Quantum Key Distribution: A Secure Key Exchange Method in Quantum Cryptography

Ajit Singh\(^1\) and Nidhi Sharma\(^2\)

Department of Computer Science & Engineering, BPS Mahila Vishwavidyalaya, Khanpur Kalan, Ðonepat-131305 Haryana (India).

\(^1\)ghanghas_ajit@rediffmail.com

ABSTRACT

Present Paper provides a detailed study of Quantum Key Distribution (QKD) which is used in the quantum cryptography to enhance the data security during communication. In the first phase a detailed description of QKD is given, which permits the secure delivery of encryption keys between two parties as an adversary cannot eavesdrop without being detected. In the next phase the emphasis is on the protocol used in the quantum cryptography for Key Distribution. Finally, the various limitations and benefits of QKD have been discussed.

KEYWORDS

Conventional Cryptography, Quantum cryptography, E91 Protocol, BB84 protocol, Quantum Key Distribution.

1. INTRODUCTION

Cryptography is the science of encrypting the data to provide the security during transmission and decrypting data at the time of receiving. Conventional cryptography uses mathematical approach to create key that can be further used for data transmission.

Conventional method has some shortcomings. For example, the problems like factorization of large prime numbers that are treated as impossible to solve are no longer remain secure.

They can be solved using Quantum computers within a finite time. Hence requirement of a better secure method is felt and Quantum Cryptography originates. [1].

2. QUANTUM CRYPTOGRAPHY

The main problem of secret-key cryptosystems is secure distribution of keys [1]. It is here that quantum mechanics offers a solution. While the security of public key cryptographic methods can be undermined by the advancement in technology and mathematical algorithms, the quantum approach will provide unconditional security [2]. Within the framework of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into any property of a classical object can be acquired without changing the state of the object. All classical signals can be monitored passively. In classical information, one bit of information is encoded in billions of photons, electrons, atoms, or other carriers. You can always deviate part of the signal and perform a measurement on it, whereas in quantum mechanics, any projective measurement will induce disturbances.

QC is an effort to allow two users of a common communication channel to create a body of shared and secret information. This information, which generally takes the form of a random string of bits, can then be used as a conventional secret key for secure communication. QC systems take advantage of Heisenberg's uncertainty principle [4], according to which the more precisely one property is measured, the less precisely the other can be measured, hence measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement. This yields a cryptographic system for the distribution of a secret random cryptographic key between two parties initially sharing no secret information that is secure against an eavesdropper [3].

QC allows for secure key agreement over an entrusted channel where the output key is entirely independent from any input value, a task that is impossible using conventional cryptography. [1]

It does not eliminate the need for other cryptographic primitives, such as authentication, but it can be used to build systems with new security properties. The properties that are used to establish secure communication are divided into three phases. These phases are:

a). Key agreement: Two parties agree upon a secure, shared private key.

b). Authentication: It assures that a message comes from a legitimate party.

c). Key usage: Once a secure key is established, it can be used for encryption, authentication, or other cryptographic purposes.

3. QUANTUM KEY DISTRIBUTION

Quantum Key Distribution [3] is a technology, based on the quantum laws of physics, rather than the assumed computational complexity of mathematical problems, to generate and distribute provably secure cipher keys over unsecured channels. It does this using single photon technology and can detect potential eavesdropping via the quantum bit error rates of the quantum channel. Sending randomly encoded information on single photons produces a shared secret that is a random string and the probabilistic nature of measuring the photon state provides the basis of its security [7].

A QKD system consists of a quantum channel and a classical channel. The quantum channel is only used to transmit qubits (single photons) and must consist of a transparent optical path (fiber, free-space and optical switches, no routers, amplifiers or
copper). It is a lossy and probabilistic channel. The classical channel can be a conventional IP channel (not necessarily optical), but depending on system design it may need to be dedicated and closely tied to the quantum channel for timing requirements. It would not be unusual for the quantum and classical channels to share a common fiber via wavelength division multiplexing.

