ABSTRACT

Quantum cryptography is known the most up-to-date in domain of realistic cryptography notably the menace of quantum cryptanalysis which threatens security firmness of public key cryptography. Quantum cryptography has a famous scheme known as Quantum Key Exchange (QKE), that administrates generation and distribution of a secured random key between legitimate channel users depicted as sender and receiver. Consequently, such key could be used as a key for one-time pad hybrid cryptosystems to encrypt and authenticate messages over a quantum channel. (QKE) is based on unifying quantum physics concepts and information theory with conventional cryptographic schemes that target to produce a short secret session key between any two legitimate parties. An important phase in key creation of BB84 protocol is Privacy Amplification phase where two interconnecting parties distill highly secret shared key from a larger body of shared key, which is only partially secret. The two legitimate parties publicly exchange information to create a compressed key free from biased bits known by an eavesdropper.

INTRODUCTION

Classical cryptosystems as (DES) or (RSA) were built on basis of guessing work and mathematics. Many theories proved that traditional secret-key cryptosystems are not reasonably secure enough if the key is not used once and at least long as the plaintext. On the contrary, the computational theory was not concluded well as to prove the computational security of public-key cryptosystems. Later, Charles Bennett (IBM Researcher) and Gillis Brassard (University of Montréal) developed a new cryptography system built on quantum physics. Conventionally, it was understood that digital communication could be always passively observed or duplicated even by less awareness people. However, when information is encoded into non-orthogonal quantum states as single photons with polarization directions of vertical (0) and rectilinear (90) degrees and the diagonal basis of (45) and (135) degrees, we can reach a communication channel whose transmissions could not be listened or duplicated reliably by an attacker unaware of specific key information used in transmission formation. The attacker would not even have partial information about this transmission without varying it arbitrarily and uncontrollable way as to be detected via channel's authenticated users (Bennett, & Brassard, 1984).

DOI: 10.4018/978-1-5225-5634-3.ch041

Recently, quantum coding was utilized in combination with public key cryptographic processes to produce many schemes for unduplicated subway tokens. This is to illustrate the quantum coding by its own achievement a main advantage of public key cryptography by permitting secure distribution of random key information between parties that have no initial shared secret information knowing that parties have access, besides the quantum channel, to another regular channel vulnerable to passive yet not active eavesdropping. Moreover, in appearance of active eavesdropping, the two communicating parties are able to distribute the key securely in case they share some initial secret information provided eavesdropping is not much active to overcome communications totally (Bennett, & Brassard, 1984).

Orthodox public key encryptions use trap door functions to seal messages' mean between two users from a passive eavesdropper, irrespective the deficiency of any initial shared secret information between two parties. In quantum public key distribution, quantum channel is not only used to transmit meaningful messages, but also it is rather used to transfer a supply of arbitrary bits between two users who have no initial shared secret information in a way these users consequently check over a regular non-quantum channel subject to passive eavesdropping. Users can determine with high opportunity if the original quantum transfer has been disturbed in transmission as of eavesdropper's activity or not. If transmission was not disturbed, users agree to use these shared secret bits in a way known as one-time pad in order to close any means of continuing meaningful communications asking for shared secret arbitrarily information. However, if transmission was disturbed, users neglect it and try again, deferring any meaningful communications until they manage to transfer adequate arbitrarily bits via quantum channel to act as a one-time pad (Bennett, & Brassard, 1984).

Quantum cryptography is appropriate as a quantum technology for uniquely secured generation and distribution of fully random secret keys among communicating parties. Quantum cryptography is a technology utilizing a combination of "quantum mechanics phenomena and classical cryptographic techniques" aiming a target of extending short secret keys shared between two communication parties. The security measure of this extended key is a "function of the error rate found in an intermediate step of the key generation protocol". Therefore, the likelihood for an eavesdropper to listen on communicated messages on the extended key up to some agreed tolerance limit is a function that relies on the error rate and the deployed protocol details. The speculated value of the attacker information can exponentially be made small via proper protocol selection, under condition of the calculated error rate after quantum communication is less than a constant value of (11%). Applying such conditions, the key gain is secured and could be developed within the framework of a variety of classic cryptographic techniques (Kollmitzer, Monyk, Peev, & Suda, 2002). The important steps in quantum key developing protocol are as follows (Kollmitzer, Monyk, Peev, & Suda, 2002):

- Creation of shifted key between (Alice) and (Bob), using one of primary processes as: single photons, entangled photons, polarization methods, phase methods and sub protocol stages as quantum cryptographic protocols as (BB84) and (B92) (Kollmitzer, Monyk, Peev, & Suda, 2002).
- Reconciliation process or error correction for errors and differences between keys with (Alice) and (Bob) (Kollmitzer, Monyk, Peev, & Suda, 2002).
- Privacy Amplification process by lessening of a potential eavesdropper gained information during the initial creation of the key (Kollmitzer, Monyk, Peev, & Suda, 2002).