The Key generation in QKD is done by communicating through quantum channels [6]. This way of communication has the ability to create true random and secret key, which can then be used as seeds to conventional cryptographic methods for the generation of suitable keys.

The exchange of information through Quantum channel can be shown with the help of diagram [8].

**Step 1:** Alice begins by sending a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarizations that correspond to vertical, horizontal or diagonal in opposing directions (0, 45, 90 or 135 degrees).

**Step 2:** Bob will randomly choose a filter and use a photon receiver to count and measure the polarization which is either rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees).

**Step 3:** Next, using an out-of-band communication system, Bob will inform Alice to the type of measurement made and which measurements were of the correct type without mentioning the actual results.

**Step 4:** The photons that were incorrectly measured will be discarded, while the correctly measured photons are translated into bits based on their polarization.

**Figure 1:** Quantum Key Exchange

### 4. CRYPTOGRAPHIC PROTOCOL

There are two protocols used for Quantum key distribution. These are as follows:

- **The BB84** [6,8]:
  - BB84 is the protocol most widely used for quantum key distribution. It was invented by Charles H. Bennett and Gilles Brassard in the year 1984. It allows two users to establish an identical and purely random sequence of bits at two different locations while allowing revealing of any eavesdropping. In the lab experiment, the BB84 protocol encodes single photon polarizations using two bases of the same 2-dimensional Hilbert space:
    - **rectilinear basis** \{0°: |→⟩, 90°: |↑⟩\}
    - **diagonal basis** \{45°: |↗⟩, 135°: |↘⟩\}

  The only requirement on the involved quantum states is actually that they belong to mutually non-orthogonal bases of their Hilbert space, where each vector of one basis has equal-length projections onto all vectors of the other basis. If a measurement on a system is performed in a basis different from the one the system is prepared in, its outcome is completely random and the system loses all the memory of its previous state.

  Any measurement in the diagonal basis on photons prepared in the rectilinear basis will yield random outcomes with equal probabilities and vice versa. On the other hand, measurements performed in the basis identical to the basis of preparation of states will produce deterministic results. The protocol relies on Heisenberg’s uncertainty principle which forbids the measurement of more than one polarization component of one photon.

  To exchange a secret key in the BB84 protocol, Alice and Bob must do as follow:
    - Alice creates a binary random number and sends it to Bob using randomly the two different bases + (rectilinear) and X (diagonal):
      - |→⟩ and |↗⟩ both represent 1
      - |↑⟩ and |↘⟩ both represent 0

    Therefore, Alice transmits photons randomly in the four polarization states |→⟩, |↑⟩, |↗⟩, and |↘⟩.

    - Bob simultaneously measures the polarization of the incoming photons using randomly the two different bases. He does not know which of his measurements are deterministic, i.e. measured in the same basis as the one used by Alice.

    - Later, Alice and Bob communicate to each other the list of the bases they used. This communication carries no information about the value of the measurement, but allows Alice and Bob to know which values was measured by Bob correctly.

    - Bob and Alice keep only those bits that were measured deterministically and will disregard those sent and measured in different bases. Statistically, their bases coincide in 50% of all cases, and Bob’s measurements agree with Alice’s bits perfectly.

    - Together, they can reconstitute the random bit string created previously by Alice.
4.1 E91 PROTOCOL
This protocol was invented by Artur Ekert (1991). The Ekert scheme uses entangled pairs of photons. These can be created by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Alice and Bob each end up with one photon from each pair[5]. The scheme relies on three properties of entanglement.

- First, we can make entangled states which are perfectly correlated in the sense that if Alice and Bob both test whether their particles have vertical or horizontal polarizations, they will always get opposite answers. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. However, their individual results are completely random: it is impossible for Alice to predict if she will get vertical polarization or horizontal polarization [9].

- Second, these states have a property often called quantum non-locality, which has no analogue in classical physics or everyday experience. If Alice and Bob carry out polarization measurements, their answers will not be perfectly correlated, but they will be somewhat correlated. That is, there is an above-50% probability that Alice can, from her measurement, correctly deduce Bob's measurement, and vice versa. And these correlations are stronger - Alice's guesses will on average be better - than any model based on classical physics or ordinary intuition would predict.

- Third, any attempt at eavesdropping by Eve will weaken these correlations, in a way that Alice and Bob can detect.

4.2 SARG04 PROTOCOL
This protocol is derived from BB84 protocol. SARG04 was defined by Scarani et al. in 2004 in Physical Review Letters as a prepare and measure version (in which it is equivalent to BB84 when viewed at the level of quantum processing). Researchers built SARG04 when they noticed that by using the four states of BB84 with a different information encoding they could develop a new protocol which would be more robust when attenuated laser pulses are used instead of single-photon sources. The intended use of SARG04 is in situations where the information is originated by a Poissonian source producing weak pulses (this means: mean number of photons < 1) and received by an imperfect detector. This protocol is more robust than BB84 protocol against incoherent PNS attacks. [11]

5. LIMITATIONS [12]
- Distance: The longer the distance that the photons have to travel, the more photons that are lost to decoherence and noise and hence the lower the rate of secret key formation. The longest QKD experiments to date have achieved secure key generation over a 184.6km fiber optic link and over a free-space link spanning a distance of 144km at a rate of 12.8 bits/second [10]. Quantum repeaters overcome the distance limitation, allowing shared quantum states to be established between distant parties. These systems are not yet operational, they are easier to implement than full-scale quantum computers; theoretical and experimental work progresses on their development.

- Key rate: While long distance experiments achieve very low key rates on the order of a few bits per second, shorter distance experiments have demonstrated very high key rates. Experimental groups have achieved key rates of over 4 MB per second over 1 km of fibre and 1 Mb per second at 20 km. These key rates are an impressive accomplishment is coming closer to the rates needed to secure real communication channels.

When a QKD key is used for encryption, current key rates may not be sufficient for a one-time pad and
hybrid schemes need to be used, in which the QKD key is used as the private key in a symmetric.

- **Cost:** QKD is currently a costly technology and requires dedicated hardware. Additionally, it requires separate sub-networks of optical fibre that enhances its cost.
- **Noise:** It affects on key establishment.
- **Exclusive Dedicated Network:** There requires a separate private network for implementation of QKD. It requires additional bandwidth to implement. QKD also requires its own sub-network to generate keys, although this sub-network may use/share existing communication infrastructure.

6. **BENEFITS OF QKD**

The benefits of QKD are that it can generate and distribute provably secure keys over unsecured channels and potential eavesdropping can be detected. QKD is not subject to threats from quantum computers or break through algorithms that can defeat the current computationally complex key exchange methods. Because QKD generates random strings for shared secrets, attaining a QKD system and reverse engineering its theory of operation would yield no mechanism to defeat QKD. QKD can use existing optical media infrastructure for both quantum and classical channels, but the quantum channel photons cannot pass through amplifiers or routers. Optically transparent switches are okay and thus switched networks of QKD systems are possible [12].

7. **CONCLUSION**

Quantum Key Distribution is the effective method for the key exchange and provide integration with the quantum cryptography to enhance the security during communication. It is based on the quantum laws of physics, rather than the assumed computational complexity of mathematical problems, to generate and distribute provably secure cipher keys over unsecured channels and provide unconditional security. There is number of protocol are used for the quantum key distribution but BB84 protocol is the one of the most commonly used protocol for the quantum key distribution in the quantum cryptosystem.

**REFERENCES**

[1]. Douglas Stebila, Michele Mosca and Norbert Lütkenhaus “The case for Quantum Key Distribution.” December 2, 2009
[3]. Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys, 4 41.1-41.8
[5]. Aditya Goel “Key Distribution in PKC through Quantas” International Journal on Applications of graph theory in wireless ad hoc networks and sensor networks (Graph-hoc), Vol. 2 No.1, March 2010.